



Вол. 71, бр. 4

2023



ISSN 0042-8469
e-ISSN 2217-4753
УДК 623 + 355/359

НАУЧНИ ЧАСОПИС МИНИСТАРСТВА ОДБРАНЕ И ВОЈСКЕ СРБИЈЕ

ВОЈНОТЕХНИЧКИ ГЛАСНИК



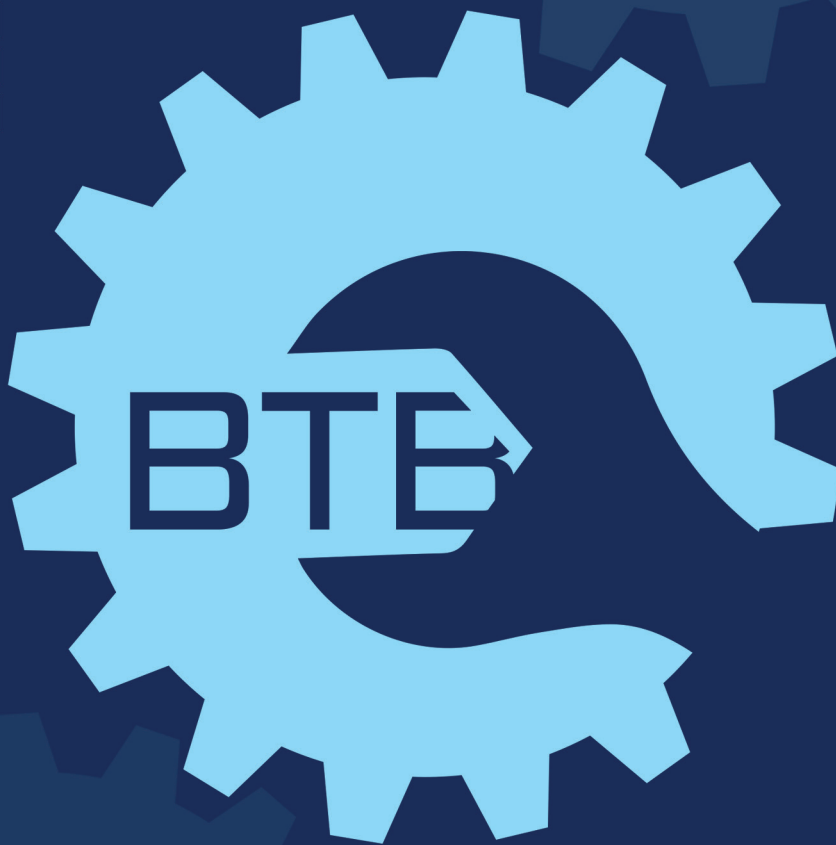


Том 71, № 4

2023



ISSN 0042-8469
e-ISSN 2217-4753
УДК 623 + 355/359



НАУЧНЫЙ ЖУРНАЛ МИНИСТЕРСТВА ОБОРОНЫ
И ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ СЕРБИЯ

ВОЕННО-ТЕХНИЧЕСКИЙ ВЕСТНИК

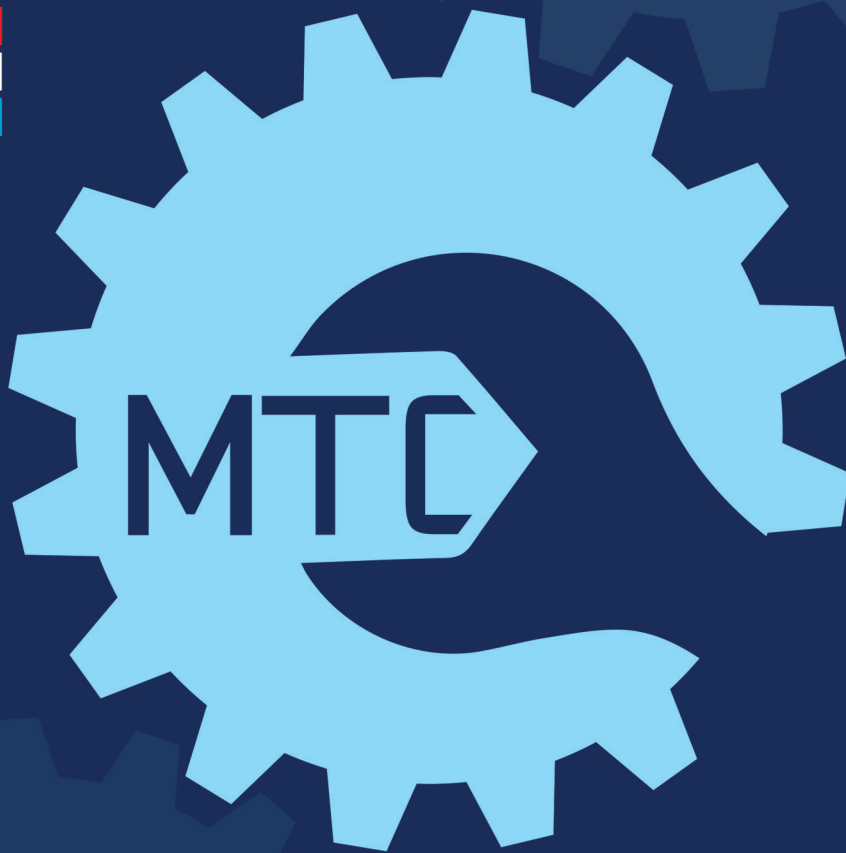




ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359

Vol. 71, Issue 4

2023



SCIENTIFIC JOURNAL OF THE MINISTRY OF DEFENCE AND THE SERBIAN ARMED FORCES

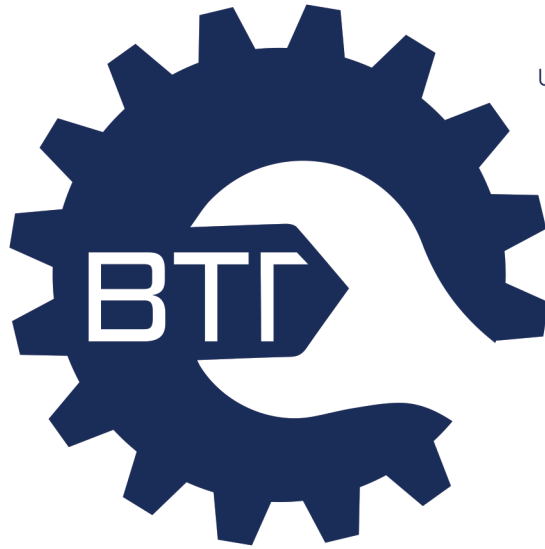
MILITARY TECHNICAL COURIER

MILITARY TECHNICAL COURIER

4 2023



ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359



НАУЧНИ ЧАСОПИС МИНИСТАРСТВА ОДБРАНЕ И ВОЈСКЕ СРБИЈЕ
ВОЈНОТЕХНИЧКИ ГЛАСНИК
ВОЛУМЕН 71 • БРОЈ 4 • ОКТОБАР – ДЕЦЕМБАР 2023.



NAUČNI ČASOPIS MINISTARSTVA ODBRANE I VOJSKE SRBIJE
VOJNOTEHNIČKI GLASNIK
VOLUMEN 71 • BROJ 4 • OKTOBAR – DECEMBAR 2023.

BT.MO.YIP.CP6
www.vtg.mod.gov.rs
COBISS.SR-ID 4423938
DOI: 10.5937/VojnotehnickiGlasnik

ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359



НАУЧНЫЙ ЖУРНАЛ МИНИСТЕРСТВА ОБОРОНЫ И ВООРУЖЁННЫХ СИЛ РЕСПУБЛИКИ СЕРБИЯ

ВОЕННО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ТОМ 71 • НОМЕР ВЫПУСКА 4 • ОКТЯБРЬ – ДЕКАБРЬ 2023.



SCIENTIFIC JOURNAL OF THE MINISTRY OF DEFENCE AND SERBIAN ARMED FORCES

MILITARY TECHNICAL COURIER
VOLUME 71 • ISSUE 4 • OCTOBER – DECEMBER 2023

втг.мо.унп.срб
www.vtg.mod.gov.rs
COBISS.SR-ID 4423938
DOI: 10.5937/VojnotehnickiGlasnik

ВЛАСНИЦИ:

Министарство одбране и Војска Србије

ИЗДАВАЧ:

Универзитет одбране у Београду, Војна академија

УРЕДНИШТВО (странице чланова уредништва у ORCID iD-у, Google Scholar-у, Web of Science ResearcherID-у, Scopus Author ID-у и РИНЦ-у доступни су на

<http://www.vtg.mod.gov.rs/urednistvo.html>):

ГЛАВНИ И ОДГОВОРНИ УРЕДНИК

Др Драган Памучар, Универзитет у Београду, Факултет организационих наука, Београд, Србија,
e-mail: dragan.pamucar@fon.bg.ac.rs

УРЕДНИК

Мр Небојша Гаћеша, Универзитет одбране у Београду, Војна академија, Београд, Србија,
e-mail: nebojsa.gacesa@mod.gov.rs, tel. 011/3603-260, 066/87-00-123

Уредник за област математике и механике

Др Драган Трифковић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област електронике, телекомуникација и информационих технологија

Др Бобан Бонцулић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област машинства

Др Бранимир Крстић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област материјала и хемијских технологија

Др Радован Каркалић, Универзитет одбране у Београду, Војна академија, Београд, Србија

УРЕЂИВАЧКИ ОДБОР:

Др Иван Гутман, Српска академија наука и уметности, Београд, Србија,

Др Градимир Миловановић, Српска академија наука и уметности, Београд, Србија,

Др Ђи-Хуан Хи, Универзитет Суџоу, Факултет за текстилну и одевну технику, Суџоу, Кина,

Др Стојан Раденовић, Универзитет у Београду, Машински факултет, Београд, Србија,

Др Мађид Тафана, Универзитет Ла Сал, Одељење за пословне системе и аналитику,
Филаделфија, САД,

Др Валентин Попов, Технички универзитет у Берлину, Одељење за динамику система и физику
трења, Берлин, Немачка,

Др Шанкар Чакраборти, Универзитет Јадавпур, Одељење за производно машинство, Калкута, Индија,

Др Радун-Емил Прекуп, Универзитет Политехника у Темишвару, Темишвар, Румунија,

Др Јургита Антуцхевичи, Технички универзитет Гедиминас у Вилњусу, Грађевински факултет,
Вилњус, Литванија,

Др Срећко Јоксимовић, Универзитет у Јужној Аустралији, Аделејд, Аустралија,

Др Мортеза Јаздани, Факултет за бизнис и маркетинг ESIC, Мадрид, Шпанија,

Др Прасенцит Чатерџи, Институт за инжењерство MCKV, Одељење за машинство, Ховрах, Индија,

Др Жељко Стевић, Универзитет у Источном Сарајеву, Саобраћајни факултет, Добој, Република Српска, БиХ,

Др Хамед Фазлопахтабар, Универзитет Дамган, Одељење за индустријско инжењерство, Дамган, Иран,

Др Јарослав Ватробски, Универзитет у Шчећину, Факултет за економију, финансије и
менаџмент, Шчећин, Пољска,

Др Кристиано Фрагаса, Универзитет у Болоњи, Одељење за индустријско инжењерство, Болоња, Италија,

Др Војцех Салабун, Западнопомерански технолошки универзитет у Шчећину, Факултет
рачунарских наука и информационих технологија, Шчећин, Пољска,

Др Иева Меидуте-Кавалиаускиене, Војна академија Литваније „Генерал Јонас Жемаитис“,
Вилњус, Литванија,

Др Шарка Мајерова, Универзитет одбране у Брну, Одељење за математику и физику, Брно, Чешка Република,

Др Фатих Ецер, Универзитет Афион Кођатепе, Факултет за економију и административне науке,
Афионкарахисар, Турска,

Др Ернесто Д.Р. Сантибанез Гонзалез, Универзитет у Талки, Одељење за индустријско
инжењерство, Талка, Чиле,

Др Драган Маринковић, Технички универзитет у Берлину, Факултет за машинске и транспортне
системе, Берлин, Немачка,

Др Стефано Валвано, Универзитет Коре у Ени, Одељење за ваздухопловни инжењеринг, Ена, Италија,

Др Рафал Мадонски, Универзитет Ђинан, Центар за истраживање електричне енергије, Гуангџоу, Кина,

Др Миленко Андрић, Универзитет одбране у Београду, Војна академија, Београд, Србија,

Др Самарџит Кар, Национални институт за технологију, Одељење за математику, Дургапур, Индија,

Др Росен Митрев, Технички универзитет у Софији, Софија, Бугарска,

Др Бојан Милановић, Универзитет одбране у Београду, Војна академија, Београд, Србија,

Др Ирик Мухамедзјанов, Државни нафтни технолошки универзитет у Уфи, Уфа, Руска Федерација,

Др Павел Отрисал, Универзитет Палацки, Оломоуц, Чешка Република,

Др Радован Радовановић, Криминалистичко-полицијски универзитет, Београд, Србија.

СОБСТВЕННИКИ: Министерство обороны и Вооружённые силы Республики Сербия

ИЗДАТЕЛЬСТВО: Университет обороны в г. Белград, Военная академия

РЕДАКЦИЯ (со страницами членов редакции в ORCID iD, Google Scholar, Web of Science ResearcherID, Scopus Author ID и РИНЦ можно ознакомиться на сайте <http://www.vtg.mod.gov.rs/redakcia.html>):

ГЛАВНЫЙ И ОТВЕТСТВЕННЫЙ РЕДАКТОР

Д-р Драган Памучар, Белградский университет, факультет организационных наук, г. Белград, Сербия, e-mail: dragan.pamucar@fon.bg.ac.rs

РЕДАКТОР

Кандидат технических наук Небойша Гачеша, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия, e-mail: nebojsa.gacesa@mod.gov.rs, тел. +381 11 3603 260, +381 66 87 00 123

Редактор в областях: математика и механика

Д-р Драган Трифкович, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия

Редактор в областях: электроника, телекоммуникации и информационные технологии

Д-р Бобан Бонджулич, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия

Редактор в области: машиностроение

Д-р Бранимир Крстич, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия

Редактор в областях: материаловедение и химические технологии

Д-р Радован Каркалич, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Д-р Иван Гутман, Сербская академия наук и искусств, г. Белград, Сербия,

Д-р Градимир Милованович, Сербская академия наук и искусств, г. Белград, Сербия,

Д-р Джи-Хуан Хи, Университет Сучжоу, факультет текстиля и производства одежды, г. Сучжоу, Китай,

Д-р Стоян Раденович, Белградский университет, машиностроительный факультет, г. Белград, Сербия,

Д-р Маджид Тафана, Университет Ла Саль, департамент бизнес-систем и аналитики, г. Филадельфия, США,

Д-р Валентин Попов, Берлинский технический университет, департамент динамики систем и физики трения, г. Берлин, Германия,

Д-р Шанкар Чакраборти, Университет Джадавпур, департамент производственных машин, г. Калькутта, Индия,

Д-р Радун-Емил Прекуп, Политехнический университет Тимишоары, г. Тимишоара, Румыния,

Д-р Юргита Антучевичене, Вильнюсский технический университет имени Гедиминаса, строительный факультет, г. Вильнюс, Литва,

Д-р Мартаз Иаздан, Школа бизнеса и маркетинга ESIC, г. Мадрид, Испания,

Д-р Прасенджит Чатерджи, Институт инженерии MCKV, департамент машиностроения, г. Хаора, Индия,

Д-р Желько Стевич, Восточно-Сараевский университет, транспортный факультет, г. Добой, Республика Сербская, БиГ,

Д-р Хамед Фазлолахтбар, Университет Дамгана, департамент промышленной инженерии, г. Дамган, Иран,

Д-р Ярослав Ватробски, Щецинский университет, факультет экономики, финансов и менеджмента, г. Щецин, Польша,

Д-р Кристиано Фрагаса, Болонский университет, департамент промышленной инженерии, г. Болонья, Италия,

Д-р Войчех Салабун, Западно-Померанский технологический университет в г. Щецин, факультет компьютерных наук и информационных технологий, г. Щецин, Польша,

Д-р Иева Меидуте-Кавалиаускиене, Литовская Военная академия им. генерала Йонаса Жемайтиса, г. Вильнюс, Литва,

Д-р Шарка Маерова, Университет обороны в г. Брно, физико-математический департамент, г. Брно, Чешская Республика,

Д-р Фатих Ецер, Университет Афьон Коджатеппе, Факультет делового администрирования, г. Афьонкарахисар, Турция,

Д-р Эрнесто Д.Р. Сантибанез Гонзалез, Университет Тальки, департамент промышленной инженерии, г. Талька, Чили,

Д-р Драган Маринкович, Берлинский технический университет, факультет машиностроительных и транспортных систем, г. Берлин, Германия,

Д-р Стефано Валвано, Университет Коре Энна, департамент авиационной инженерии, г. Энна, Италия,

Д-р Рафал Мадонски, Университет Цзинань, Центр энергетических исследований, г. Гуанчжоу, Китай,

Д-р Миленко Андрич, Университет обороны в г. Белград, Военная академия, г. Белград, Сербия,

Д-р Самарджит Кар, Национальный технологический институт, департамент математики, г. Дургапур, Индия,

Д-р Росен Митрев, Софийский технический университет, г. София, Болгария,

Д-р Боян Миланович, Университет обороны в г. Белград, г. Белград, Сербия,

Д-р Ирик Мухаметзянов, Уфимский государственный нефтяной технический университет, г. Уфа, Российская Федерация,

Д-р Павел Отрисал, Университет Палацкого, Оломоуц, Чешская Республика,

Д-р Радован Радованович, Университет криминалистики и полицейской подготовки, г. Белград, Сербия.

OWNERS:

Ministry of Defence and Serbian Armed Forces

PUBLISHER:

University of Defence in Belgrade, Military Academy

EDITORIAL TEAM (the pages of the Editorial Team's members in ORCID iD, Google Scholar, Web of Science ResearcherID, Scopus Author ID, and ПИИЦ can be accessed at <http://www.vtg.mod.gov.rs/editorial-team.html>):

EDITOR IN CHIEF

Dr. Dragan Pamučar, University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia, e-mail: dragan.pamucar@fon.bg.ac.rs

EDITOR

Nebojša Gaćeša, MSc, University of Defence in Belgrade, Military Academy, Belgrade, Serbia, e-mail: nebojsa.gacesa@mod.gov.rs, tel. +381 11 3603 260, +381 66 87 00 123

Editor for Mathematics and Mechanics

Dr. Dragan Trifković, University of Defence in Belgrade, Military Academy, Belgrade, Serbia

Editor for Electronics, Telecommunications and Information Technology

Dr. Boban Bondžulić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia

Editor for Mechanical Engineering

Dr. Branimir Krstić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia

Editor for Materials and Chemical Technologies

Dr. Radovan Karkalić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia

EDITORIAL BOARD:

Dr. Ivan Gutman, Serbian Academy of Sciences and Arts, Belgrade, Serbia,

Dr. Gradimir Milovanović, Serbian Academy of Sciences and Arts, Belgrade, Serbia,

Dr. Ji-Huan He, Soochow University, College of Textile and Clothing Engineering, Soochow, China,

Dr. Stojan Radenović, University of Belgrade, Faculty of Mechanical Engineering, Belgrade, Serbia,

Dr. Madjid Tavana, La Salle University, Business Systems and Analytics Department, Philadelphia, USA,

Dr. Valentin Popov, Technical University Berlin, Department of System Dynamics and Friction Physics, Berlin, Germany,

Dr. Shankar Chakraborty, Jadavpur University, Department of Production Engineering, Kolkata, India,

Dr. Radu-Emil Precup, Politehnica University of Timisoara, Department of Automation and Applied Informatics, Timisoara, Romania,

Dr. Jurgita Antuchevičienė, Vilnius Gediminas Technical University, Faculty of Civil Engineering, Vilnius, Lithuania,

Dr. Morteza Yazdani, ESIC Business and Marketing School, Madrid, Spain,

Dr. Prasenjit Chatterjee, MCKV Institute of Engineering, Department of Mechanical Engineering, Howrah, India,

Dr. Željko Stević, University of East Sarajevo, Faculty of Transportation, Doboј, Republic of Srpska, Bosnia and Herzegovina,

Dr. Hamed Fazlollahtabar, Damghan University, Department of Industrial Engineering, Damghan, Iran,

Dr. Jarosław Wątróbski, University of Szczecin, Faculty of Economics, Finance and Management, Szczecin, Poland,

Dr. Cristiano Fragassa, University of Bologna, Department of Industrial Engineering, Bologna, Italy,

Dr. Wojciech Sałabun, West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, Szczecin, Poland,

Dr. Ieva Meidutė-Kavaliauskienė, General Jonas Žemaitis Military Academy of Lithuania, Research Group on Logistics and Defense Technology Management, Vilnius, Lithuania,

Dr. Šárka Mayerová, University of Defence in Brno, Department of Mathematics and Physics, Brno, Czech Republic,

Dr. Fatih Ecer, Afyon Kocatepe University, Faculty of Economics and Administrative Sciences, Afyonkarahisar, Turkey,

Dr. Ernesto D.R. Santibanez Gonzalez, Universidad de Talca, Department of Industrial Engineering, Talca, Chile,

Dr. Dragan Marinković, Technical University Berlin, Faculty of Mechanical and Transport Systems, Berlin, Germany,

Dr. Stefano Valvano, Kore University of Enna, Department of Aerospace Engineering, Enna, Italy,

Dr. Rafal Madonski, Jinan University, Energy Electricity Research Center, Guangzhou, China,

Dr. Milenko Andrić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia,

Dr. Samarjit Kar, National Institute of Technology, Department of Mathematics, Durgapur, India,

Dr. Rosen Mitrev, Technical University of Sofia, Sofia, Bulgaria,

Dr. Bojan Milanović, University of Defence in Belgrade, Military Academy, Belgrade, Serbia,

Dr. Irik Mukhametzyanov, Ufa State Petroleum Technological University, Ufa, Russian Federation,

Dr. Pavel Otrisal, Palacký University, Olomouc, Czech Republic,

Dr. Radovan Radovanović, University of Criminal Investigation and Police Studies, Belgrade, Serbia.

САДРЖАЈ

ОРИГИНАЛНИ НАУЧНИ РАДОВИ

<i>Иван Гутман</i>	
О тополошким индексима који зависе од степена чворова и грана.....	855-863
<i>Зоран Каделбург, Никола Фабиано, Милица Саватовић, Стојан Раденовић</i>	
Критичке напомене о „постојању решења диференцијала другог реда једначина кроз резултате фиксне тачке за нелинеарне f-контракције укључујући w_G -дистанце”	864-875
<i>Јонс Абделбади Мабрук, Башир Моктари, Тајиб Алауи</i>	
Примена фази логичког контролера типа 2 и контролера фракционог реда за регулисање брзине директног управљања моментом силе у индукционом мотору	876-897
<i>Маошенг Џенг, Ђаи Ју</i>	
Евалуација окретања челика помоћу вишекритеријумске оптимизације на бази вероватноће са одговарајућим бројем атрибута.....	898-910
<i>Мохамед Зуауи М. Лаидуни, Таки-еддине Ахмед А. Бенјахија, Бобан З. Павловић, Салем-Билал Б. Амокрне, Туати Б. Адли</i>	
Процена канала дубоког учења за 5G бежичне комуникације	911-940
<i>Туати Б. Адли, Салем-Билал Б. Амокрне, Бобан З. Павловић, Мохамед Зуауи М. Лаидуни, Таки-еддине Ахмед А. Бенјахија</i>	
Систем откривања аномалија у мрежи на бази NetFlow протокола применом машинског/дубоког учења	941-969
<i>Данијела Д. Протић, Миомир М. Станковић</i>	
Напади на сајбер безбедност: који скуп података треба користити за евалуацију система за детекцију упада?	970-995
<i>Дејан Б. Цизел, Томислав Б. Ункашевић, Зоран Ђ. Бањац</i>	
Концепт приватности података у електронском здравственом систему заснован на блокчејн технологији.....	996-1027
<i>Стефан В. Милићевић, Иван А. Благојевић</i>	
Повећање ефикасности гусеничног возила оптимизацијом преносних односа и стратегије промене степена преноса	1028-1047
<i>Сара Затар, Наср Рахал, Худа Багден, Абдулазиз Суајси, Халима Туауад, Халид Ебммахди</i>	
Експериментална анализа изложености бетона термичким променама	1048-1068
<i>Срејко Р. Стопић, Владимир Дамјановић, Радислав Филиповић, Мери Д. Камарад, Бернд Г. Фридрих</i>	
Третирање бокситних остатака – лужење (први део).....	1069-1086
<i>Иван М. Потић, Ненад М. Комазец, Љиљана М. Михајловић, Александар М. Милић, Саша Т. Баќрач</i>	
Управљање ризиком од неексплодираних убојних средстава у Републици Србији у функцији заштите животне средине – студија случаја Боровац.....	1087-1114
ПРЕГЛЕДНИ РАДОВИ	
<i>Никола Фабиано</i>	
Колективни феномени	1115-1126
<i>Ненад М. Милорадовић, Горан М. Вукадиновић</i>	
Изазови четврте индустријске револуције, трансформација савремених оружаних снага и морална дилема у вези са роботизацијом	1127-1147
<i>Влада С. Соколовић, Горан Б. Марковић</i>	
Интернет ствари у војној примени	1148-1171
<i>Срђан В. Атанасијевић, Моника Н. Захар, Дејан Д. Ранчић, Иван Б. Вулић, Татјана Ј. Атанасијевић</i>	
Омогућавање дигиталног раста кроз континуирану едукацију менаџера пројеката: оквир за колаборативно, комплементарно, одрживо и истовремено учење у организацијама за софтверско инжењерство	1172-1197
ПРИКАЗИ	
<i>Небојша Н. Гаћеша</i>	
Приказ књиге Discrete communication systems, аутор Стеван Бербер, Oxford University Press, 2021	1198-1207
САВРЕМENO HAOPУЖAЊE И BOЈHA OПPEMA	1208-1227
<i>Драган М. Вучковић</i>	
ПОЗИВ И УПУТСТВО АУТОРИМА	1228-1244

СОДЕРЖАНИЕ

ОРИГИНАЛЬНЫЕ НАУЧНЫЕ СТАТЬИ

<i>Иван Гутман</i> О топологических индексах, зависящих от степеней вершин и ребер	855-863
<i>Зоран Кадельбурге, Никола Фабиано, Милица Саватович, Стоян Раденович</i> Критические замечания о "существовании решения дифференциала второго порядка уравнение через результаты фиксированной точки для нелинейных f-сопряжений вовлечение w_0 -расстояние	864-875
<i>Юнес Абдельбади Мабрук, Башир Мохтари, Тайеб Аллауи</i> Применение контроллера нечеткой логики типа 2 и контроллера дробного порядка при регулировании скорости прямого управления крутящим моментом в асинхронном двигателе	876-897
<i>Маошенг Чжэн, Джи Йю</i> Оценка точения стали, основанная на вероятности многоцелевой оптимизации с соответствующим количеством атрибутов	898-910
<i>Мохамед Зуауи М. Лаидуни, Таки-эддине Ахмед А. Беняхия, Бобан З. Павлович, Салем-Билал Б. Амокрание, Туати Б. Адли</i> Оценка канала глубокого обучения в 5G беспроводной связи	911-940
<i>Туати Б. Адли, Салем-Билал Б. Амокрание, Бобан З. Павлович, Мохамед Зуауи М. Лаидуни, Таки-эддине Ахмед А. Беняхия</i> Аномальная система обнаружения вторжений в сеть на основе NetFlow с использованием машинного/глубокого обучения	941-969
<i>Даниела Д. Протич, Миомир М. Станкович</i> Угрозы кибербезопасности: Какой набор данных следует использовать для оценки системы обнаружения атак?	970-995
<i>Деян Б. Цизель, Томислав Б. Ункашевич, Зоран Дж. Баняц</i> Концепция конфиденциальности данных в электронной системе здравоохранения на основе технологии Блокчейн	996-1027
<i>Стефан В. Миличевич, Иван А. Благоевич</i> Повышение эффективности гусеничной машины за счет оптимизации передаточных чисел и стратегии переключения передач	1028-1047
<i>Сара Затар, Наср Рахал, Худа Багден, Абдулайзиз Суайси, Халима Туауад, Халид Ебммахди</i> Экспериментальное исследование тепловых свойств бетона	1048-1068
<i>Сречко Р. Столич, Владимир Дамянович, Радислав Филипович, Мери Д. Камарад, Бернд Г. Фридрих</i> Обработка бокситового шлама – кислотное выщелачивание (первая часть)	1069-1086
<i>Иван М. Потич, Ненад М. Комазец, Лиляна М. Михайлович, Александр М. Милич, Саша Т. Бакрач</i> Управление рисками, связанными с неразорвавшимися боеприпасами, в Республике Сербия в целях защиты окружающей среды – исследование случая Боровац	1087-1114
ОБЗОРНЫЕ СТАТЬИ	
<i>Никола Фабиано</i> Коллективные явления	1115-1126
<i>Ненад М. Милорадович, Горан М. Вукадинович</i> Вызовы четвертой промышленной революции, трансформация современных вооруженных сил и моральная дилемма, связанная с роботизацией	1127-1147
<i>Влада С. Соколович, Горан Б. Маркович</i> Интернет вещей в военном применении	1148-1171
<i>Срджан В. Атанасиевич, Моника Н. Захар, Деян Д. Ранчич, Иван Б. Вулич, Татьяна Я. Атанасиевич</i> Образование и применение водорода в металлургии цветных металлов	1172-1197
ОБЗОРЫ	
<i>Небойша Н. Гачеша</i> Обзор книги «Дискретные системы связи», Автор: Стивен Бербер, Издательство Оксфордского университета, 2021г.	1198-1207
СОВРЕМЕННОЕ ВООРУЖЕНИЕ И ВОЕННОЕ ОБОРУДОВАНИЕ	1208-1227
<i>Драган М. Вучкович</i>	
ПРИГЛАШЕНИЕ И ИНСТРУКЦИИ ДЛЯ АВТОРОВ РАБОТ	1228-1244

CONTENTS

ORIGINAL SCIENTIFIC PAPERS

<i>Ivan Gutman</i> On vertex and edge degree-based topological indices	855-863
<i>Zoran Kadelburg, Nicola Fabiano, Milica Savatović, Stojan Radenović</i> Critical remarks on "existence of the solution to second order differential equation through fixed point results for nonlinear f-contractions involving w_D -distance"	864-875
<i>Younes Abdelbadie Mabrouk, Bachir Mokhtari, Tayeb Allaoui</i> Application of the type-2 fuzzy logic controller and the fractional order controller to regulate the DTC speed in an induction motor	876-897
<i>Maosheng Zheng, Jie Yu</i> Evaluation of steel turning by means of probability – based multi - objective optimization with appropriate numbers of attributes	898-910
<i>Mohammed zouaoui M. Laidouni, Taki-eddine Ahmed A. Benyahia, Boban Z. Pavlović, Salem-Bilal B. Amokrane, Touati B. Adli</i> Deep learning channel estimation for 5G wireless communications	911-940
<i>Touati B. Adlia, Salem-Bilal B. Amokrane, Boban Z. Pavlović, Mohammad Zouaoui M. Laidouni, Taki-eddine Ahmed A. Benyahia</i> Anomaly network intrusion detection system based on NetFlow using machine/deep learning	941-969
<i>Danijela D. Protić, Miomir M. Stanković</i> Cybersecurity attacks: which dataset should be used to evaluate an intrusion detection system?	970-995
<i>Dejan B. Cizelj, Tomislav B. Unkašević, Zoran D. Banjac</i> eHealthcare system data privacy concept based on Blockchain technology	996-1027
<i>Stefan V. Milićević, Ivan A. Blagojević</i> Optimization of gear ratios and gear-shifting strategy for enhanced efficiency in tracked vehicles	1028-1047
<i>Sara Zahir, Nacer Rahal, Houda Beghdad, Abdelaziz Souici, Halima Aouad, Khaled Benmahdi</i> Experimental analysis of the thermal behavior of concrete	1048-1068
<i>Srećko R. Stopić, Vladimir Damjanović, Radislav Filipović, Mary D. Kamarad, Bernd G. Friedrich</i> Treatment of bauxite residues - acidic leaching (first part)	1069-1086
<i>Ivan M. Potić, Nenad M. Komazec, Ljiljana M. Mihajlović, Aleksandar M. Milić, Saša T. Bakrač</i> Risk management of unexploded ordnance in the Republic of Serbia for environmental protection - Borovac case study	1087-1114
REVIEW PAPERS	
<i>Nicola Fabiano</i> Collective phenomena	1115-1126
<i>Nenad M. Miloradović, Goran M. Vukadinović</i> Challenges of the Fourth Industrial Revolution (4IR), transformation of modern armed forces and the ethical dilemma of robotic automation	1127-1147
<i>Vlada S. Sokolović, Goran B. Marković</i> Internet of Things in military applications	1148-1171
<i>Srdan V. Atanasijević, Monika N. Zahar, Dejan D. Rančić, Ivan B. Vulić, Tatjana J. Atanasijević</i> Enabling digital growth through continuous education of project managers: a framework for collaborative, complementary, sustained, and simultaneous learning in software engineering organizations	1172-1197
REVIEWS	
<i>Nebojša N. Gačeša</i> Review of the book entitled Discrete Communication Systems by Stevan Berber, Oxford University Press, 2021	1198-1207
MODERN WEAPONS AND MILITARY EQUIPMENT	1208-1227
<i>Dragan M. Vučković</i>	
CALL FOR PAPERS AND INSTRUCTIONS FOR AUTHORS	1228-1244

On vertex and edge degree-based topological indices

Ivan Gutman

University of Kragujevac, Faculty of Science,
Kragujevac, Republic of Serbia,
e-mail: gutman@kg.ac.rs,
ORCID iD: <https://orcid.org/0000-0001-9681-1550>

DOI: 10.5937/vojtahg71-45971; <https://doi.org/10.5937/vojtahg71-45971>

FIELD: mathematics (mathematics subject classification: primary 05C07,
secondary 05C09)

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: The entire topological indices (TI_{ent}) are a class of graph invariants depending on the degrees of vertices and edges. Some general properties of these invariants are established.

Methods: Combinatorial graph theory is applied.

Results: A new general expression for TI_{ent} is obtained. For triangle-free and quadrangle-free graphs, this expression can be significantly simplified.

Conclusion: The paper contributes to the theory of vertex and edge degree-based graph invariants.

Key words: entire topological index, vertex and edge degree-based graph invariant, degree (of vertex), degree (of edge).

Introduction

In this paper, we are concerned with connected simple graphs. Let G be such a graph, and let $V = V(G)$ and $E = E(G)$ be its vertex and edge sets, respectively. The graph G has $|V(G)| = n$ vertices and $|E(G)| = m$ edges. Two vertices u, v of the graph are said to be adjacent, denoted as $u \sim v$, if u and v are the endpoints of an edge. The respective edge will then be denoted by uv . A vertex u and an edge e are said to be incident, denoted as $u \sim e$, if u is an endpoint of the edge e . Two edges e, f are said to be incident, denoted as $e \sim f$, if the edges e and f have a common vertex as the endpoint.



The degree of a vertex $u \in \mathbf{V}(G)$, denoted as d_u , is the number of vertices of G that are adjacent to u . The degree of an edge $e \in \mathbf{E}(G)$, denoted by d_e , is the number of edges of G that are incident to e . If the endpoints of the edge e are the vertices u and v , then it is easy to see that $d_e = d_u + d_v - 2$.

A graph is said to be regular of degree r if $d_u = r$ holds for all $u \in \mathbf{V}(G)$. A regular graph of degree r with n vertices, has $m = \frac{1}{2}nr$ edges.

The distance between two vertices $u, v \in \mathbf{V}(G)$ (= length of the shortest path connecting u and v) is denoted by $d(u, v)$. If u and v are adjacent, then $d(u, v) = 1$.

For additional details of graph theory, see (Harary, 1969; Bondy & Murty, 1976).

In contemporary graph theory, especially in network theory and chemical graph theory, a large number of invariants of the form

$$TI = TI(G) = \sum_{\substack{x, y \in \mathbf{V}(G) \\ x \sim y}} F(d_x, d_y) \quad (1)$$

are being considered. They are usually referred to as “vertex-degree-based topological indices”. In formula (1), the summation goes over all pairs of adjacent vertices of the underlying graph G , i.e., over the pairs of vertices at the unit distance, $d(x, y) = 1$. F stands for a real-valued function with the property $F(x, y) = F(y, x)$ and $F(x, y) \geq 0$ for all values of the variables x and y that the vertex degrees of the graph G may assume. Some best known and most studied invariants of this kind are the first Zagreb index ($F = x + y$), the second Zagreb index ($F = xy$), the Randić index ($F = 1/\sqrt{xy}$), the forgotten index ($F = x^2 + y^2$), the atom-bond-connectivity index ($F = \sqrt{(x + y - 2)/(xy)}$), and the Sombor index ($F = \sqrt{x^2 + y^2}$). For details see (Todeschini & Consonni, 2000; Gutman, 2023).

Motivated by the success of both the mathematical theory and (mainly chemical) applications of the vertex-degree-based indices of type (1), their modified version

$$TI_{ve} = TI_{ve}(G) = \sum_{\substack{x \in \mathbf{V}(G), e \in \mathbf{E}(G) \\ x \sim e}} F(d_x, d_e) \quad (2)$$

was put forward, first for $F = x + y$ and $F = xy$ (Kulli, 2016), and recently also for $F = \sqrt{x^2 + y^2}$ (Kulli, 2022; Kulli & Gutman, 2022). The latter graph invariant is now called the KG-Sombor index, and is denoted

by $KG = KG(G)$ (Kulli & Gutman, 2022; Kulli et al., 2022; Kosari et al., 2023; Madhumitha et al., 2024). In the case of the KG-Sombor index, it has been shown (Kulli et al., 2022; Kulli & Gutman, 2022) that

$$KG(G) = \sum_{\substack{x,y \in V(G) \\ x \sim y}} \left[\sqrt{d_x^2 + (d_x + d_y - 2)^2} + \sqrt{d_y^2 + (d_x + d_y - 2)^2} \right].$$

It is straightforward to state the generalization of the above formula:

Theorem 1. *Let G be a simple graph. Then the invariant TI_{ve} , Eq. (2), can be expressed solely in terms of the vertex degrees of G , and satisfies the relation*

$$TI_{ve}(G) = \sum_{\substack{x,y \in V(G) \\ x \sim y}} \left[F(d_x, d_x + d_y - 2) + F(d_y, d_x + d_y - 2) \right]. \quad (3)$$

Proof. The edge e in formula (2) has two endpoints, say x and y . Bearing this in mind, the summation in (2), for any particular edge e , must go over both x and y . This results in the two terms on the right-hand side of (3). Formula (3) follows now by taking into account that $d_e = d_x + d_y - 2$ for any edge $e = xy$. \square

Entire topological indices

Short time after the vertex- and edge-degree-based graph invariants of the type (2) were conceived (Kulli, 2016), the “entire” topological indices were put forward (Alwardi et al., 2018), first for the choices $F = x + y$ (first Zagreb index) and $F = xy$ (second Zagreb index). Eventually, entire indices were considered for the forgotten index ($F = x^2 + y^2$), (Bharali et al., 2020), the Randić index ($F = 1/\sqrt{xy}$), (Saleh & Cangul, 2021), and quite recently for the Sombor index ($F = \sqrt{x^2 + y^2}$), (Movahedi & Akhbari, 2023).

The general form of these indices is

$$TI_{ent} = TI_{ent}(G) = \sum_{\substack{x,y \in V(G) \cup E(G) \\ x \sim y}} F(d_x, d_y). \quad (4)$$

Before stating Theorem 2, we recall some basic facts on line graphs (Harary, 1969; Bondy & Murty, 1976).



The line graph $L(G)$ of the graph G is defined so that its vertex set is $\mathbf{E}(G)$, and two vertices of $L(G)$ are adjacent if the respective edges of G are incident. Thus the line graph of the graph G has $|\mathbf{E}(G)| = m$ vertices and $m(L(G)) = \sum_{u \in \mathbf{V}(G)} \binom{d_u}{2}$ edges.

Theorem 2. *Let G be a simple graph and let $L(G)$ be its line graph. Then the invariant TI_{ent} , Eq. (4), can be expressed solely in terms of the vertex degrees of G and $L(G)$, and satisfies the relation*

$$TI_{ent} = TI_{ent}(G) = \sum_{\substack{x, y \in \mathbf{V}(G) \\ x \sim y}} \left[F(d_x, d_y) + F(d_x, d_x + d_y - 2) + F(d_y, d_x + d_y - 2) \right] + \sum_{\substack{x, y \in \mathbf{V}(L(G)) \\ x \sim y}} F(d_x, d_y). \quad (5)$$

Proof. It is evident that the summation on the right-hand side of (4) can be divided into three parts, namely for

- (a) $x \in \mathbf{V}(G)$ and $y \in \mathbf{V}(G)$
- (b) $x \in \mathbf{V}(G)$ and $y \in \mathbf{E}(G)$ or vice versa;
- (c) $x \in \mathbf{E}(G)$ and $y \in \mathbf{E}(G)$

In view of Eq. (1), the component of TI_{ent} pertaining to (a) is equal to TI , i.e.,

$$\sum_{\substack{x, y \in \mathbf{V}(G) \\ x \sim y}} F(d_x, d_y) \quad (6)$$

whereas by Eqs. (2) and (3), the component pertaining to (b) is equal to TI_{ve} , i.e.,

$$\sum_{\substack{x, y \in \mathbf{V}(G) \\ x \sim y}} \left[F(d_x, d_x + d_y - 2) + F(d_y, d_x + d_y - 2) \right]. \quad (7)$$

The component of TI_{ent} , corresponding to the choice of pairs of incident edges, namely (c), is equal to the TI -index of the line graph of the graph G :

$$\sum_{\substack{x, y \in \mathbf{V}(L(G)) \\ x \sim y}} F(d_x, d_y) \quad (8)$$

Combining (6)–(8), we arrive at

$$TI_{ent}(G) = TI(G) + TI_{ve}(G) + TI(L(G))$$

from which Eq. (5) directly follows. \square

Special cases of expressions (6) and (8) were recognized by the authors of the earlier papers on entire topological indices (Alwardi et al., 2018; Bhargali et al., 2020; Saleh & Cangul, 2021; Movahedi & Akhbari, 2023), but no one of them was aware of formula (7).

Theorem 2, and in particular formula (7), are stated here for the first time.

Corollary 1. *If G is a regular graph of the degree r , with n vertices and m edges, then*

$$TI_{ent}(G) = \frac{1}{2}nr [F(r, r) + 2F(r, 2r - 2) + (r - 1)F(2r - 2, 2r - 2)].$$

Proof. In formula (5), all vertex degrees of G are equal to r , whereas all vertex degrees of $L(G)$ are equal to $2r - 2$. The first summation in (5) goes over $m = \frac{1}{2}nr$ terms, whereas the second summation goes over $m(L(G)) = \frac{1}{2}nr(r - 1)$ terms. \square

In the case of triangle-free and quadrangle-free graphs (such are the trees, hexagonal systems, fullerene graphs, nanotubes, etc.), formula (5) can be simplified. Namely, the entire topological indices TI_{ent} of triangle-free and quadrangle-free graphs can be expressed in terms of vertex degrees of the underlying graph G , without any reference to its line graph $L(G)$.

Corollary 2. *If G is a triangle-free and quadrangle-free graph, then Eq. (9) holds:*

$$\begin{aligned} TI_{ent} = TI_{ent}(G) &= \sum_{\substack{x, y \in \mathbf{V}(G) \\ x \sim y}} \left[F(d_x, d_y) + F(d_x, d_x + d_y - 2) + \right. \\ &+ \left. F(d_y, d_x + d_y - 2) \right] + \\ &+ \sum_{\substack{u, v \in \mathbf{V}(G) \\ d(u, v) = 2}} F(d_u + d_w - 2, d_v + d_w - 2) \end{aligned} \quad (9)$$

where w is the (unique) vertex lying between the vertices u and v .

Proof. If the graph G does not contain triangles and quadrangles, then two vertices at distance 2, say u and v , have a unique vertex between them, say w . Then uw and vw form a pair of incident edges, resulting in

$$\sum_{\substack{x, y \in V(L(G)) \\ x \sim y}} F(d_x, d_y) = \sum_{\substack{u, v \in V((G)) \\ d(u, v) = 2}} F(d_u + d_w - 2, d_v + d_w - 2). \quad (10)$$

Substituting (10) back into (5) yields (9). \square

References

- Alwardi, A., Alqesmah, A., Rangarajan, R. & Cangul, I.N. 2018. Entire Zagreb indices of graphs. *Discrete Mathematics, Algorithms and Applications*, 10(03), p. 1850037. Available at: <https://doi.org/10.1142/S1793830918500374>.
- Bharali, A., Doley, A. & Buragohain, J. 2020. Entire forgotten topological index of graphs. *Proyecciones (Antofagasta)*, 39(4), pp. 1019–1032. Available at: <https://doi.org/10.22199/issn.0717-6279-2020-04-0064>.
- Bondy, J.A. & Murty, U.S.R. 1976. *Graph theory with applications*. Macmillan Press. ISBN: 0-444-19451-7.
- Gutman, I. 2023. On the spectral radius of VDB graph matrices. *Vojnotehnički glasnik/Military Technical Courier*, 71(1), pp. 1–8. Available at: <https://doi.org/10.5937/vojtehg71-41411>.
- Harary, F. 1969. *Graph Theory*. Boca Raton: CRC Press. ISBN: 9780429493768.
- Kosari, S., Dehgardi, N. & Khan, A. 2023. Lower bound on the KG-Sombor index. *Communications in Combinatorics and Optimization*, 8(4), pp. 751–757. Available at: <https://doi.org/10.22049/CCO.2023.28666.1662>.
- Kulli, V.R. 2016. On K Banhatti indices of graphs. *Journal of Computer and Mathematical Sciences*, 7(4), pp. 213–218. ISSN 0976-5727 (Print), ISSN 2319-8133 (Online).
- Kulli, V.R. 2022. KG Sombor indices of certain chemical drugs. *International Journal of Engineering Sciences & Research Technology*, 11(6), pp. 27–35 [online]. Available at: <https://www.ijesrt.com/index.php/J-ijesrt/article/view/48> [Accessed: 10 August 2023].
- Kulli, V.R. & Gutman, I. 2022. Sombor and KG-Sombor Indices of Benzenoid Systems and Phenylenes. *Annals of Pure and Applied Mathematics*, 26(2), pp. 49–53. Available at: <https://doi.org/10.22457/apam.v26n2a01883>.
- Kulli, V.R., Harish, N., Chaluvvaraju, B. & Gutman, I. 2022. Mathematical properties of KG Sombor index. *Bulletin of International Mathematical Virtual Institute*, 12(2), pp. 379–386[online]. Available at: http://www.imvibl.org/buletin/bulletin_imvi_12_2_22/bulletin_imvi_12_2_22_379_386.pdf [Accessed: 10 August 2023].

Madhumitha, K., D'Souza, S. & Nayak, S. 2024. KG Sombor energy of graphs with self loops. *Communications in Combinatorics and Optimization*. in press.

Movahedi, F. & Akhbari, M.H. 2023. Entire Sombor index of graphs. *Iranian Journal of Mathematical Chemistry*, 14(1), pp. 33–45. Available at: <https://doi.org/10.22052/IJMC.2022.248350.1663>.

Saleh, A. & Cangul, I.N. 2021. On the entire Randic index of graphs. *Advances and Applications in Mathematical Sciences*, 20(8), pp. 1559–1569 [online]. Available at: https://www.mililink.com/upload/article/1367760163aams_vol_208_june_2021_a_20_p1559-1569_a_saleh_and_i_n_canguli.pdf [Accessed: 10 August 2023].

Todeschini, R. & Consonni, V. 2000. *Handbook of molecular descriptors*. Weinheim: Wiley–VCH. ISBN: 3-52-29913-0.

О топологических индексах, зависящих от степеней вершин и ребер

Иван Гутман

Крагуевацкий университет, естественно-математический факультет, г. Крагуевац, Республика Сербия

РУБРИКА ГРНТИ: 27.29.19 Краевые задачи и задачи на собственные значения для обыкновенных дифференциальных уравнений и систем уравнений

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Все топологические индексы (TI_{ent}) представляют собой класс инвариантов графа, зависящих от степеней расположения вершин и ребер. Установлены некоторые общие свойства этих инвариантов.

Методы: В данной статье применяется комбинаторная теория графов.

Результаты: Получено новое обобщенное выражение для TI_{ent} . Для графов без треугольников и четырехугольников это выражение может быть значительно упрощено.

Выводы: Данная статья вносит вклад в теорию инвариантов графов, зависящих от степеней вершин и ребер.

Ключевые слова: полный топологический индекс, инварианты графов, зависящих от степеней вершин и ребер, степень (вершины), степень (ребра).

О тополошким индексима који зависе од степена чворова и грана

Иван Гутман

Универзитет у Крагујевцу, Природно-математички факултет,
Крагујевац, Република Србија

ОБЛАСТ: математика

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Потпуни тополошки индекси (TI_{ent}) образују класу графовских инваријанти који зависе од степена чворова и степена грана. Установљене су неке опште особине ових инваријанти.

Метод: Примењивани су поступци комбинаторне теорије графова.

Резултати: Нађена је нова општа формула за TI_{ent} . За графове без троуглова и четвороуглова ова формула се значајно поједностављује.

Закључак: Рад доприноси теорији графовских инваријанти који зависе од степена чворова и степена грана.

Кључне речи: потпуни тополошки индекси, графовске инваријанте које зависе од степена чворова и грана, степен (чвора), степен (гране).

EDITORIAL NOTE: The author of this article, Ivan Gutman, is a current member of the Editorial Board of the Military Technical Courier. Therefore, the Editorial Team has ensured that the double blind reviewing process was even more transparent and more rigorous. The Team made additional effort to maintain the integrity of the review and to minimize any bias by having another associate editor handle the review procedure independently of the editor – author in a completely transparent process. The Editorial Team has taken special care that the referee did not recognize the author's identity, thus avoiding the conflict of interest.

КОММЕНТАРИЈ РЕДКОЛЛЕГИИ: Автор данной статьи Иван Гутман является действующим членом редколлегии журнала «Военно-технический вестник». Поэтому редколлегия провела более открытое и более строгое двойное слепое рецензирование. Редколлегия приложила дополнительные усилия для того чтобы сохранить целостность рецензирования и свести к минимуму предвзятость, вследствие чего второй редактор-сотрудник управлял процессом рецензирования независимо от редактора-автора, таким образом процесс рецензирования был абсолютно прозрачным. Редколлегия во избежание конфликта интересов позаботилась о том, чтобы рецензент не узнал кто является автором статьи.

РЕДАКЦИЈСКИ КОМЕНТАР: Аутор овог чланка Иван Гутман је актуелни члан Уређивачког одбора Војнотехничког гласника. Због тога је уредништво спровело транспарентнији и ригорознији двоструко слепи процес рецензије. Уложило је додатни напор да одржи интегритет рецензије и необјективност сведе на најмању могућу меру тако што је други уредник сарадник водио процедуру рецензије независно од уредника аутора, при чему је тај процес био апсолутно транспарентан. Уредништво је посебно водило рачуна да рецензент не препозна ко је написао рад и да не дође до конфликта интереса.

Paper received on / Дата получения работы / Датум пријема чланка: 14.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.11.2023.

Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 23.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.spb>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.spb>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.spb>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).





Critical remarks on “Existence of the solution to second order differential equation through fixed point results for nonlinear F -contractions involving w_0 -distance”

Zoran Kadelburg^a, Nicola Fabiano^b,
Milica Savatović^c, Stojan Radenović^d

^a University of Belgrade, Faculty of Mathematics,
Belgrade, Republic of Serbia,
e-mail: kadelbur@matf.bg.ac.rs,

ORCID iD: <https://orcid.org/0000-0001-9103-713X>

^b University of Belgrade, “Vinča” Institute of Nuclear Sciences - National
Institute of the Republic of Serbia, Belgrade, Republic of Serbia,

e-mail: nicola.fabiano@gmail.com, **corresponding author**

ORCID iD: <https://orcid.org/0000-0003-1645-2071>

^c University of Belgrade, School of Electrical Engineering,
Belgrade, Republic of Serbia,

e-mail: milica.makragic@etf.rs,

ORCID iD: <https://orcid.org/0000-0003-0439-1451>

^d University of Belgrade, Faculty of Mechanical Engineering,
Belgrade, Republic of Serbia,

e-mail: radens@beotel.rs,

ORCID iD: <https://orcid.org/0000-0001-8254-6688>

DOI: 10.5937/vojtehg71-46505; <https://doi.org/10.5937/vojtehg71-46505>

FIELD: mathematics

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: In this paper, several critical remarks are presented concerning the paper of Iqbal & Rizwan: Existence of the solution to second order differential equation through fixed point results for nonlinear F -contractions involving w_0 -distance from 2020.

Methods: Conventional theoretical methods of functional analysis.

Results: It is shown that their use of the non-decreasing “control” function F instead of a strictly increasing one in Wardowski-type results usually produces contradictions.

Conclusion: It is shown that such results can be obtained in a more general class of metric-like spaces, where strict monotonicity is the only as-

ACKNOWLEDGMENT: The research of Milica Savatović was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia, Project No 174032.

sumption that has to be imposed on the function F . An example is presented showing that the obtained results are stronger than the classic ones.

Key words: F -contraction, fixed point, metric-like space, strictly increasing function.

Introduction and preliminaries

D. Wardowski’s result from (Wardowski, 2012) can be considered as one of the significant generalizations of S. Banach’s basic result from 1922. In this generalization, Wardowski used a function $F : (0, +\infty) \rightarrow \mathbb{R}$ satisfying the following three properties:

- (F1) F is strictly increasing, i.e., $t_1 < t_2$ implies $F(t_1) < F(t_2)$;
- (F2) for any sequence $\{a_n\} \subset (0, +\infty)$, $\lim_{n \rightarrow +\infty} a_n = 0$ if and only if $\lim_{n \rightarrow +\infty} F(a_n) = -\infty$ (i.e., $\lim_{t \rightarrow 0^+} F(t) = -\infty$);
- (F3) there exists $k \in (0, 1)$ such that $\lim_{t \rightarrow 0^+} t^k F(t) = 0$.

He proved that a self-map T on a complete metric space (X, d) has a unique fixed point if there exists a positive number τ and a function F satisfying the previously mentioned conditions, such that, for all $x, y \in X$ with $Tx \neq Ty$,

$$\tau + F(d(Tx, Ty)) \leq F(d(x, y)) \tag{1}$$

holds.

Later on, in another work (Wardowski, 2018), he generalized the mentioned result, replacing the condition (1) by the following one

$$\varphi(d(x, y)) + F(d(Tx, Ty)) \leq F(d(x, y)), \tag{2}$$

where φ is some function from $(0, +\infty)$ to itself satisfying $\liminf_{s \rightarrow t^+} \varphi(s) > 0$ for each $t \geq 0$ (he called such mappings (φ, F) -contractions).

In a multitude of subsequent papers, dozens of authors used Wardowski’s approach for mappings acting in various spaces (such as b -metric spaces, partial metric spaces, metric-like spaces, cone metric spaces, G -metric spaces, rectangular metric spaces, as well as in spaces endowed with a w -distance) – a review of these results until 2022 can be found in (Fabiano et al, 2022). We recall here the definitions of w -distance p of O. Kada, T. Suzuki and W. Takahashi and metric-like μ of A. Amini-Harandi.

Definition 1. (Kada et al, 1996) Let (X, d) be a metric space and let a mapping $p : X \times X \rightarrow [0, +\infty)$ satisfy:



(p1) $p(x, z) \leq p(x, y) + p(y, z)$ for all $x, y, z \in X$;

(p2) for any $x \in X$, the function $p(x, \cdot) : X \rightarrow [0, +\infty)$ is d -lower semi-continuous;

(p3) for any $\varepsilon > 0$, there exists $\delta > 0$ such that $p(z, x) < \delta$ and $p(z, y) < \delta$ imply $d(x, y) < \varepsilon$.

Then, p is called a w -distance on X .

Definition 2. (Amini-Harandi, 2012) A metric-like on a nonempty set X is a function $\mu : X \times X \rightarrow [0, +\infty)$ if the following conditions hold for all $x, y, z \in X$:

($\mu 1$) $\mu(x, y) = 0$ implies $x = y$;

($\mu 2$) $\mu(x, y) = \mu(y, x)$;

($\mu 3$) $\mu(x, y) \leq \mu(x, z) + \mu(z, y)$.

Then (X, μ) is called a metric-like space.

Note that, see, e.g. (Iqbal & Rizwan, 2020) or (Kadelburg & Radenović, 2024), for a w -distance p on a set X , the mapping

$$\mu(x, y) = \max\{p(x, y), p(y, x)\}$$

is a metric-like on X .

The notions of convergent and Cauchy sequences, and continuous functions, were introduced in metric-like spaces as follows.

Definition 3. (Amini-Harandi, 2012) Let (X, d) be a metric-like space and $\{x_n\}$ be a sequence in X .

1. The sequence $\{x_n\}$ is said to converge to $x \in X$ if $\lim_{n \rightarrow +\infty} d(x, x_n) = d(x, x)$.
2. $\{x_n\}$ is a Cauchy sequence if $\lim_{m, n \rightarrow +\infty} d(x_m, x_n)$ exists and is finite.
3. The space (X, d) is said to be complete if every Cauchy sequence $\{x_n\}$ in X converges to some $x \in X$ such that $\lim_{m, n \rightarrow +\infty} d(x_m, x_n) = d(x, x) = \lim_{n \rightarrow +\infty} d(x_n, x)$.
4. A mapping $T : X \rightarrow X$ is continuous at a point $x \in X$ if $\lim_{n \rightarrow +\infty} x_n = x$ implies $\lim_{n \rightarrow +\infty} Tx_n = Tx$.

On the other hand, some authors considered different conditions on the "control" function F , culminating in O. Popescu's and G. Stan's proof, see

(Popescu & Stan, 2020), Theorem 5, that in fact just condition (F1) is sufficient for obtaining the basic result from (Wardowski, 2012), see also (Fabiano et al, 2022), Theorem 2.3 and Remark 2.4.

It is natural to ask whether the property (F1) of the function F can be replaced by a weaker property that F is non-decreasing, but not strictly increasing. Of course, there are a lot of such functions.

In the recent paper (Iqbal & Rizwan, 2020), the authors tried to generalize the results of papers (Wardowski, 2012) and (Wardowski, 2018) in two ways – firstly, instead of metric d they used w -distance p or metric-like μ . On the other hand, instead of the assumption (F1), the authors of (Iqbal & Rizwan, 2020) used the weaker assumption

(F1') the function F is non-decreasing on $(0, +\infty)$, i.e. $t_1 \leq t_2$ implies $F(t_1) \leq F(t_2)$,

together with the assumptions (F2) and (F3).

Unfortunately, all their results obtained under the assumption (F1') may be incompatible with a Wardowski-type contractive condition. To show that, the following observation can be useful.

LEMMA 4. If $F : (0, +\infty) \rightarrow \mathbb{R}$ is a non-decreasing, but not strictly increasing function, then there exists an interval $(a, b) \subset (0, +\infty)$ such that the restriction of F to this interval is constant.

Proof. Since F is non-decreasing but not strictly increasing, then there are $a, b \in (0, +\infty)$ such that $a < b$ and $F(a) = F(b)$. But then F is a constant function on (a, b) . \square

Now, it is easy to construct examples like the following one.

EXAMPLE. Consider $X = [0, +\infty)$ with the standard metric $d(x, y) = |x - y|$ and the mapping $T : X \rightarrow X$ given by $Tx = \frac{3}{4}x$. The function

$$F(t) = \begin{cases} \log t, & 0 < t < 1, \\ 0, & 1 \leq t \leq 2, \\ \log(t - 1), & t > 2, \end{cases}$$

satisfies conditions (F1'), (F2) and (F3) (but not (F1)!). However, if $\frac{4}{3} \leq |x - y| \leq 2$, then the condition (1) reduces to $\tau + 0 \leq 0$, i.e., $\tau \leq 0$, which is incompatible with the basic assumption $\tau > 0$.

One possible additional assumption when we use the function F satisfying just the condition (F1') could be that

$$\{d(x, y) : x, y \in X\} \cap \left(\bigcup_C I_C\right) = \emptyset,$$

where I_C is the interval (a, b) such that $F(t) = C$ for each $t \in (a, b)$.

In order to improve and generalize the results from (Iqbal & Rizwan, 2020), we first state the following two known lemmas that are of interest in themselves and can be used in proving the Cauchyness of a Picard sequence $\{x_n\} = \{T^n x_0\}$ in both metric and metric-like spaces, see some references on these lemmas in (Fabiano et al, 2022).

LEMMA 5. Let (X, d) be a metric-like space and $\{x_n\}$ be a Picard sequence in it. If

$$d(x_{n+1}, x_n) < d(x_n, x_{n-1}),$$

for all $n \in \mathbb{N}$, then $x_n \neq x_m$ whenever $n \neq m$.

LEMMA 6. Let (X, d) be a metric-like space and $\{x_n\}$ be a sequence in X such that $\{d(x_{n+1}, x_n)\}$ is a non-increasing sequence and that $\lim_{n \rightarrow +\infty} d(x_{n+1}, x_n) = 0$. If $\{x_n\}$ is not a Cauchy sequence, then for some $\varepsilon > 0$ there exist two sequences $\{m_k\}$ and $\{n_k\}$ of positive integers with $n_k > m_k > k$, such that the following sequences tend to ε^+ as $k \rightarrow +\infty$:

$$\begin{aligned} & d(x_{2m_k}, x_{2n_k}), \quad d(x_{2m_k}, x_{2n_k-1}), \quad d(x_{2m_k+1}, x_{2n_k}), \\ & d(x_{2m_k-1}, x_{2n_k+1}), \quad d(x_{2m_k+1}, x_{2n_k+1}), \quad \dots \end{aligned}$$

REMARK 7. Lemma 6 is true without the hypothesis that the sequence $\{d(x_{n+1}, x_n)\}$ is non-increasing. In that case one can get that the following sequences tend to ε^+ as $k \rightarrow +\infty$:

$$\begin{aligned} & d(x_{m_k}, x_{n_k}), \quad d(x_{m_k}, x_{n_k-1}), \quad d(x_{m_k+1}, x_{n_k}), \\ & d(x_{m_k-1}, x_{n_k+1}), \quad d(x_{m_k+1}, x_{n_k+1}), \quad \dots \end{aligned}$$

In this paper, besides already mentioned problems with using non-decreasing functions in Wardowski-type results, we show how generalizations of such results can be derived in the framework of metric-like spaces, using just strict monotonicity of the "control" function F . Modifying the original Wardowski's example, we show that the obtained results are stronger than Banach-type ones.

Results

In this part of the work, φ will be a function that maps $(0, +\infty)$ to itself and for which $\liminf_{s \rightarrow t^+} \varphi(s) > 0$ is fulfilled for each $t \geq 0$, while F will be a strictly increasing function that maps $(0, +\infty)$ to \mathbb{R} . We aim to generalize and improve all three results from (Iqbal & Rizwan, 2020) by replacing the metric d and the w -distance w with a metric-like μ . Concerning the function F , just its strict monotonicity will be assumed. This will also extend D. Wardowski's result from (Wardowski, 2018).

THEOREM 8. Let (X, μ) be a complete metric-like space and $T : X \rightarrow X$. If φ and F are functions with the properties stated above, and such that, for all $x, y \in X$,

$$x \neq y \text{ and } \mu(Tx, Ty) > 0 \text{ implies } \varphi(\mu(x, y)) + F(\mu(Tx, Ty)) \leq F(\mu(x, y)), \quad (3)$$

then T has a unique fixed point in X .

Proof. We first prove the uniqueness of a possible fixed point. Indeed, if x and y be two distinct fixed points of the mapping T , then both conditions would be met and still it would hold that $\varphi(\mu(x, y)) + F(\mu(x, y)) \leq F(\mu(x, y))$, which is a contradiction with $\varphi(\mu(x, y)) > 0$.

Similar as in the case of metric spaces, the continuity of mapping T follows from the contractive condition (2); however, due to the definition of limits in metric-like spaces (see Definition 3), the proof is a bit different. Namely, we have to prove that, for every sequence $\{x_n\}$ in X , $\mu(x_n, x) \rightarrow \mu(x, x) = 0$ as $n \rightarrow +\infty$ implies that $\mu(Tx_n, Tx) \rightarrow 0$ as $n \rightarrow +\infty$.

But it follows from the contractive condition (2) that $\mu(Tx_n, Tx) \leq \mu(x_n, x)$, implying that $\mu(Tx_n, Tx) \rightarrow 0$ as $n \rightarrow +\infty$. It remains to prove that $\mu(Tx_n, Tx) \rightarrow \mu(Tx, Tx)$, which will follow if we show that $\mu(Tx, Tx) = 0$. However, $\mu(Tx, Tx) \leq 2\mu(Tx, Tx_n)$ according to the triangle relation. Thus, we have proved that the continuity follows from the contractive condition.

In order to prove the existence of at least one fixed mapping point of T , starting from an arbitrary point $x_0 \in X$, form the corresponding Picard sequence $\{x_n\}$. If, for some k , $x_k = x_{k-1}$ holds, then according to the first part of the proof, x_{k-1} is a unique fixed point of T . Hence, assume that $x_n \neq x_{n-1}$ for each $n \in \mathbb{N}$. Then, putting $x = x_{n-1}$ and $y = x_n$ into the contractive condition (3), it directly follows that the sequence $\mu(x_n, x_{n+1})$

is non-increasing and so it has a limit as $n \rightarrow +\infty$. If we denote it by μ^* , using the property of strict monotonicity of the function F , we get a contradiction with $\varphi(\mu^*) > 0$. Then, according to Lemma 5, assuming that the constructed sequence $\{x_n\}$ is not a Cauchy sequence, the conditions for applying of Lemma 6 are fulfilled. Namely, by putting $x = x_{n_k}$, $y = x_{m_k}$ we get

$$\varphi(\mu(x_{n_k}, x_{m_k})) + F(\mu(x_{n_{k+1}}, x_{m_{k+1}})) \leq F(\mu(x_{n_k}, x_{m_k})).$$

Passing to the limit as $k \rightarrow +\infty$, we get a contradiction with $\liminf_{s \rightarrow t^+} \varphi(s) > 0$.

Since $\{x_n\}$ is a Cauchy sequence in the complete metric-like space (X, μ) , then there exists a (unique) point $x^* \in X$ such that

$$\lim_{m, n \rightarrow +\infty} \mu(x_n, x_m) = \lim_{n \rightarrow +\infty} \mu(x_n, x^*) = \mu(x^*, x^*) = 0.$$

Since T is continuous, $Tx^* = x^*$ holds. □

We now state several consequences of our Theorem 8.

Putting $\varphi(t) = \tau$ for each $t > 0$ in the contractive condition (3) of Theorem 8, where τ is a positive constant, we get the main result of D. Wardowski from (Wardowski, 2012), but in the framework of metric-like spaces and with a weaker assumption on the function F :

COROLLARY 9. Let (X, μ) be a complete metric-like space and $T : X \rightarrow X$. If $F : (0, +\infty) \rightarrow \mathbb{R}$ is a strictly increasing function, such that, for all $x, y \in X$,

$$x \neq y \text{ and } \mu(Tx, Ty) > 0 \text{ implies } \tau + F(\mu(Tx, Ty)) \leq F(\mu(x, y)),$$

then T has a unique fixed point in X .

The following example (which is adapted from (Wardowski, 2012), Example 2.5) shows that our Corollary 9 is stronger than the Banach-type fixed point result in metric-like spaces.

EXAMPLE. Consider the set $X = \{S_n : n \in \mathbb{N}\}$, where $S_n = \frac{n(n+1)}{2}$, and let $\mu(x, y) = \max\{x, y\}$ for $x, y \in X$. Then, (X, μ) is a complete metric-like space (of course, it is not a metric space). Let a mapping $T : X \rightarrow X$ be given by $TS_1 = S_1$ and $TS_n = S_{n-1}$ for $n > 1$.

We show first that T is not a Banach-type contraction in (X, μ) . Indeed, it is

$$\begin{aligned} \lim_{n \rightarrow +\infty} \frac{\mu(TS_n, TS_1)}{\mu(S_n, S_1)} &= \lim_{n \rightarrow +\infty} \frac{\max\{S_{n-1}, 1\}}{\max\{S_n, 1\}} = \lim_{n \rightarrow +\infty} \frac{S_{n-1}}{S_n} \\ &= \lim_{n \rightarrow +\infty} \frac{\frac{1}{2}(n-1)n}{\frac{1}{2}n(n+1)} = 1, \end{aligned}$$

which means that $\mu(TS_n, TS_1) \leq \lambda \mu(S_n, S_1)$ cannot hold for any $\lambda < 1$ and all $n \in \mathbb{N}$.

Now, we show that the contractive condition of Corollary 9 holds if we take $F(t) = t + \log t$ and $\tau = 1$. In this case, this condition can be rewritten as

$$\frac{\mu(Tx, Ty)}{\mu(x, y)} e^{\mu(Tx, Ty) - \mu(x, y)} \leq e^{-1},$$

for all $x, y \in X$ with $x \neq y$ and $\mu(Tx, Ty) > 0$, i.e., in our example, as

$$\frac{\max\{TS_m, TS_n\}}{\max\{S_m, S_n\}} e^{\max\{TS_m, TS_n\} - \max\{S_m, S_n\}} < e^{-1}.$$

Note that $TS_m \neq TS_n$ holds (for $m > n$) if and only if one of the following holds: 1° $m > 2, n = 1$ or 2° $m > n > 1$. Consider separately these two cases.

1° In this case we have

$$\frac{\max\{TS_m, TS_1\}}{\max\{S_m, S_1\}} e^{\max\{TS_m, TS_1\} - \max\{S_m, S_1\}} = \frac{S_{m-1}}{S_m} e^{S_{m-1} - S_m} < e^{-m} < e^{-1}.$$

2° Similarly, in this case it is

$$\frac{\max\{TS_m, TS_n\}}{\max\{S_m, S_n\}} e^{\max\{TS_m, TS_n\} - \max\{S_m, S_n\}} = \frac{S_{m-1}}{S_m} e^{S_{m-1} - S_m} < e^{-m} < e^{-1}.$$

Hence, all conditions of Corollary 9 are fulfilled and the conclusion follows.

REMARK 10. Since every partial metric space, in the sense of (Matthews, 1994), is also a metric-like space, Theorem 8 and Corollary 9 are also true in the class of partial metric spaces.

REMARK 11. Since convergence, Cauchyness, completeness and continuity are defined in the same way for all following classes of spaces: partial,



metric-like, partial b-metric (Shukla, 2014) and b-metric-like spaces (Alghamdi et al, 2013), then Theorem 8 can most likely be formulated and proved for all these classes of spaces, including the most general one—b-metric like spaces.

REMARK 12. Just like Theorem 2.1, the other two Theorems 2.2 and 2.3 from (Iqbal & Rizwan, 2020) can be formulated and proved within the class of metric-like spaces. And then only *strict* growth of the function F has to be assumed. One can use some function φ or a given constant τ as in our Theorem 8 or Corollary 9.

REMARK 13. Finally, note that the authors of (Iqbal & Rizwan, 2020), in the examples and applications at the end of the paper, used just functions with *strict* growth, in contrast with the theoretical results in the paper which they claim to hold when a non-decreasing function F is used. Moreover, in all these examples and applications, the only function F that is used is $F(t) = \ln t$, which is trivially known to produce only very well-known results which can be treated in a classical way, without using the ideas from the papers (Wardowski, 2012) and (Wardowski, 2018). That was also one of our motivations to consider and discuss the work (Iqbal & Rizwan, 2020).

References

Alghamdi, M.A., Hussain, N. & Salimi, P. 2013. Fixed point and coupled fixed point theorems on b-metric-like spaces. *Journal of Inequalities and Applications*, art.number:402. Available at: <https://doi.org/10.1186/1029-242X-2013-402>.

Amini-Harandi, A. 2012. Metric-like spaces, partial metric spaces and fixed points. *Fixed Point Theory and Applications*, art.number:204. Available at: <https://doi.org/10.1186/1687-1812-2012-204>.

Fabiano, N., Kadelburg, Z., Mirkov, N., Šešum Čavić, V. & Radenović, S. 2022. On F -contractions: A survey. *Contemporary Mathematics*, 3(3), pp.327-342. Available at: <https://doi.org/10.37256/cm.3320221517>.

Iqbal, I. & Rizwan, M. 2020. Existence of the Solution to Second Order Differential Equation Through Fixed Point Results for Nonlinear F -Contractions Involving w_0 -Distance. *Filomat*, 34(12), pp.4079-4094. Available at: <https://doi.org/10.2298/FIL2012079I>.

Kada, O. Suzuki, T. & Takahashi, W. 1996. Nonconvex minimization theorems and fixed point theorems in complete metric spaces. *Mathematica Japonicæ*, 44(2), pp.381-391. Available at: <https://cir.nii.ac.jp/crid/1570009749812799360>.

Kadelburg, Z. & Radenović, S. 2024. Some new observations on w -distance and F -contractions. *Matematički Vesnik*, 76(1), in press.

Matthews, S.G. 1994. Partial Metric Topology. *Annals of the New York Academy of Sciences*, 728(1), pp.183-197. Available at: <https://doi.org/10.1111/j.1749-6632.1994.tb44144.x>.

Popescu, O. & Stan, G. 2020. Two Fixed Point Theorems Concerning F -Contraction in Complete Metric Spaces. *Symmetry*, 12(1), art.number:58. Available at: <https://doi.org/10.3390/sym12010058>.

Shukla, S. 2014. Partial b -Metric Spaces and Fixed Point Theorems. *Mediterranean Journal of Mathematics*, 11, pp.703-711. Available at: <https://doi.org/10.1007/s00009-013-0327-4>.

Wardowski, D. 2012. Fixed points of a new type of contractive mappings in complete metric spaces. *Fixed Point Theory and Applications*, art.number:94. Available at: <https://doi.org/10.1186/1687-1812-2012-94>.

Wardowski, D. 2018. Solving existence problems via F -contractions. *Proceedings of the American Mathematical Society*, 146(4), pp.1585-1598. Available at: <https://doi.org/10.1090/proc/13808>.

Критические замечания о статье «О существовании решения дифференциального уравнения второго порядка через результаты о неподвижной точке для нелинейных F -сжатий с использованием w_0 -дистанцией»

Зоран Кадельбург^а, Никола Фабиано^б,
Милица Саватович^в, Стоян Раденович^г

^а Белградский университет, факультет математики,
г. Белград, Республика Сербия

^б Белградский университет, Институт ядерных исследований
«Винча» – Институт государственного значения для Республики
Сербия, г. Белград, Республика Сербия, **корреспондент**

^в Белградский университет, факультет электротехники,
г. Белград, Республика Сербия

^г Белградский университет, Машиностроительный факультет,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 27.00.00 МАТЕМАТИКА,
27.25.17 Метрическая теория функций,
27.39.15 Линейные пространства,
снабженные топологией, порядком
и другими структурами

ВИД СТАТЬИ: оригинальная научная статья



Резюме:

Введение/цель: В этой статье представлено несколько критических замечаний относительно статьи, написанной в 2020 году Iqbal & Rizwan: Existence of the solution to second order differential equation through fixed point results for nonlinear F-contractions involving w_0 -distance.

Методы: Общепринятые теоретические методы функционального анализа.

Результаты: Доказано, что использование ими неубывающей "управляющей" функции F вместо строго возрастающей в результатах типа Вардовского обычно приводит к противоречиям.

Выводы: Показано, что такие результаты могут быть получены в более общем классе пространств подобных метрическим, где строгая монотонность является единственным условием, которое необходимо наложить на функцию F . Приведен пример, показывающий, что полученные результаты сильнее классических.

Ключевые слова: F -сжатие, неподвижная точка, метрическое пространство, строго возрастающая функция.

Критичке напомене о чланку „Постојање решења диференцијалне једначине другог реда помоћу резултата о непокретној тачки F -контракција користењем w_0 -дистанцу”

Зоран Каделбург^а, Никола Фабиано^б,
Милица Саватовић^в, Стојан Раденовић^г

^а Универзитет у Београду, Математички факултет,
Београд, Република Србија

^б Универзитет у Београду, Институт за нуклеарне науке “Винча”
– Национални институт Републике Србије, Београд, Република
Србија, **аутор за преписку**

^в Универзитет у Београду, Електротехнички факултет,
Београд, Република Србија

^г Универзитет у Београду, Машински факултет,
Београд, Република Србија

ОБЛАСТ: математика

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: У овом раду изнето је неколико критичких напомена у вези са радом Iqbal & Rizwan: *Existence of the solution to second order differential equation through fixed point results for nonlinear F-contractions involving w_0 -distance*, из 2020. године.

Методе: Конвенционалне теоријске методе функционалне анализе.

Резултати: Показано је да њихова употреба неоппадајуће „контролне“ функције F уместо стриктно растуће у резултатима типа Вардовског обично производи контрадикцију.

Закључак: Такви резултати могу се добити у општијој класи метричких простора, где је строга монотоност једина претпоставка која се мора наметнути функцији F . Приказан је пример који показује да су добијени резултати јачи од класичних.

Кључне речи: F -контракција, фиксна тачка, простор сличан метрици, строго растућа функција.

Paper received on / Дата получения работы / Датум пријема чланка: 12.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 21.11.2023.

Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 22.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).


© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Application of the type-2 fuzzy logic controller and the fractional order controller to regulate the DTC speed in an induction motor

Younes Abdelbadie Mabrouk^a, Bachir Mokhtari^b,
Tayeb Allaoui^c

^a University Ammar Telidji, Electrotechnics Department,
The laboratory for the study and development of semiconductors and
dielectric materials (LEDMASD),
Laghouat, People's Democratic Republic of Algeria,
e-mail: mab.younes@lagh-univ.dz, **corresponding author**,
ORCID iD:  <https://orcid.org/0009-0007-5220-3685>

^b University Ammar Telidji, Electrotechnics Department,
The laboratory for the study and development of semiconductor and
dielectric materials (LEDMASD),
Laghouat, People's Democratic Republic of Algeria,
e-mail: ba.mokhtari@lagh-univ.dz,
ORCID iD:  <https://orcid.org/0000-0003-4643-8940>

^c University of Tiaret, Department of Electrical Engineering, Energy
Engineering and Computer Engineering Laboratory (L2GEGI),
Tiaret, People's Democratic Republic of Algeria,
e-mail: tayeb.allaoui@univ-tiaret.dz,
ORCID iD:  <https://orcid.org/0000-0001-9295-073X>

DOI: 10.5937/vojtehg71-45972; <https://doi.org/10.5937/vojtehg71-45972>

FIELD: mathematics, computer science, electrical machines and control
ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Among excellent strategies available to control the torque of asynchronous motors, we distinguish direct torque control. This technique of control allows direct control of magnetic flux and electromagnetic torque without the need to decouple them. Also, direct torque control like each control strategy has some drawbacks, the major drawbacks of this technique being operation at a variable switching frequency and flux and electromagnetic ripples due to the use of hysteresis regulators. It worsens acoustic noise, especially at low speeds, as well as the control performances.

Methods: To improve the performance of direct torque control especially at low speeds, the authors propose using fractional order PID in combination with type-2 fuzzy logic controllers to regulate the speed of an induction motor controlled by direct torque control.

Results: The results obtained by the proposed regulators show the improvements made to the system.

Conclusion: The proposed contribution can exert better control efforts.

Keywords: direct torque control (DTC), fuzzy logic controller (FLC), fractional order controller (FO), induction motor (IM), FFT analysis.

Introduction

Induction motors (IMs) are widely used in many industrial applications because of their low cost and simple construction (Berrabah et al, 2017). In comparison between IMs and direct current motors, IMs have a simple and rugged structure, higher maintainability, and economy (Belhamdi & Amar, 2017). On the other hand, these motors are not without inconvenience: their dynamic behavior is often very complex since their modeling results in a system of nonlinear equations, strongly coupled and multivariable. Some of its variables are not measurable, e.g. magnetic flux. For these reasons, the IM requires an advanced algorithm to control the torque and flux. From such algorithms, we distinguish direct torque control (DTC) which was proposed by Mr. Takahashi in 1985 as an alternative to field-oriented control (Prasad & Durgasukuamar, 2021). Fast dynamic reaction, a straightforward control strategy, the lack of coordinate transformations, the absence of position feedback, and current regulators are all benefits of DTC (Quang & Dittrich, 2015; Trabelsi et al, 2012). Despite all these advantages, this control has disadvantages such as high torque and flux ripples due to the use of a hysteresis band, stator current distortions, and poor performance at low and starting speeds (Trabelsi et al, 2012). For these reasons, several research studies were developed to master the performance of this control technique such as the use of artificial intelligence techniques to replace the hysteresis regulators and the switching table (Bounar et al, 2015; El Ouanjli et al, 2018), to control the motor speed (Sai Krishna & Narasimha Reddy, 2019; Lakshmi Prasanna et al, 2018), a combination between the SVM and DTC was proposed in (Cherif & Yahia, 2020; Massoum et al, 2021). In (Benbouhenni et al, 2017), the authors proposed to replace the conventional controller used to control the speed of the IM by an adaptive fuzzy logic controller. In (Ben Salem & Derbel, 2017), the authors proposed to control the speed of the motor by sliding mode control and used AI to improve the DTC performances.

As mentioned previously, among the disadvantages of the DTC command is that it presents poor performance at low and starting speeds, as well as the noise caused by the torque ripples. For these reasons,

researchers have always worked to improve the performance of this control, and they have used several techniques as we cited previously. Among the best control strategies, we distinguish fuzzy logic controllers (FLCs) which offer several benefits in various applications due to their ability to handle imprecise, uncertain, or vague information. Also, FLCs can model complex, nonlinear systems without requiring precise mathematical models, and manage uncertainty and imprecision in input data and system parameters. For these reasons, we propose in this paper to replace the conventional regulator used to control the speed of the IM with a developed one, such as type-2 fuzzy logic controller and the fractional-order PID regulator after that to see the improvements made to the system. In the second section, we present the model of the IM in the stationary frame; after that we discuss the basics of DTC control, and then in section 4, we present the different regulators used in this work. The simulation results and their discussion make the objective of section 5. Finally, we conclude the paper with a conclusion.

Model of the IM

The representation of the IM in the stationary reference to the α and β axes is given by the following equations (Cherif & Yahia, 2020).

For the electrical variables

$$\begin{cases} \frac{d\varphi_{\alpha s}}{dt} = V_{\alpha s} - R_s I_{\alpha s} \\ \frac{d\varphi_{\beta s}}{dt} = V_{\beta s} - R_s I_{\beta s} \\ \frac{d\varphi_{\alpha r}}{dt} = -R_r I_{\alpha r} - \omega_m \varphi_{\beta r} \\ \frac{d\varphi_{\beta r}}{dt} = -R_r I_{\beta r} + \omega_m \varphi_{\alpha r} \end{cases} \quad (1)$$

where the subscripts s and r refer to the stator and the rotor, α and β refer to the components in the (α, β) frame, the terms V , I , and φ are used to describe voltage, current, and flux, respectively, while R_s and R_r refer to the stator and the rotor resistances and ω_m is rotor pulsation.

The relationships between currents and flux are given by equation (2)

$$\begin{bmatrix} \varphi_{s\alpha} \\ \varphi_{r\alpha} \end{bmatrix} = \begin{bmatrix} L_s & M \\ M & L_r \end{bmatrix} \begin{bmatrix} I_{\alpha s} \\ I_{\alpha r} \end{bmatrix},$$

$$\begin{bmatrix} \varphi_{s\beta} \\ \varphi_{r\beta} \end{bmatrix} = \begin{bmatrix} L_s & M \\ M & L_r \end{bmatrix} \begin{bmatrix} I_{\beta s} \\ I_{\beta r} \end{bmatrix} \quad (2)$$

L and M represent the motor and the mutual inductance, respectively.

The mechanical component of the motor is explained as follows (Cherif & Yahia, 2020):

$$\frac{d\Omega}{dt} = \frac{1}{J} (T_{em} - T_L) \quad (3)$$

T_{em} and T_L represent respectively the electromagnetic torque and load one, and J represents the motor inertia.

Direct torque control of an IM

DTC is a technique that directly controls the torque and flux of an IM by adjusting the inverter voltage and frequency. This allows for precise control of the motor speed and torque, without the need for complex feedback control loops. It also enables an IM to have an accurate and quick electromagnetic torque response.

The appropriate voltage vector is selected by means of a switching table. The variation in the motor stator flux and torque is directly related to the selection of switching states.

As a result, the choice is made by keeping the magnitudes of the flux and torque within two hysteresis bands. These controllers ensure that these two quantities are controlled separately (Takahashi & Noguchi, 1986; Depenbrock, 1987).

The inputs of hysteresis controllers are flux and torque errors, and the voltage vector that is appropriate for each commutation period is determined by the controllers' outputs (Shyu et al, 2010).

Generally, the purpose of this control is to regulate the stator flux and the electromagnetic torque without having measured the speed, flux, or torque. Only the measurements of voltages and currents are necessary. A synoptic schema of the DTC of an IM is shown in Figure 1.

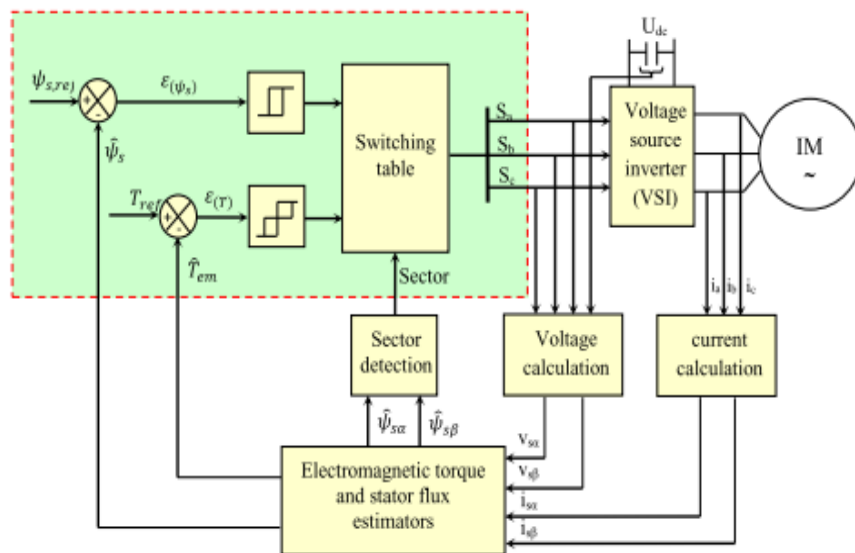


Figure 1 – Synoptic schema of the DTC of an IM

Рис. 1 – Наглядная схема прямого регулирования крутящего момента в асинхронном двигателе

Слика 1 – Синоптичка шема директног управљања моментом у индукционом мотору

Estimation of flux and electromagnetic torque

In DTC, the electromagnetic torque and stator flux are calculated from the primary motor inputs, stator voltages, and currents (V_s and I_s). The expressions of the flux into the stator can be evaluated as in equation (4).

$$\varphi_s = \sqrt{\varphi_{\alpha s}^2 + \varphi_{\beta s}^2} \quad (4)$$

The variables in equation (4) are given as (Cherif & Yahia, 2020)

$$\begin{cases} \varphi_{\alpha s} = \int (V_{\alpha s} - R_s I_{\alpha s}) \\ \varphi_{\beta s} = \int (V_{\beta s} - R_s I_{\beta s}) \end{cases} \quad (5)$$

$\varphi_{\alpha s}$ and $\varphi_{\beta s}$ are the components of the flux in the (α, β) frame (Cherif & Yahia, 2020).

The angle θ between the components of the flux is given in (6).

$$\theta = \arctg \frac{\varphi_{\beta s}}{\varphi_{\alpha s}} \quad (6)$$

To determine the electromagnetic torque produced by the IM, the cross-product of the stator quantities (stator flux and stator currents) can be employed as follows

$$T_{em} = \frac{3}{2} p (\varphi_{\alpha s} I_{\beta s} - \varphi_{\beta s} I_{\alpha s}) \quad (7)$$

where p is the number of poles pairs.

The conventional switching DTC table

The conventional switching DTC table used to select the appropriate voltage vector proposed by Takahashi (Takahashi & Noguchi, 1986), is given in the following table.

Table 1 – DTC switching table

Таблица 1 – Таблица переключателей прямого управления крутящим моментом
Табела 1 – Табела прекидача при директном управљању моментом силе

Sector		1	2	3	4	5	6
Flux	Torque						
$C_{flux}=1$	$C_{trq}=1$	V2	V3	V4	V5	V6	V1
	$C_{trq}=0$	V7	V0	V7	V0	V7	V0
	$C_{trq}=-1$	V6	V1	V2	V3	V4	V5
$C_{flux}=0$	$C_{trq}=1$	V3	V4	V5	V6	V1	V2
	$C_{trq}=0$	V0	V7	V0	V7	V0	V7
	$C_{trq}=-1$	V5	V6	V1	V2	V3	V4

C_{flux} and C_{trq} represent the flux and electromagnetic torque errors, respectively (Mokhtari, 2014).

Fuzzy Logic Controller

Fuzzy Logic Controllers (FLCs) are used in applications where traditional binary logic controllers may not be suitable or efficient. FLCs introduce a degree of "fuzziness" or uncertainty into decision making, which can be advantageous in various scenarios. We need to use FLCs for many reasons, such as: handling uncertainty, human-like reasoning, tolerance to noise and adaptive control (Aib et al, 2023).

FLC structure

Four principal components build the FLC controller: (Kamalapur & Aspalli, 2023)

Fuzzification

The following operations are performed via the fuzzification interface which

- measures the input variable's values, and
- performs the fuzzification function, which transforms input data into appropriate linguistic values.

Knowledge base

A linguistic control rule base plus a database make up a knowledge base.

- The definitions needed to define linguistic control rules are provided by the database;
- Using a set of language control rules, the rule base described the domain experts' control objectives and control strategy.

Decision

An FLC's core is the logic for making decisions. It can use fuzzy implications and the rules of inference from fuzzy logic to infer fuzzy control actions and simulate human decision making based on fuzzy concepts.

Defuzzification

The defuzzification interface performs the following functions:

- A scale mapping that converts the distribution of output variable values into the associated discourse universe, and
- Defuzzification, which involves changing an implied fuzzy control action into an explicit control action (Aib et al, 2023; Kamalapur & Aspalli, 2023).

Inference and the formulation of rules

Fuzzy systems typically map input fuzzy sets to output fuzzy sets. The relations between input and output fuzzy sets are known as fuzzy rules. Any of the following can be used to derive fuzzy rules:

- Master insight and control designing information,
- Control actions were taken by the operator, or
- Gaining knowledge from the training examples.

The fuzzy rules in this study are created by learning from the training instances. In this instance, the fuzzy control rules' general form is

If x is A_i AND y is B_j THEN $z = f_i(x, y)$

Where x , y , and z are the linguistic variables that, respectively, indicate the control variable and the process state variables. A first-order Sugeno fuzzy model is the outcome of a fuzzy inference system (FIS) that takes the form of a first-order Sugeno fuzzy model. A_i and B_j are the linguistic values of the linguistic variables, $f_i(x, y)$ is a function of the process state variables x , y .

Engine for fuzzy inference

The feature of the inference engine is to calculate the general price of the manipulated output variable primarily based on the character contributions of each rule in the rule of thumb base, i.e., the defuzzification system. There's no systematic method for choosing defuzzification. In the first-order Sugeno fuzzy model, each rule has a crisp output and the usual output is acquired as weighted common as a consequent hence averting the time-ingesting manner of defuzzification required in a conventional FLC (Precup et al, 2020).

Type-2 fuzzy logic controller

A type-2 FLC is an extension of the traditional FLC, which allows for the handling of uncertainties and higher levels of complexity in the system being controlled. While a traditional FLC uses linguistic variables and fuzzy rules to make decisions, a type 2-FLC (T2-FLC) goes a step further by considering the uncertainties associated with the linguistic variables. In a T2-FLC, each linguistic variable has a fuzzy set associated with it, and each fuzzy set has a footprint of uncertainty (FOU) associated with it (Aib et al, 2023). The FOU represents the level of confidence or uncertainty in the membership values of the fuzzy set. By incorporating this uncertainty information, a T2-FLC can handle situations where the membership values are not precise or known with certainty. T2-FLCs are particularly useful in systems with highly uncertain or imprecise input data. They allow for the modeling and control of complex systems that exhibit varying degrees of uncertainty. However, the increased complexity of T2-FLCs also means that they require more computational resources and are often more challenging to design and implement compared to traditional FLCs (Saidi et al, 2020; Henini et al, 2021).

General type-2 fuzzy sets

A kind-1 fuzzy unit A on a time-honored set X can be characterized by the club function as (8). (Shi, 2020)

$$A = \{ x, u(x) | \forall x \in X, \mu(x) \in [0,1] \} \quad (8)$$

α cuts of A can be defined as (9).

$$A_\alpha = \{ x, | \mu(x) \geq \alpha, \alpha \in [0,1] \} \quad (9)$$

A_α consists of all of the element's x within the domain X whose club degree is extra than or identical to α , the function characteristic of which is proven as:

$$\mu_{A_\alpha} = \begin{cases} 1, & x \in A_\alpha \\ 0, & x \notin A_\alpha \end{cases} \quad (10)$$

The definition of fuzzy units of variety multiplication is shown as (11).

$$\forall x \in X, \alpha A(x) = \alpha \wedge A(x) = \begin{cases} \alpha & A(x) > \alpha \\ A(x) & A(x) \leq \alpha \end{cases} \quad (11)$$

Then, type-1 fuzzy unit A may be represented through its α cuts as (12).

$$A = \bigcup_{\alpha \in [0,1]} \alpha A_\alpha \quad (12)$$

Type-2 fuzzy sets have 2 club capabilities, and a kind-2 fuzzy set \tilde{A} an established set X may be characterized by the way of the membership function as (sixteen), where $x \in X$.

$$\tilde{A} = \{(x, u), u_{\tilde{A}}(x, u) | \forall x \in X, \forall u \in [0,1]\} \quad (13)$$

μ is the primary club function and $\mu_{\tilde{A}}(x, u)$ is the secondary membership function. Liu extended α cuts of type-1 fuzzy sets to popular type-2 fuzzy sets and α cuts (α planes) of widespread type-2 fuzzy units \tilde{A} α can be described as

$$\tilde{A}_\alpha = \{(x, u), \mu_{\tilde{A}}(x, u) | \forall x \in X, \forall u \in [0,1]\} \quad (14)$$

A well-known kind-2 fuzzy units \tilde{A} can be represented because the union of its associated kind-2 fuzzy sets \tilde{A}_α

$$A = \bigcup_{\alpha \in [0,1]} FOU(\tilde{A}_\alpha) \quad (15)$$

For a general type-2 fuzzy set, A is the union of the centroids of its associated type-2 fuzzy sets for the minimum t-norm operation. \tilde{A}_α , with $\alpha \in [0, 1]$:

$$CA_\alpha(x) = [l_{\tilde{A}_\alpha}, r_{\tilde{A}_\alpha}] \quad (16)$$

$\{l\tilde{A}^{\alpha}, r\tilde{A}^{\alpha}\}$ represent each α -plane's estimated endpoints using the KM type reduction procedure. Therefore, D times of the KM technique will be used if the number of planes is D to produce the defuzzification result of general type-2 fuzzy sets. (Shi, 2020).

The design of the type-2 FLC system

The structure of T2-FLC shown in Figure 2 is similar to that of type-1, the only difference between them being the type of sets (Figure 3), and in type-2 we have to use another step called type-reducer to change the output of fuzzy into a type-1 fuzzy set.

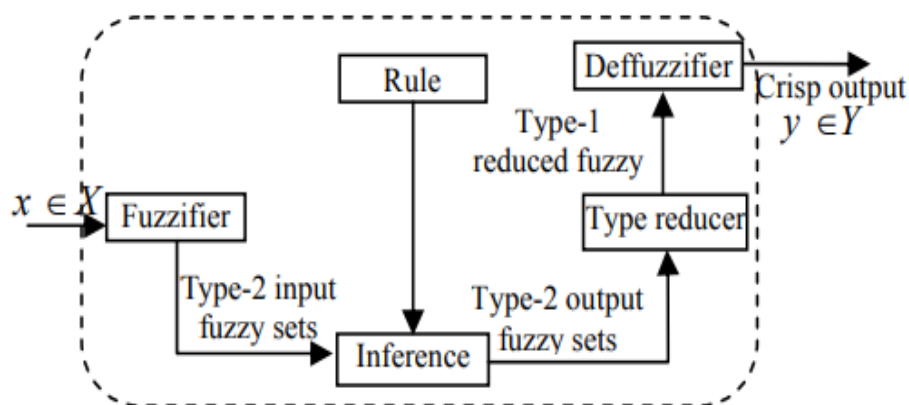


Figure 2 – Structure of a T2FLC
 Рус. 2 – Структура T2FLC
 Слика 2 – Структура T2FLC

In the type reduction stage, the type 2 interval fuzzy outputs of the inference engine are converted into the type 1 interval fuzzy in order to do defuzzification. The type reduction block is the primary distinction between types 1 and 2 of fuzzy logic systems (Henini et al, 2021).

Consider a T2FLS having:

n , inputs, $x = [x_1 \dots x_n] \in X_1 \times \dots \times X_n$;

one output $y \in Y$, and M rules, where the i^{th} rules have the form:

R^i IF x_1 is F_1^i and ...and x_n is F_n^i THEN $y^i = C^i$; $i = 1, \dots, M$.

With $F_1^i, F_2^i \dots F_n^i$ are the linguistic terms used in the past. The interval Type-2 Gaussian fuzzy sets serves as their model (Fig. 11).

y is the output of the i^{th} rule R^i ; C^i is the consequent parameter.

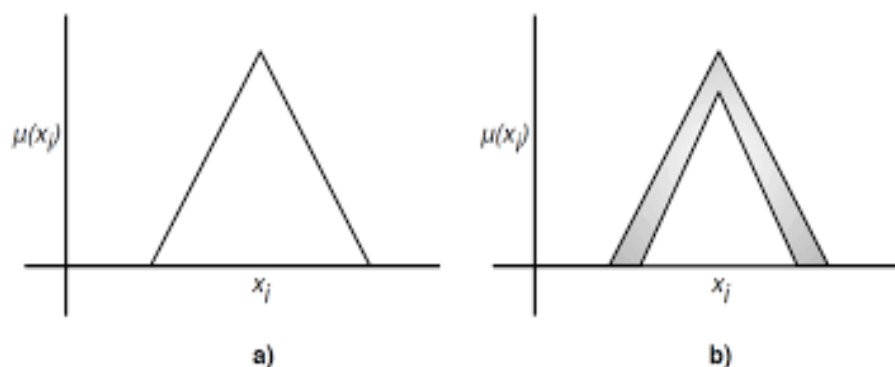


Figure 3 – Difference between type-1 and type-2 membership functions
 Рис. 3 – Разница между функциями принадлежности типа 1 и типа 2
 Слика 3 – Разлика између функција припадности типа 1 и типа 2

In Fig. 3, the upper membership function $\bar{u}_{FIj}(xj)$ can be used to represent the footprint of uncertainty (FOU) as a bound interval and the lower membership function $u_{FIj}(xj)$, where

$$\bar{u}_{FIj}(xj) = \exp \left[-\frac{1}{2} \left(\frac{xj - mj}{\sigma_{kj}} \right)^2 \right] = N(mj, \sigma_j, xj) \quad (17)$$

and:

$$u_{FIj}(xj) = 0.8 \bar{u}_{FIj}(xj) \quad (18)$$

m_j , and σ_j are respectively the imply and the usual deviation of Gaussian primary MF of the kind-2 fuzzy set \tilde{F}_j^u (Shi, 2020).

In this study, we use T2-FLC to control the speed of the IM; for this, three membership functions (MFs) are established for output and are used to characterize the range of fuzzy controller inputs (speed error and speed error variation). The fuzzy inference system bases its inference of gains on nine rules. MFs for both inputs and output are Negative (Ne), Zero (Zo), and Positive (Po). Two trapezoidal mfs for the two fuzzy sets (Po) and (Ne) and a triangular one for the fuzzy set (Zo) are used in this study.

Fractional order PID

A fractional order PID (Proportional-Integral-Derivative) controller, often referred to as a FO-PID controller, is an advanced control strategy that extends the classical PID controller by introducing fractional calculus principles. In a regular PID controller, the control action is determined based on the current error, the integral of the error, and the derivative of

the error (Maiti et al, 2020). The goal is to minimize the difference between the desired setpoint and the actual process variable by adjusting a control signal. In a FO-PID controller, the integral and derivative terms are modified by using fractional calculus operators such as fractional integrals and derivatives. Instead of the usual integer values for the integral and derivative terms, fractional orders (non-integer values) are employed, allowing for a more flexible and adaptable control action (Sharma et al, 2015).

The FO-PID controller can be mathematically represented as follows:

$$u(t) = K_p * e(t) + K_i * D^{(m)} * e(t) + K_d * D^{(n)} * e(t) \quad (19)$$

where:

- $u(t)$ is the control output (control signal) at time t ,
- $e(t)$ is the error at time t , calculated as the difference between the desired setpoint and the actual process variable,
- K_p , K_i , and K_d are the traditional PID gains for the proportional, integral, and derivative terms, respectively,
- $D^{(m)}$ represents the fractional integral operator of the order ' m ', and
- $D^{(n)}$ represents the fractional derivative operator of the order ' n '.

The use of fractional orders in the integral and derivative terms allows for more control flexibility and better performance in systems with non-linear dynamics or time-varying processes. It can effectively deal with processes that exhibit fractional-order behavior, which cannot be adequately controlled by traditional integer order PID controllers (Sharma et al, 2015).

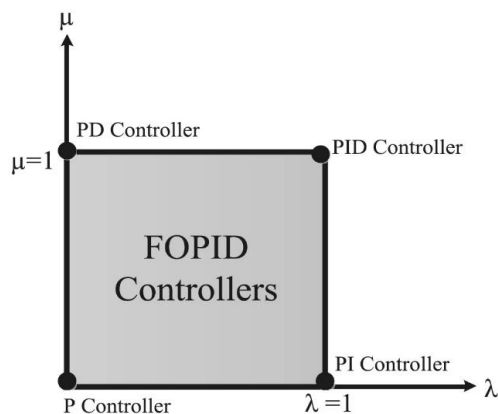


Figure 4 – Structure schema of the FO- $P^{\lambda}D^{\mu}$ controller
 Рис. 4 – Схема структуры контроллера FO- $P^{\lambda}D^{\mu}$
 Слика 4 – Шема структуре контролера FO- $P^{\lambda}D^{\mu}$

FO-PID controllers have been applied in various fields, including industrial process control, robotics, aerospace, and biomedical engineering, where precise and adaptable control is required. However, it is worth noting that the design and tuning of fractional order PID controllers can be more complex than that of their classical counterparts, as the choice of fractional orders introduces additional degrees of freedom that need to be carefully optimized for optimal control performance.

We propose in this part to use T2-FLC, and FO-PID to control the speed of an IM controlled by DTC. In the following section, we present and discuss the simulation results of this proposition.

Simulation results and the discussion

We present a discussion which follows the simulation results and the current spectral analysis of the DTC control applied to an IM, with three different speed regulators, a load torque applied between $t=0.2\text{s}$ and $t=0.4\text{s}$ and the rotation speed reduced from 150 to 50 at $t=0.5\text{s}$.

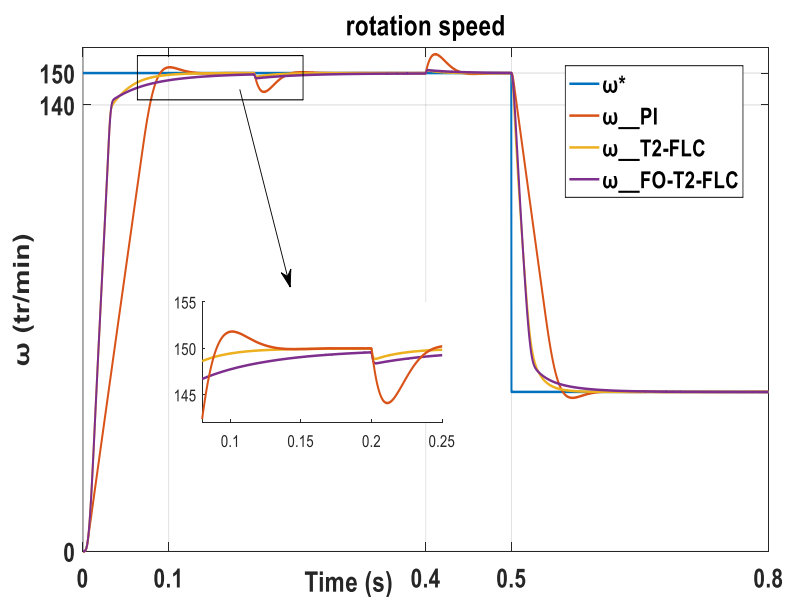


Figure 5 – Rotation speed of the IM

Рис. 5 – Скорость вращения асинхронного двигателя

Слика 5 – Брзина ротације индукционог мотора

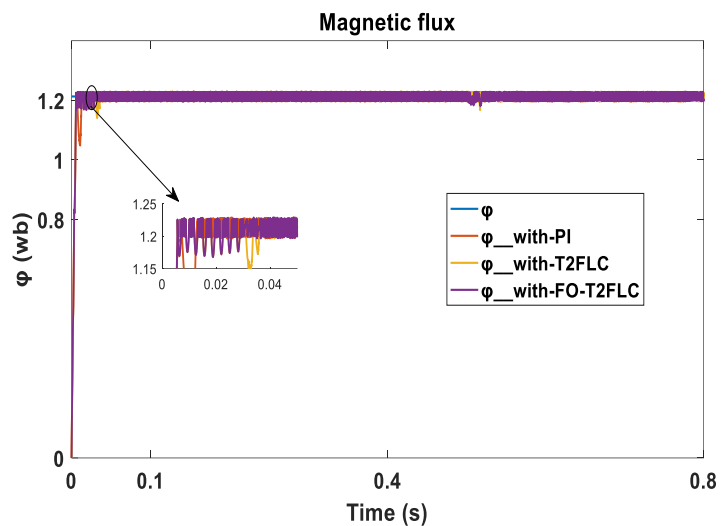


Figure 6 – Magnetic flux
 Рис. 6 – Магнитный поток
 Слика 6 – Магнетни флукс

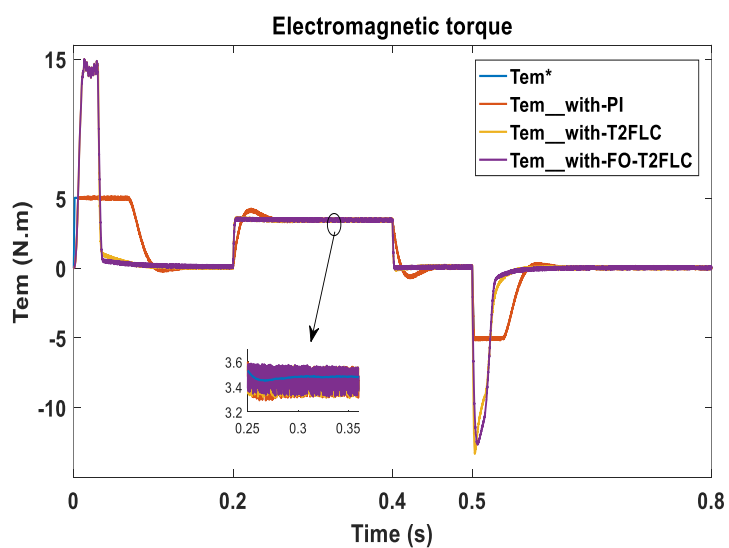


Figure 7 – Electromagnetic torque
 Рис. 7 – Электромагнитный момент
 Слика 7 – Электромагнетни моменат силе

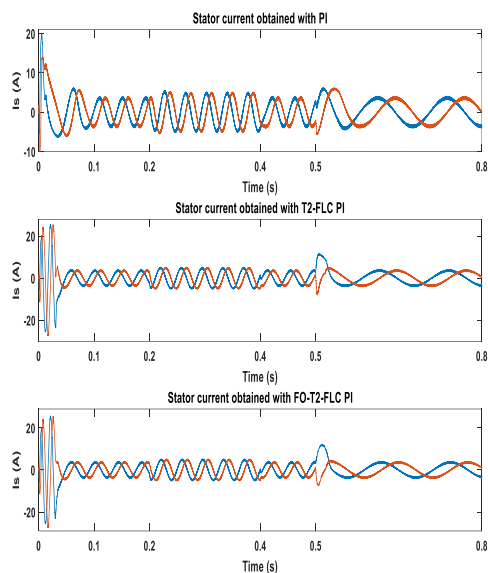


Figure 8 – Stator currents
 Рис. 8 – Ток статора
 Слика 8 – Струје статора

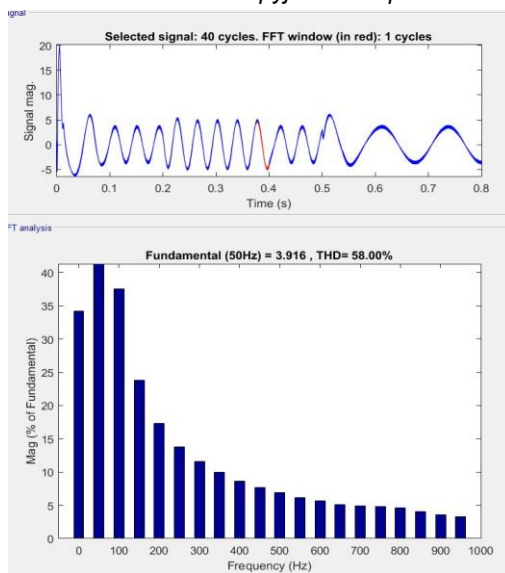


Figure 9 – FFT analysis of the stator current obtained with a classical regulator
 Рис. 9 – БПФ-анализ тока статора, полученного с помощью классического регулятора
 Слика 9 – ФФТ анализа струје статора добијена помоћу класичног регулатора

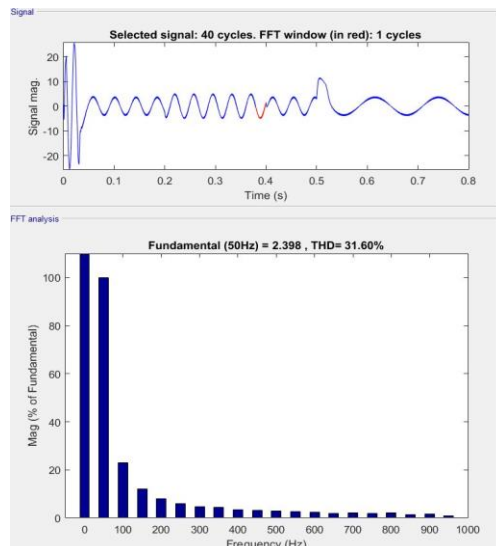


Figure 10 – FFT analysis of the stator current obtained with a T2FLC regulator
 Рис. 10 – БПФ-анализ тока статора, полученный с помощью регулятора T2FLC
 Слика 10 – ФФТ анализа струје статора добијена помоћу регулятора T2FLC

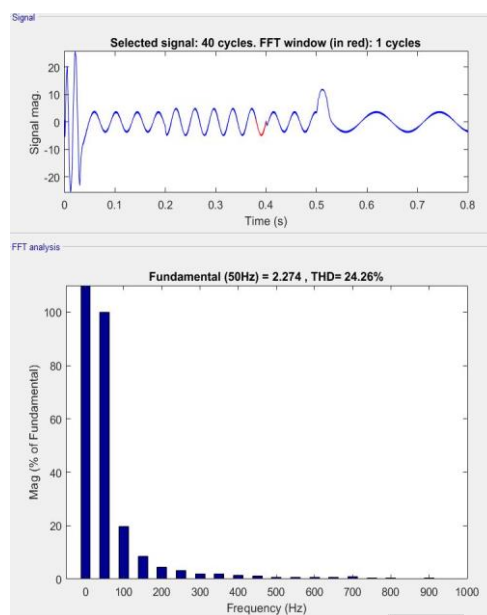


Figure 11 – FFT analysis of the stator current obtained with a FO-T2FLC regulator
 Рис. 11 – БПФ-анализ тока статора, полученный с помощью регулятора FO-T2FLC
 Слика 11 – ФФТ анализа струје статора добијена помоћу регулятора FO-T2FLC

From the results shown in Figures (5 to 9), we can notice that:

With the T2-FLC and FO-T2-FLC regulators, the dynamics of the IM is faster than with the classical one (Fig. 5), and the rotational speed reaches its reference without any exceeding; also, we can notice that the effect of the load torque with the T2-FLC and FO-T2-FLC is inconsiderable.

The magnetic flux and the electromagnetic torque (Figs. 6 and 7) follow their references with a good dynamics and fewer ripples when using T2-FLC and FO-T2-FLC regulators.

From the spectral analysis of the stator current (Figs. 9, 10, and 11), we can conclude that with the FO-T2-FLC we obtained the best quality of the current (as shown in the peaks in Fig. 8) with a reduced THD value.

Conclusion

This paper deals with a DTC scheme applied to an IM. Initially, the motor system was studied and modeled, and all the corresponding equations were given. Then, based on the hysteresis controller, the conventional DTC design was presented and then explained. As this traditional technique has numerous problems, such as torque and flux ripples, and especially poor motor speed performances, we proposed using a type-2 fuzzy logic controller (FLCT2) and the fractional order controller (FOC) to regulate the rotation speed of this motor, and show its influence on the behaviour of the motor. The simulation results showed that the use of the t2-FLC and the FO-PID made it possible to bring several improvements to the performance of DTC such as the speed of the dynamic response, the improvement of the quality of the current by reducing its THD value and the minimization of torque ripples. We propose to carry out an experimental study of this strategy in future work.

References

Aib, A., Khodja, D.E. & Chakroune, S. 2023. Field programmable gate array hardware in the loop validation of fuzzy direct torque control for induction machine drive. *Electrical Engineering & Electromechanics*, 3, pp. 28-35. Available at: <https://doi.org/10.20998/2074-272X.2023.3.04>.

Belhamdi, S. & Amar, G. 2017. Direct Field-Oriented Control using Fuzzy Logic Type-2 for Induction Motor with Broken Rotor Bars. *MSE JOURNALS-AMSE IIETA publication-2017-Series: Advances C*; Vol. 72; N°4; pp 203-212 Available at: https://doi.org/10.18280/ama_c.720401.

Benbouhenni, H., Taleb, R. & Chabni, F. 2017. Commande DTC cinq niveaux à 24 secteurs d'un moteur asynchrone par méthodes intelligentes. In: *1st Algerian Multi-Conference on Computer, Electrical and Electronic Engineering (AMCEEE'17)*, Algiers, Algeria, April 24-27.

Ben Salem, F. & Derbel, N. 2017. DTC-SVM-Based Sliding Mode Controllers with Load Torque Estimators for Induction Motor Drives. In: Derbel, N., Ghommam, J. & Zhu, Q. (Eds.) *Applications of Sliding Mode Control. Studies in Systems, Decision and Control*, 79. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-10-2374-3_14.

Berrabah, F., Chebabhi, A., Zeglache, S. & Saad, S. 2017. Direct Torque Control of Induction Motor Fed by Three-level Inverter Using Fuzzy Logic. *Advances in Modelling and Analysis C*, 72(4), pp.248-265. Available at: https://doi.org/10.18280/ama_c.720404.

Boumar, N., Boulkroune, A., Boudjema, F., M'Saad, M. & Farza, M. 2015. Adaptive fuzzy vector control for a doubly-fed induction motor. *Neurocomputing*, 151(Part 2), pp.756-769. Available at: <https://doi.org/10.1016/j.neucom.2014.10.026>.

Cherif, D. & Yahia, M. 2020. Direct Torque Control Strategies of Induction Machine: Comparative Studies. In: Ben Salem, F. (Eds.) *Direct Torque Control Strategies of Electrical Machines*. London, UK: IntechOpen. Available at: <https://doi.org/10.5772/intechopen.90199>.

Depenbrock, M. 1987. Direct self-control (DSC) of inverter fed induction machine. In: *IEEE Power Electronics Specialists Conference*, Blacksburg, VA, USA, pp.632-641, June 21-26. Available at: <https://doi.org/10.1109/PESC.1987.7077236>.

El Ouanjli, N., Taoussi, M., Derouich, A., Chebabhi, A., El Ghzizal, A. & Bossoufi, B. 2018. High Performance Direct Torque Control of Doubly Fed Induction Motor using Fuzzy Logic. *Gazi University Journal of Science*, 31(2), pp.532-542 [online]. Available at: <https://dergipark.org.tr/en/pub/gujs/issue/37206/363820> [Accessed: 10 August 2023].

Henini, N., Tlemçani, A. & Barkat, S. 2021. Adaptive Interval Type-2 Fuzzy Con-troller Based Direct Torque Control of Permanent Magnet Synchronous Motor. *Advances in Electrical and Computer Engineering (AECE)*, 21(2), pp.15-22. Available at: <https://doi.org/10.4316/AECE.2021.02002>.

Kamalapur, G. & Aspalli, M.S. 2023. Direct torque control and dynamic performance of induction motor using fractional order fuzzy logic controller. *International Journal of Electrical and Computer Engineering (IJECE)*, 13(4), pp.3805~3816. Available at: <https://doi.org/10.11591/ijece.v13i4.pp3805-3816>.

Lakshmi Prasanna, K., Chandra Sekhar, J.N. & Marutheaswar, G. 2018. Implementation of DTC in Induction Motor Using Anfis Pi Controller. *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, 4(4), pp.422-428 [online]. Available at: <https://ijsrset.com/IJSRSET1844108> [Accessed: 10 August 2023].

Mokhtari, B. 2014. *DTC Intelligente Appliquée à la Commande de la Machine Asynchrone*. Ph.D. thesis. Batna, Algeria: University of Batna [online]. Available at: <http://eprints.univ-batna2.dz/1244/> [Accessed: 10 August 2023].

Maiti, D., Biswas, S. & Konar, A. 2020. Design of a Fractional Order PID Controller Using Particle Swarm Optimization Technique. *arXiv:0810.3776*. Available at: <https://doi.org/10.48550/arXiv.0810.3776>.

Massoum, S., Meroufel, A., Massoum, A. & Patrice, W. 2021. DTC based on SVM for induction motor sensorless drive with fuzzy sliding mode speed controller. *International Journal of Electrical and Computer Engineering (IJECE)*, 11(1), pp.171-181. Available at: <https://doi.org/10.11591/ijece.v11i1.pp171-181>.

Prasad, R.R. & Durgasukumar, G. 2021. Enhanced Performance of Indirect Vector Controlled Induction Motor Drive with a Modified Type 2 Neuro-Fuzzy Torque Controller in Interfacing with dSPACE DS-2812. *Journal Européen des Systèmes Automatisés*, 54(2), pp.219-228. Available at: <https://doi.org/10.18280/jesa.540203>.

Precup, R.-E., Preitl, S., Petriu, E., Bojan-Dragos, C.-A., Szedlak-Stinean, A.-I., Roman, R.-C. & Hedrea, E.-L. 2020. Model-Based Fuzzy Control Results for Networked Control Systems. *Reports in Mechanical Engineering*, 1(1), pp.10-25 [online]. Available at: <https://www.rme-journal.org/index.php/asd/article/view/2>.

Quang, N.P. & Dittrich, J.-A. 2015. *Vector Control of Three-Phase AC Machines*. Berlin, Heidelberg: Springer. Available at: <https://doi.org/10.1007/978-3-662-46915-6>.

Sai Krishna, N. & Narasimha Reddy, G. 2019. Direct Torque Control of VSI Fed Induction Motor with Fuzzy Controller. *Turkish Journal of Computer and Mathematics Education*, 10(3), pp.914-918 [online]. Available at: <https://turcomat.org/index.php/turkbilmat/article/view/11839> [Accessed: 10 August 2023].

Saidi, A., Naceri, F., Youb, L., Cernat, M. & Guasch Pesquer, L. 2020. Two Types of Fuzzy Logic Controllers for the Speed Control of the Doubly-Fed Induction Machine. *Advances in Electrical and Computer Engineering (AECE)*, 20(3), pp. 65-74. Available at: <https://doi.org/10.4316/AECE.2020.03008>.

Sharma, R., Gaur, P. & Mittal, A.P. 2015. Performance analysis of two-degree of freedom fractional order PID controllers for robotic manipulator with payload. *ISA Transactions*, 58, pp.279-291. Available at: <https://doi.org/10.1016/j.isatra.2015.03.013>.

Shi, J.Z. 2020. A Fractional Order General Type-2 Fuzzy PID Controller Design Algorithm. *IEEE Access*, 8, pp.52151-52172. Available at: <https://doi.org/10.1109/ACCESS.2020.2980686>.

Shyu, K.-K., Lin, J.-K., Pham, V.-T., Yang, M.-J. & Wang, T.-W. 2010. Global Minimum Torque Ripple Design for Direct Torque Control of Induction Motor Drives. *IEEE Transactions on Industrial Electronics*, 57(9), pp.3148-3156. Available at: <https://doi.org/10.1109/TIE.2009.2038401>.

Takahashi, I. & Noguchi, T. 1986. A New Quick-Response and High-Efficiency Control Strategy of an Induction Motor. *IEEE Transactions on Industry Applications*, IA-22(5), pp.820-827. Available at: <https://doi.org/10.1109/TIA.1986.4504799>.

Trabelsi, R., Khedher, A., Mimouni, M.F. & M'sahli, F. 2012. Backstepping control for an induction motor using an adaptive sliding rotor-flux observer. *Electric Power Systems Research*, 93, pp.1-15. Available at: <https://doi.org/10.1016/j.epsr.2012.06.004>.

Применение контроллера нечеткой логики типа 2 и контроллера дробного порядка при регулировании скорости прямого управления крутящим моментом в асинхронном двигателе

Юнес Абдельбади Мабрук^а, корреспондент, Башир Мохтари^а, Тайеб Аллауи^б

^а Университет Аммара Телиджи, факультет электротехники, Лаборатория по изучению и разработке полупроводниковых и диэлектрических материалов (LEDMASD), г. Лагуат, Алжирская Народная Демократическая Республика

^б Университет Тиарет, факультет электротехники и энергетики и лаборатория инженерного и вычислительного машиностроения (L2GEGI), г. Тиарет, Алжирская Народная Демократическая Республика

РУБРИКА ГРНТИ: 27.47.19 Исследование операций,
28.17.00 Теория моделирования,
45.29.00 Электрические машины

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Среди отличных стратегий в управлении крутящим моментом асинхронных двигателей выделяется прямое регулирование крутящего момента. Этот метод управления позволяет напрямую управлять магнитным потоком и электромагнитным моментом без необходимости их разъединения. Однако прямое регулирование крутящего момента, как и любая другая стратегия управления, имеет некоторые недостатки. Основными недостатками этого метода являются работа при переменных частотах переключения, а также электромагнитные колебания вследствие использования гистерезисных регуляторов. Это приводит к увеличению акустического шума, особенно на малых скоростях, а также ухудшению характеристик рулевого управления.

Методы: В целях улучшения производительности прямого регулирования крутящего момента, особенно на низких скоростях, предлагается использовать PID дробного порядка в сочетании с контроллерами нечеткой логики типа 2 для регулирования частоты вращения асинхронного двигателя, управляемого прямым регулированием крутящего момента.

Результаты: Результаты, полученные при использовании предлагаемых регуляторов, показывают заметное улучшение в системе.

Выводы: Результаты данного исследования могут внести вклад в улучшение управления.

Кључеве слова: прямое регулирование крутящего момента (DTC), контроллер нечеткой логики (FLC), контроллер дробного порядка (FO), асинхронный двигатель (IM), анализ БПФ.

Примена фази логичког контролера типа 2 и контролера фракционог реда за регулисање брзине директног управљања моментом силе у индукционом мотору

*Јонс Абделбади Мабрук^а, аутор за преписку,
Башир Моктари^а, Тајиб Алауи^б*

^а Универзитет Аммар Телидји, Одсек за електротехнику,
Лабораторија за проучавање и развој полупроводника и
диелектричних материјала (ЛЕДМАСД),
Лагуат, Народна Демократска Република Алжир

^б Универзитет у Тиарету, Одсек за електротехнику и енергетику
и Лабораторија за инжењерство и рачунарско инжењерство (L2GEGI),
Тиарет, Народна Демократска Република Алжир,

ОБЛАСТ: математика, рачунарске науке, електротехника
КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Међу одличним стратегијама за управљање моментом силе код асинхронних мотора издваја се директно управљање моментом силе. Ова техника омогућава директно управљање магнетним флуksom и електромагнетним моментом силе без потребе да се рездвајају. Такође, директно управљање моментом, као и свака стратегија управљања, има своје недостатке од којих су највећи рад на променљивим прекидачким фреквенцијама, као и електромагнетна таласност услед коришћења регулатора хистерезе. То доводи до погоршања акустичке буке, нарочито при малим брзинама, као и до погоршања перформанси управљања.

Методe: Да би се побољшале перформансе директног управљања моментом, нарочито при малим брзинама, предлаже се коришћење ПИД контролера фракционог реда у комбинацији са фази логичким контролером типа 2, како би се регулисала брзина индукционог мотора контролисаног путем директног управљања моментом.

Резултати: Испитивања која су вршена помоћу предложених регулатора показују да је дошло до побољшања у систему.

Закључак: Предложена решења могу да доведу до бољег управљања.

Кључне речи: директно управљање моментом силе, фази логички контролер, контролер фракционог реда, индукциони мотор, ФФТ.

Paper received on / Дата получения работы / Датум пријема чланка: 14.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 21.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 22.11.2023.

© 2023 The Authors. Published by *Vojnotehnički glasnik / Military Technical Courier*
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / *Vojnotehnički glasnik / Military
Technical Courier*» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / *Vojnotehnički glasnik / Military Technical Courier*
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Evaluation of steel turning by means of probability – based multi - objective optimization with appropriate numbers of attributes

Maosheng Zheng^a, Jie Yu^b

^a Northwest University, School of Chemical Engineering,
Xi'an, People's Republic of China,
e-mail: mszhengok@aliyun.com, **corresponding author**,
ORCID iD:  <https://orcid.org/0000-0003-3361-4060>

^b Northwest University, School of Life Science & Technology,
Xi'an, People's Republic of China,
e-mail: yujie@nwu.edu.cn,
ORCID iD:  <https://orcid.org/0000-0001-6606-5462>

DOI: 10.5937/vojtehg71-42843; <https://doi.org/10.5937/vojtehg71-42843>

FIELD: mathematics, materials

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Turning is a typical machining process. However, an appropriate solution for a concurrent optimization of minimizing surface roughness, minimizing cutting forces and vibrations, and maximizing the material removal rate in turning processes has not been found yet. This article formulates the rule of separating an independent attribute from multiple attributes by using the linear correlation coefficient in the spirit of the cluster analysis first. Moreover, the evaluation of the concurrent optimization of steel turning by means of probability - based multi - objective optimization (PMOO) is taken as an example to show the procedure including the separation of an independent attribute from multiple attributes by using PMOO.

Methods: PMOO is a promising solution for turning processes. It is necessary to have an independent attribute in the evaluation of PMOO to be analogical as an independent event in the view of the probability theory. The separation of an independent attribute from multiple attributes by using the linear correlation coefficient is conducted in the spirit of the cluster analysis. It further assumes that if the linear correlation coefficient of two attributes in the cluster analysis is higher than 0.8, i.e., in case of very strong correlation, then they could be put into one category, and only one of them could be taken as an independent attribute to join the evaluation of PMOO.

Results: The formulation reflects the essence of PMOO and its application in material machining rationally, which opens a new way for solving the

relevant problem. The example of the parameter optimization of steel turning by means of PMOO indicates the rationality of the appropriate solution.

Conclusion: This innovative study has practical significance of making the utilization of PMOO method reasonable by providing a rational rule of separating independent attributes from multiple attributes of PMOO.

Key words: multi – objectives, cluster analysis, independent attributes, linear correlation coefficient, metal turning.

Introduction

Turning is a typical machining process. The number of turning machines is about 30% of all cutting machines in a cutting workshop (Thien Van et al, 2021; Hegde et al, 2022; Yıldız et al, 2023, Nguyen & Vo Thi, 2022).

The surface roughness of machining, cutting forces, vibrations, and the material removal rate (MRR) are usually used as the assessed attributes of quality evaluation for the overall machining process. In order to ensure the minimum value of surface roughness, Taguchi design and the Response Surface Method (RSM) were frequently used to conduct the optimization of cutting parameters such as cutting velocity, feed rate, and cutting depth in the turning process for various materials with minimizing surface roughness, or minimizing cutting forces, or maximizing the MRR, solely (Thien Van et al, 2021; Hegde et al, 2022; Yıldız et al, 2023, Nguyen & Vo Thi, 2022; Irzaev et al, 2021).

However, until now, an appropriate solution for a concurrent optimization of minimizing surface roughness, minimizing cutting forces and vibrations, and maximizing the MRR in turning processes has not been achieved yet (Thien Van et al, 2021; Hegde et al, 2022; Yıldız et al, 2023, Nguyen & Vo Thi, 2022; Irzaev et al, 2021).

Actually, the concurrent optimization of minimizing surface roughness, minimizing cutting forces and vibrations, and maximizing the MRR in turning processes is a typical optimization problem with multiple objectives (attributes); it is essentially focused on the simultaneity of the optimization of multiples objectives.

Probability – based multi – objective optimization (PMOO) is a newly developed approach to conduct the concurrent optimization problem of multiple attributes (objectives). A new idea of preferable probability and its assessment have been put forward (Zheng et al, 2024).

The core content of PMOO is taking the "simultaneous optimization of multiple attributes" from the entire or systematic viewpoint of the

system theory; therefore, a probability - based method was formulated on the basis of the probability theory and the set theory, taking each attribute as an independent event in the subsequent treatment.

The advantages of PMOO are its probabilistic foundation in view of the system theory, rationality and certainty of its solution without any artificial factors, and a simple and convenient algorithm in mathematical treatment, which are obviously superior to other methods of multi-objective optimization such as the Analytic Hierarchy Process (AHP), the Višekriterijumsko KOmpromisno Rangiranje (VIKOR), the Technique of Ranking Preferences by Similarity to the Ideal Solution (TOPSIS), Multi-Objective Optimization (MOO) on the basis of the Ratio Analysis (MOORA) , the Pareto solution, the Grey Relational Analysis (GRA), etc. (Zheng et al, 2024; Salomon, 2019). Besides, this approach is superior regarding simplicity in data processing to other metaheuristics.

The new approach could be employed in many fields involving multiple attributes, including energy planning, economic affairs, operation research, programming problems, material selection, mechanical design, etc. Therefore, PMOO is a promising solution for a concurrent optimization of minimizing surface roughness, minimizing cutting forces and vibrations, and maximizing the MRR of turning processes in view of the system theory (Zheng et al, 2024).

Moreover, from the perspective of the probability theory and the set theory, the intersection of independent events and the joint probability of independent events could be used to characterize the concurrent occurrence of multiple independent events as the concurrent optimization of multiple attributes. In this way, when it allocates each attribute to an independent event, the problem of the simultaneous optimization of multiple attributes becomes "rule - based". However, the allocation of each attribute to an independent event naturally relies on the separation of independent events from multiple attributes such that the PMOO method could be used rationally.

Thus, separating an independent event from multiple attributes is of considerable significance to ensure the appropriate application of the PMOO method in material selection.

While, the cluster analysis could fortunately be employed to conduct the separation of an independent attribute from multiple attributes. By classifying things rationally, problems in the material world could be clarified and understood gradually (Backhaus et al, 2021; Scitovski et al, 2021). In the process of the cluster analysis, the class is often not given in advance, but it needs to be determined according to the characteristics of the observed data, and there is no need to make any assumptions

about the number and structure of classes. In the clustering results, attributes belonging to the same class tend to be similar to each other in a sense, while attributes belonging to different classes tend to be dissimilar. The purpose of the cluster analysis is to classify attributes into several classes according to certain rules. The cluster analysis can be divided into the Q – type cluster analysis and the R – type cluster analysis in accordance with different classification objectives. The Q - type clustering analysis is for samples and the R - type clustering is for performances (Backhaus et al, 2021; Scitovski et al, 2021).

Generally speaking, according to the degree of similarity, attributes (or samples) are classified one by one; closely related classes are clustered into a small taxon, and then gradually expanded, so that the alienated ones are clustered into a large taxon, until all samples (or performances) are clustered, forming a cluster diagram that represents the affinity. Samples (or performances) are classified in accordance with some requirements in turn (Backhaus et al, 2021; Scitovski et al, 2021).

The general viewpoint of classification is that the closer the similarity of attributes is, the closer their similarity coefficient is to 1 or -1 , while the similarity coefficient of unrelated attributes is closer to 0.

Those with higher similarity are classified into one category, and those with higher dissimilarity are classified into different categories. The distance in the variable "space" is the characteristic between the "points". Each sample is regarded as a point in the P -dimensional space, and the distance between the points is measured by some kind of measurement. The points that are closer to each other belong to one category while the points that are farther away belong to different categories.

This paper mainly focuses on separating independent attributes from multiple attributes of PMOO in respect of the R - type cluster analysis rationally, so as to guarantee the appropriate application of the PMOO method in material selection first. The evaluation of steel turning by means of PMOO is presented as an example of the process of separating independent attributes from multiple attributes for subsequent evaluation.

Procedure of separating an independent attribute from multiple attributes in PMOO for material machining by means of the cluster analysis

The formulation of separating an independent attribute from multiple attributes in PMOO for material machining by means of the cluster analysis is as follows:

1. Representative of similarity

As a representative of similarity, the linear correlation coefficient is frequently employed as a branch to identify similarity (Backhaus et al, 2021; Scitovski et al, 2021).

The linear correlation coefficient is defined by

$$r_{jk} = \frac{\sum_{i=1}^m (y_{ij} - u_j) \cdot (y_{ik} - u_k)}{\left[\sum_{i=1}^m (y_{ij} - u_j)^2 \cdot \sum_{i=1}^m (y_{ik} - u_k)^2 \right]^{0.5}} \quad (1)$$

In equation (1), r_{jk} is the linear correlation coefficient which is employed to identify the degree of linear correlation between two attributes y_{ij} and y_{ik} ; u_j is the average value of the j -th attribute and u_k is the average value of the k -th attribute.

Obviously, the linear correlation coefficient is just the right coefficient to reflect the linear proportional relationship between two attribute indexes y_{ij} and y_{ik} ; it is more reasonable to reflect the similarity between samples or attributes; in addition, the linear correlation coefficient also has the invariance of normalization similar to the equation (Backhaus et al, 2021; Scitovski et al, 2021).

2. Rules of separating an independent attribute from multiple attributes

As mentioned previously, in the PMOO method for material selection, allocating each attribute to an independent event depends on differentiating an independent event from multiple attributes through the cluster analysis. This section gives the formulation of separation of an independent attribute from multiple attributes.

In the light of the general rule of the R - type clustering analysis for performance classification and the advantage of the linear correlation coefficient in the cluster analysis, the linear correlation coefficient is employed to formulate the separation of an independent attribute from multiple attributes. The appropriate rules are given in the following steps:

a) Evaluations of the similarity of attributes and classification

The linear correlation coefficient in the cluster analysis is used to characterize the similarity of attribute indexes in the performance classification first.

b) Identification of the attribute category

As for the attribute classification, it further assumes that if the linear correlation coefficient of two attributes in the cluster analysis is higher than 0.8, i.e., in case of very strong correlation, they can be put into one category, and only one of them can be used as an independent attribute to join the evaluation of PMOO while the attributes with the linear correlation coefficient lower than 0.8 in the cluster analysis are considered to be in different categories.

c) Evaluation of an independent attribute in PMOO for material machining

Take each independent attribute to join the evaluation of PMOO for material machining only. Especially, if more attributes than the independent attribute are used to join the evaluation and the analysis of the multi - objective optimization problem, it is equivalent to the increase of the weighting factors of the corresponding attributes.

Application in the optimization of the steel turning parameters

Thien Van et al. reported the results of the multi - objective optimization problem of turning EN 10503 steel by using the VIKOR method (Thien Van et al, 2021). However, the shortcomings of the “closeness” to the “virtual ideal solution” and the additional weighting factor of the VIKOR method remained.

In this article, the multi - objective optimization problem of the turning of EN 10503 steel is re-analyzed by means of PMOO with the cluster analysis rationally. In Thien Van’s research, the cutting velocity n , the feed rate f , the depth of cut t , and the insert nose radius r were chosen as the input parameters with three levels for each parameter. Taguchi's orthogonal array $L_9(3^4)$ was used to conduct the design and experiments, as shown in Table 1. The surface roughness R_a , the cutting force components F_x , F_y , and F_z (in the x, y, and z directions), the vibration component amplitudes A_x , A_y and A_z (in the x, y, and z directions), and the material removal rate (the MRR) were taken as their evaluated attributes (objectives). Their results are given in Table 2.

Table 1 – Experiment design with $L_9(3^4)$
 Таблица 1 – Планирование эксперимента с $L_9(3^4)$
 Табела 1 – Дизајн експеримента са $L_9(3^4)$

No.	Coded value				Actual value			
	n	f	t	r	n (rev/min)	f (mm/rev)	t (mm)	r (mm)
1	1	1	1	1	460	0.08	0.20	0.4
2	1	2	2	2	460	0.194	0.35	0.6
3	1	3	3	3	460	0.302	0.50	1.2
4	2	1	2	3	650	0.08	0.35	1.2
5	2	2	3	1	650	0.194	0.50	0.4
6	2	3	1	2	650	0.302	0.20	0.6
7	3	1	3	2	910	0.08	0.50	0.6
8	3	2	1	3	910	0.194	0.20	1.2
9	3	3	2	1	910	0.302	0.35	0.4

Table 2 – Experimental results with the $L_9(3^4)$ design
 Таблица 2 – Результаты эксперимента разработки $L_9(3^4)$
 Табела 2 – Резултати експеримента са дизајном $L_9(3^4)$

No.	Ra (μm)	F _x (N)	F _y (N)	F _z (N)	A _x (μm)	A _y (μm)	A _z (μm)	MRR (mm ³ /s)
1	0.840	85.2740	24.9800	107.4400	2.385	5.3594	5.5826	7.948
2	0.605	166.2340	47.5420	230.3210	3.9816	8.5019	9.0195	54.471
3	0.644	563.7300	153.285	965.2270	5.9601	12.1603	16.2276	178.071
4	1.122	219.2030	64.0220	335.7370	5.9392	8.8440	13.9882	57.823
5	0.669	152.2660	38.5830	191.5410	4.3123	7.6545	9.3600	42.398
6	0.643	175.3230	44.1470	211.6830	5.0853	9.9639	12.5087	31.447
7	0.621	191.0840	51.7270	300.1620	4.4647	7.4923	10.1177	60.009
8	0.729	212.9260	59.1170	307.8790	5.8284	8.4602	14.1956	33.694
9	0.675	124.9690	40.5450	164.2060	6.2633	10.1637	15.2682	38.130

Let us study the similarity of attributes (objectives) first.

The similarity analysis of these data shows that there is a strong linear correlation among the cutting force components of F_x , F_y and F_z , and among the vibration component amplitudes of A_x , A_y and A_z of the turning process.

The linear correlation coefficients of F_x vs F_y and F_x vs F_z are $r_{F_x F_y} = 99.72\%$ and $r_{F_x F_z} = 99.64\%$, respectively, see Figure 1. The linear correlation coefficients of A_x vs A_y and A_x vs A_z are $r_{A_x A_y} = 97.77\%$ and $r_{A_x A_z} = 80.39\%$, respectively, see Figure 2.

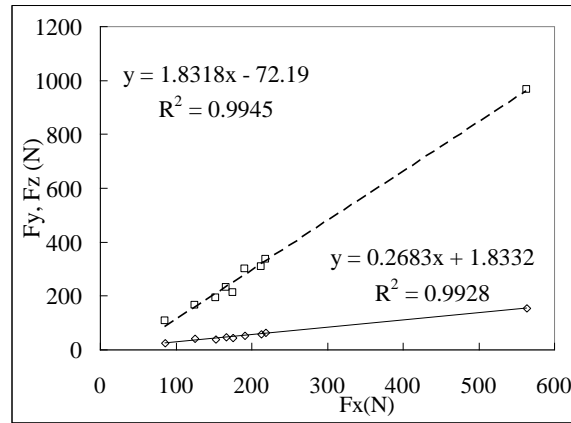


Figure 1 – Linear correlations of F_x vs F_y and F_x vs F_z
 Рис. 1 – Линейные корреляции между F_x и F_y , а также между F_x и F_z
 Слика 1 – Линеарне корелације између F_x и F_y , као и између F_x и F_z

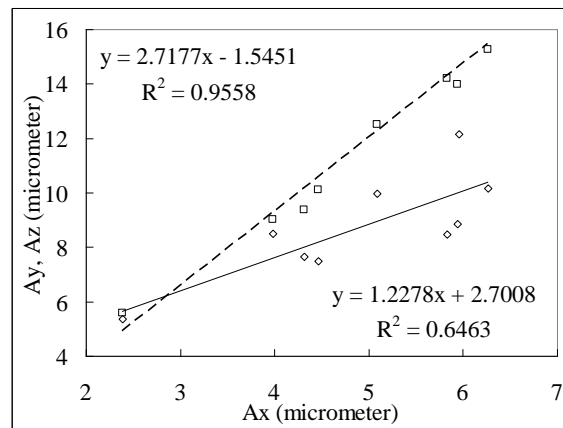


Figure 2 – Linear correlations of A_x vs A_y and A_x vs A_z
 Рис. 2 – Линейные корреляции между A_x и A_y , а также между A_x и A_z
 Слика 2 – Линеарне корелације између A_x и A_y , као и између A_x и A_z

As stated in the previous section, since there is a strong linear relationship among F_x , F_y and F_z , only one component of them can be employed as the independent attribute to join the evaluation of PMOO. The same applies for A_x , A_y and A_z . Therefore, F_x and A_x are taken as the independent attributes to join the evaluation of PMOO.

Finally, the surface roughness R_a , the cutting force components F_x , the vibration component amplitudes A_x , and the material removal rate MRR were taken as the actual evaluated independent multiple attributes.

Furthermore, in accordance with PMOO, the *MRR* belongs to the beneficial performance index to join the evaluation of partial preferable probability while R_a , F_x , and A_x , belong to the unbeneficial performance index to join the evaluation of their partial preferable probabilities.

The assessed consequences are shown in Table 3 which indicates that experiment No. 2 has the highest total preferable probability P_t at the first glance, followed by experiment No. 7.

However, the optimal configuration of Thien Van et al. is just experiment No. 7 which obviously exhibits poorer responses than experiment No. 2 integrally (see the following detail for comparison).

As for experiment No. 2, the responses of the surface roughness, the cutting force and the vibration component amplitudes (in the X, Y, and Z directions), and the material removal rate (MRR) of experiment No. 2 are 0.605 μm , 166.2340 N, 47.5420 N, 230.3210 N, 3.9816 μm , 8.5019 μm , 9.0195 μm , and 54.471 mm^3/s , respectively, while in experiment No. 7, the responses of the surface roughness, the cutting force and the vibration component amplitudes (in the X, Y, and Z directions), and the material removal rate (MRR) are 0.621 μm , 191.084 N, 51.727 N, 300.162 N, 4.465 μm , 7.492 μm , 10.118 μm , and 60.009 mm^3/s , respectively.

Furthermore, the range analysis can be conducted for the total preferable probability P_t to perform successive optimization, as shown in Table 4. It indicates that the order of impact of the input variables is $r > t > f > n$, and the subsequent optimal configuration will be $r_2t_3f_2n_3$.

Table 3 – Assessed results of preferable probability and ranking
Таблица 3 – Полученные результаты предпочтительной вероятности и ранжирования

Табела 3 – Добијени резултати пожељне вероватноће и рангирање

No.	P_{Ra}	P_{F_x}	P_{A_x}	P_{MRR}	$P_t \times 10^4$	Rank
1	0.0986	0.1427	0.1863	0.0158	0.4135	9
2	0.1247	0.1222	0.1388	0.1081	2.2875	1
3	0.1204	0.0216	0.0800	0.3533	0.7344	6
4	0.0673	0.1088	0.0806	0.1147	0.6767	8
5	0.1176	0.1258	0.1290	0.0841	1.6051	3
6	0.1205	0.1199	0.1060	0.0624	0.9558	4
7	0.1230	0.1159	0.1245	0.1191	2.1123	2
8	0.1110	0.1104	0.08309	0.0669	0.6870	7
9	0.1170	0.1327	0.0710	0.0757	0.8329	5

Table 4 – Results of the range analysis
 Таблица 4 – Результаты анализа ранжирования
 Табела 4 – Резултати анализе рангирања

Level	n	f	t	r
1	1.1451	1.0675	0.6854	0.9505
2	1.0792	1.5265	1.2657	1.7852
3	1.2107	0.8410	1.4839	0.6994
Range	0.1315	0.6855	0.7985	1.0858
Order	4	3	2	1
Optimum	n ₃	f ₂	t ₃	r ₂

Conclusion

By using the linear correlation coefficient as similarity of the cluster analysis to conduct the classification of attributes, the separation of an independent attribute from multiple attributes could be performed rationally for the assessment of PMOO for material machining. In the evaluation, only each independent attribute could join the evaluation of PMOO. If more attributes than an independent attribute are used to join the analysis and the evaluation of multi - objective optimization problem, it is equivalent to the increase of the weighting factors of the corresponding attributes. The example of parameter optimization of steel turning by means of PMOO indicates the rationality of the appropriate solution.

References

- Backhaus, K., Erichson, B., Gensler, S., Weiber, R. & Weiber, T. 2021. *Multivariate Analysis: An Application-Oriented Introduction*. Wiesbaden: Springer Fachmedien. Available at: <https://doi.org/10.1007/978-3-658-32589-3>.
- Hegde, A., Hindi, J., Gurumurthy, B.M., Sharma, S. & Ki, A. 2022. Machinability study and optimization of tool life and surface roughness of ferrite: Bainite dual phase steel. *Journal of Applied Engineering Science*, 20(2), pp.358-364. Available at: <https://doi.org/10.5937/jaes0-32927>.
- Irzaev, G., Kanaev, M. & Isalova, M. 2021. Selection of the preferred design for manufacturability by constructing the Pareto tuple. *Journal of Applied Engineering Science*, 19(2), pp.275-281. Available at: <https://doi.org/10.5937/jaes0-26922>.
- Nguyen, H.S., & Vo Thi, N.U. 2022. Multi-Objective Optimization in Turning Process Using RIM Method. *Applied Engineering Letters: Journal of Engineering and Applied Sciences*, 7(4), pp.143-153. Available at: <https://doi.org/10.18485/aeletters.2022.7.4.2>.

Salomon, S. 2019. *Active Robust Optimization: Optimizing for Robustness of Changeable Products*. Cham: Springer. Available at: <https://doi.org/10.1007/978-3-030-15050-1>.

Scitovski, R., Sabo, K., Martínez-Álvarez, F. & Ungar, Š. 2021. *Cluster Analysis and Applications*. Cham: Springer. Available at: <https://doi.org/10.1007/978-3-030-74552-3>.

Thien Van, N., Tien Hoang, D., Trung Duc, D. & Nguyen, N.-T. 2021. Multi-objective optimization of turning process using a combination of Taguchi and VIKOR methods. *Journal of Applied Engineering Science*, 19(4), pp.868-873. Available at: <https://doi.org/10.5937/jaes0-29654>.

Yildiz, A., Uğur, L. & Parlak, I.E. 2023. Optimization of the Cutting Parameters Affecting the Turning of AISI 52100 Bearing Steel Using the Box-Behnken Experimental Design Method. *Applied Sciences*, 13(1), art.number:3. Available at: <https://doi.org/10.3390/app13010003>.

Zheng, M., Yu, J., Teng, H., Cui, Y. & Wang, Y. 2024. *Probability-Based Multi-objective Optimization for Material Selection, 2nd Edition*. Singapore: Springer. Available at: <https://doi.org/10.1007/978-981-99-3939-8>.

Оценка точения стали, основанная на вероятности многоцелевой оптимизации с соответствующим количеством атрибутов

Маошенг Чжэн^а, Джи Юю^б

Северо-западный политехнический университет,
г. Сиань, Народная Республика Китай

^а факультет химической инженерии, **корресподент**

^б факультет естественных наук и технологий

РУБРИКА ГРНТИ: 27.47.00 Математическая кибернетика,
81.09.00 Материаловедение

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Точение – это типичный процесс механической обработки металла. Однако подходящее решение по одновременной оптимизации минимизации шероховатости поверхности, минимизации силы резания и вибраций, максимального увеличения скорости удаления стружки в течение точения пока не найдено. В данной статье на основании кластерного анализа сформулировано правило выделения независимого атрибута из множества атрибутов с использованием коэффициента линейной корреляции. Помимо того, на примере оценки одновременной оптимизации токарной обработки стали с помощью многокритериальной вероятностной оптимизации (РМОО) продемонстрирована процедура выделения независимого атрибута из множества атрибутов с помощью РМОО.

Методи: РМОО является перспективным решением в токарной обработке. В оценке РМОО необходимо присутствие независимого атрибута, аналогичного независимому событию в теории вероятностей. Выделение независимого атрибута из множества атрибутов с помощью коэффициента линейной корреляции осуществляется на основании кластерного анализа. Далее предполагается, что если коэффициент линейной корреляции двух признаков при кластерном анализе превышает 0,8, т.е. в случае очень высокой корреляции, то их можно отнести к одной категории и только один из них может рассматриваться как независимый атрибут в оценке РМОО.

Результаты: Формулировка отражает суть РМОО и ее применения в механической обработке материалов, что открывает новые возможности для решения важной задачи. Пример оптимизации параметров точения стали с помощью РМОО свидетельствует о рациональности соответствующего решения.

Выводы: Это инновационное исследование имеет практическое значение, поскольку оно подчеркивает удобство использования методов РМОО, предоставляя рациональное правило для выделения независимых атрибутов из множества атрибутов РМОО.

Ключевые слова: многоцелевой подход, кластерный анализ, независимые атрибуты, коэффициент линейной корреляции, токарная обработка металла.

Евалуација окретања челика помоћу вишекритеријумске оптимизације на бази вероватноће са одговарајућим бројем атрибута

Маошенг Ценг^а, Ђаи Ју^б

Универзитет Северозапад, Сијан, Народна Република Кина

^а Факултет хемијског инжењерства, **аутор за преписку**

^б Факултет природних наука и технологија

ОБЛАСТ: математика, материјали

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Окретање је типичан процес машинске обраде. Међутим, још није пронађено адекватно решење за истовремену оптимизацију свођења храпавости, сила резања и вибрација на најмању могућу меру уз највећу брзину уклањања материјала при процесу окретања. У овом раду формулише се правило за одвајање независног атрибута од вишеструких атрибута коришћењем

коэффициента линеарне корелације, најпре на основу кластер анализе. Штавише, на примеру евалуације истовремене оптимизације окретања челика помоћу вишекритеријумске оптимизације на бази вероватноће (РМОО) приказан је поступак одвајања независног атрибута од вишеструких атрибута њеним коришћењем.

Методи: У прецесима окретања РМОО би могла бити добро решење. Неопходно је да постоји независни атрибут у евалуацији РМОО, слично независном догађају у теорији вероватноће. Одвајање независног атрибута од вишеструких атрибута помоћу коэффициента линеарне корелације врши се у складу са кластер анализом. Претпоставља се да ако је коэффициент линеарне корелације два атрибута у кластер анализи већи од 0,8, односно ако је корелација веома висока, тада они могу бити стављени у једну категорију, а само један од њих може, као независни атрибут, да се придружи евалуацији РМОО.

Резултати: Формулација одсликава суштину РМОО и њену примену у машинској обради материјала на рационалан начин, што отвара нове могућности за решавање битног проблема. Пример оптимизације параметара окретања челика помоћу РМОО указује на рационалност одговарајућег решења.

Закључак: Ова иновативна студија има практичан значај, јер истиче погодност коришћења метода РМОО, представљајући рационално правило за одвајање независних атрибута од вишеструких атрибута РМОО.

Кључне речи: вишекритеријумски, кластер анализа, независни атрибут, коэффициент линеарне корелације, окретање метала.

Paper received on / Дата получения работы / Датум пријема чланка: 14.02.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 24.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 25.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons licencem (<http://creativecommons.org/licenses/by/3.0/rs/>).



Deep learning channel estimation for 5G wireless communications

Mohammed Zouaoui M. Laidouni^a,
Taki-eddine Ahmed A. Benyahia^b, Boban Z. Pavlović^c,
Salem-Bilal B. Amokrane^d, Touati B. Adli^e

University of Defence in Belgrade, Military Academy, Department of Telecommunications and Informatics, Belgrade, Republic of Serbia,

^a e-mail: mohammedz.laidouni@gmail.com, **corresponding author**,
ORCID iD: <https://orcid.org/0009-0008-6042-0513>

^b e-mail: benyahia.taki@gmail.com,
ORCID iD: <https://orcid.org/0009-0006-6025-6915>

^c e-mail: bobanpav@yahoo.com,
ORCID iD: <https://orcid.org/0000-0002-5476-7894>

^d e-mail: amokranesalembilal@gmail.com,
ORCID iD: <https://orcid.org/0009-0009-7588-5708>

^e e-mail: adlitouati94@gmail.com,
ORCID iD: <https://orcid.org/0009-0000-2673-6954>

DOI: 10.5937/vojtehg71-46057; <https://doi.org/10.5937/vojtehg71-46057>

FIELD: computer sciences, telecommunications

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: In recent years, deep learning techniques, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable performance in 5G communication systems by significantly improving the accuracy of channel estimation compared to conventional methods. This article aims to provide a comprehensive review of the existing literature on CNN-based channel estimation techniques, as well as to enhance the state-of-the-art CNN-based channel estimation methods by proposing a novel method called VDSR (Very Deep Super Resolution), inspired by Image Super-Resolution techniques.

Methods: To evaluate the effectiveness of various approaches, we conduct a comprehensive comparison considering different scenarios, including low Signal-to-Noise Ratio (SNR) and high SNR, as well as Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) scenarios. Through this comparative analysis, we assess the performance of the existing methods and highlight the advantages offered by the proposed VDSR-based technique.

Results: Our findings reveal a significant potential of CNN-based channel estimation in 5G communication systems, with the VDSR method demonstrating a consistent performance across all scenarios. This re-

search contributes to the advancement of channel estimation techniques in 5G networks, paving the way for enhanced wireless communication systems with improved reliability.

Conclusion: The VDSR architecture demonstrates remarkable adaptability to different types of channels, which results in achieving requested performances for all analyzed SNR values.

Key words: deep learning, CNN, 5G communication systems, very deep super resolution.

Introduction

With the advent of 5G communication technology, the demand for high-speed, low-latency, and reliable wireless communication is increasing exponentially (Albreem, 2015). The key enabler for 5G communication is accurate channel estimation, which refers to the process of estimating the wireless channel parameters between the transmitter and the receiver (Morocho-Cayamcela et al., 2019). Accurate channel estimation is critical for improving the performance of 5G communication systems, including data rates, spectral efficiency, and reliability (Ma et al., 2015). In recent years, convolutional neural networks (CNNs) have emerged as a promising technique for channel estimation in 5G communication systems (James et al., 2011). CNNs are powerful deep learning algorithms that can learn and extract complex features from large amounts of data. By leveraging the power of CNNs, channel estimation in 5G communication systems can achieve high accuracy, robustness, and efficiency (Ye et al., 2017; Kaur et al., 2021).

This work aims to investigate the effectiveness of CNN-aided channel estimation in 5G communication systems. Specifically, through exploring the existing literature on CNN-aided channel estimation, a novel architecture for CNN-based channel estimation is being proposed, and the performance of the suggested approach will be assessed through simulations.

The rest of this paper is structured as follows. Section 2 describes the 5G new radio SISO-OFDM system. Section 3 provides a literature review on CNN-aided channel estimation and describes the architecture used for our method. Section 4 presents the results and analysis of the simulation. Section 5 discusses the implications of our findings and provides recommendations for future research. Finally, Section 6 presents the conclusions of this work.

5G new radio SISO-OFDM system

The focus of this paper is on analyzing a SISO-OFDM system that employs a single antenna at both the transmitter and receiver. This system is depicted in the diagrams shown in Figure 1 and Figure 2, and the channel model is constructed accordingly.

Transmitter

Figure 1 shows the architecture of the transmitter, which involves converting serial binary input bits (a sequences of zeros and ones) into a parallel form. Based on the chosen modulation scheme, the binary bits are then mapped onto symbols, with each symbol being $K - dimensional$ and the binary bits selecting one of M constellation points. Typically, K is 2, and M is determined by the modulation scheme chosen at the higher layer. Additionally, intermittent pilot symbols are inserted among the modulated symbols, which serve as a reference for channel estimation and are also recognizable to the receiver.

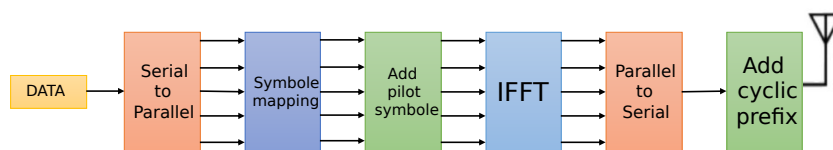


Figure 1 – Block diagram for the OFDM transmitter model

Рис. 1 – Блок-схема модели передатчика OFDM

Слика 1 – Блок-дијаграм за модел OFDM предајника

Let $X_S \in \{X_m, X_p\}$ where $X_m \in \{s_0, s_1, s_2, \dots, s_{M-1}\}$ is the modulated symbol selected by $\log_2 M$ binary input bits and $X_p \in \{p_0, p_1, p_2, \dots, p_{K-1}\}$ are pilot symbols respectively. Equation 1 in the digital domain is Inverse Discrete Fourier Transform operation which can be efficiently realized by the Inverse Fast Fourier transform (IFFT) before adding the cyclic prefix (Banerjee et al., 2022).

$$x_s(n) = \frac{1}{N_s} \sum_{k=1}^{N_s-1} X_s(k) \exp(j2\pi \frac{k}{N_s} n). \quad (1)$$

where N_S is the IFFT length. A parallel to serial converter is present after the IFFT operation to serialize the output.

Receiver

Figure 2 shows the architecture of the receiver, which includes a process for estimating the timing of the received signal.

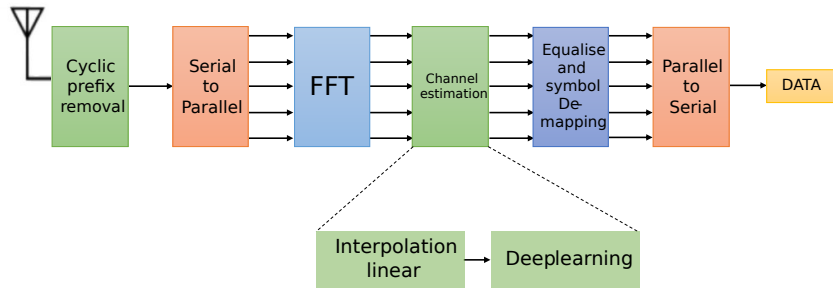


Figure 2 – Block diagram for the OFDM receiver model
 Рис. 2 – Блок-схема модели приемника OFDM
 Слика 2 – Блок-дијаграм за модел OFDM пријемника

This process involves cross-correlating the input waveform with a reference waveform and compensating for any timing offset. Once the timing offset has been accounted for, the cyclic prefix is removed from the received waveform. If Y_S is the received OFDM symbol and y_S is the output of the FFT operation, then y_S can be expressed in the following manner (Banerjee et al., 2022):

$$y_s(n) = \frac{1}{N_s} \sum_{l=1}^{N_s-1} Y_s(l) \exp(-j2\pi \frac{l}{N_s} n) \quad (2)$$

The pilot samples, which are located at predetermined positions, are extracted from the signal and utilized to estimate the channel characteristics. This channel estimation information is then used to equalize the output $y_S(n)$. After equalization, the signal is demodulated based on the modulation scheme that was employed at the transmitter.

Signal model

In an OFDM system (Soltani et al., 2019), for the k_{th} time slot and the i th subcarrier, the input-output relationship is represented as:

$$Y_{i,k} = H_{i,k}X_{i,k} + Z_{i,k} \quad (3)$$

Considering an OFDM subframe of size $N_S N_D$, the time slot index k is between $[0, N_D - 1]$, and the range of the subcarrier index i is $[0, N_S - 1]$.

$Y_{i,k}$: The received signal

$X_{i,k}$: Transmitted OFDM symbol

$Z_{i,k}$: white Gaussian noise

$H_{i,k}$: the (i, k) element of $H \in C^{N_S N_D}$. H represents time-frequency response of the channel for all subcarriers and time slots.

5G data architecture

The physical layer of the 5G NR is based on resource blocks allowing the NR physical layer to adapt to various spectrum allocations. A resource block spans 12 subcarriers with a given sub-carrier spacing. A radio frame has a duration of 10 ms and consists of 10 sub-frames with a sub-frame duration of 1ms as shown in figure 3 . A sub-frame is formed by 1 or multiple slots each having 14 adjacent symbols (a variable number of OFDM symbols per subframes, different from LTE) (3GPP. 2018).

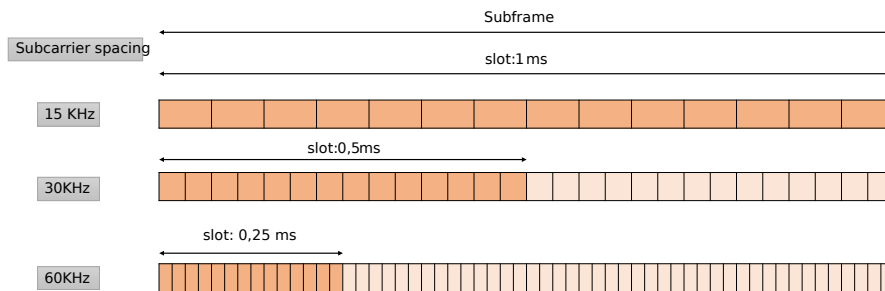


Figure 3 – Sub-frame architecture in 5G
Рис. 3 – Подкадровая архитектура в 5G
Слика 3 – Архитектура подоквира у 5G

In 5G NR, the pilot symbols are referred to as demodulation reference symbols (DMRS) and this is used by the receiver for radio channel estimation. The DMRS symbols are uniformly placed within sub-carriers as shown in figure 4. We assume the DMRS symbols used in the 3GPP specification (3GPP. 2020a).

Figure 4 shows the DM-RS pattern and frequency for type 1 and type 2. Type 1 on the left corresponds to every other resource element in the frequency being occupied by a DM-RS symbol. Type 2 on the right shows two consecutive resource elements occupied by the DM-RS symbols out of

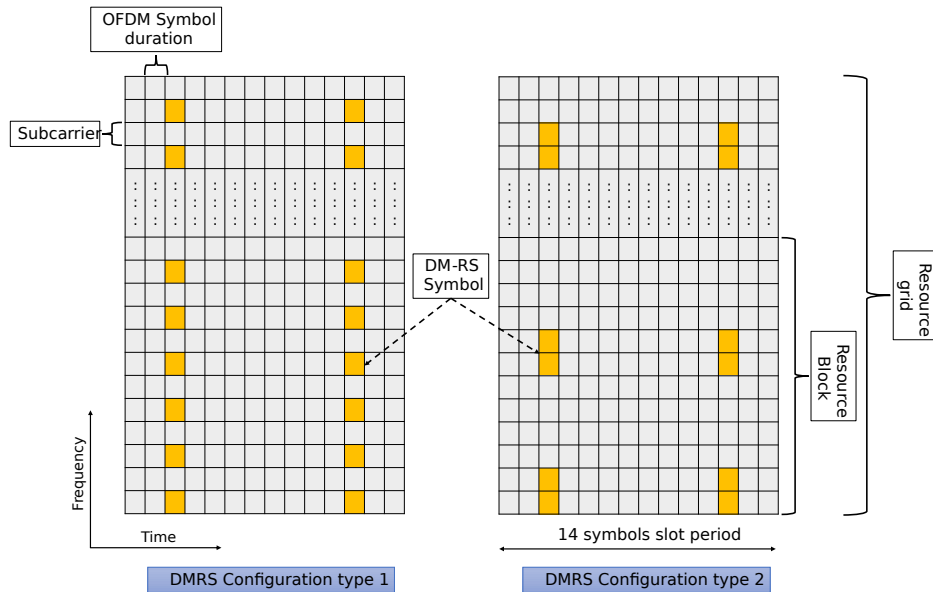


Figure 4 – Representational figure of the distribution of DM-RS
 Рис. 4 – Репрезентативное изображение распределения DM-RS
 Слика 4 – Репрезентативни приказ дистрибуције DM-RS

each group of six resource elements. Therefore, type 1 has a denser occupancy at 50% of the resource estimates, versus one-third of the resource elements for type 2. On the other hand, you can only have two such columns of type 1 DM-RS, whereas there can be three different sets of type 2 DM-RS as there are two more possible positions for a set of two DM-RS in each group of six resource elements. This means that type 2 supports a larger number of orthogonal signals, which is more suitable for multi-user MIMO. These two types correspond to a trade-off between density and frequency and the number of orthogonal DM-RS sequences supported.

Channel model

In wireless communication channels, the signal transmitted from a base station to user equipment not only includes a direct line-of-sight (LOS) component, but also other components that are reflected off scatterers, leading to a multipath propagation environment. Each path of the signal experiences different amounts of attenuation and delay (Wang et al., 2018). The channel's impulse response can be expressed as:

$$h(t) = \sum_{i=0}^{L-1} \alpha_i \delta(\tau - t_i), \quad (4)$$

where a_i is the attenuation and t_i is the delay in the i_{th} path.

Tap Delay Line models

In TDL models, the channel impulse response (CIR) is represented by a linear finite impulse response (FIR) filter. Each tap of the TDL model is composed of several multipath component (MPCs) with non-resolvable delays. Tap weights are modeled by a random process with amplitudes following Rayleigh, Rician, or Weibull distributions (Wang et al., 2018).

A TDL (Tap Delay Line) profile in 5G communication represents a specific channel model that simulates the characteristics of radio wave propagation in a wireless communication system. Three TDL models, namely TDL-A, TDL-B and TDL-C, are constructed to represent three different channel profiles for NLOS while TDL-D and TDL-E are constructed for LOS (3GPP. 2020b).

CNN-aided channel estimation

In recent times, there has been a significant surge in interest in channel estimation techniques based on deep learning. This is due to their ability to adapt and learn from data, as opposed to conventional estimation techniques that rely on a model-based approach.

A convolutional neural network (CNN) approach is chosen because the channel estimation problem can be modelled as an image-processing problem (Banerjee et al., 2022; Soltani et al., 2019; Gizzini et al., 2021). The CNN-based deep learning approach has proven to be efficient for handling image processing problems as it keeps the number of parameters in weight matrix less in comparison to a fully connected neural network model by making use of parameter sharing and sparsity of connections.

Recently, the channel estimation in OFDM systems has been approached using a deep learning-based framework, where the time-frequency grid of the channel response is represented as a 2D-image that is only available at the pilot positions. (Soltani et al., 2019) presented a deep learning-based framework for channel estimation in OFDM systems,



which proposed an image super-resolution (SRCNN) and image denoising (DnCNN) algorithms to estimate the channel. In (Banerjee et al., 2022) a CNN model for Over-the-Air channel estimation has been applied, and the model is proposed by Matlab.

In this paper, we present a novel method for channel estimation that utilizes a very deep convolutional network inspired by VGG-net used for ImageNet classification; the method was proposed by (Kim et al., 2016) and presents a highly accurate single-image super-resolution (SR) technique. The next sections will provide detailed explanations of the three methods.

Method 1: channel estimation using super-resolution (SRCNN) and denoising techniques

The method treats the channel grid with several pilots as a low-resolution (LR) image and aims to estimate the high-resolution (HR) channel. To achieve this, the framework models the channel response as a super-resolution image problem (Soltani et al., 2019).

The channel grid estimation is performed using two phases. In the first phase, the image super-resolution (SR) CNN-based (Convolutional Neural Network) algorithms (Dong et al., 2015), SRCNN, are implemented to increase the resolution of the low-resolution (LR) input. The schema for the CNN-based (Convolutional Neural Network) algorithms is shown in Figure 5.

In the second phase, an image restoration (IR) method based on CNN (Figure 6) is utilized to eliminate the noise effects and improve the quality of the estimated channel grid (Zhang et al., 2017).

Network architecture for SRCNN and DnCNN

The SRCNN technique involves utilizing an interpolation technique to estimate the high-resolution image (channel) values initially, and then refining the resolution by employing a three-layer convolutional network as shown in Figure 7:

- The first convolutional layer uses 64 filters of size 9×9 followed by ReLu activation,
- The second layer uses 32 filters of size 1×1 followed by ReLu activation.

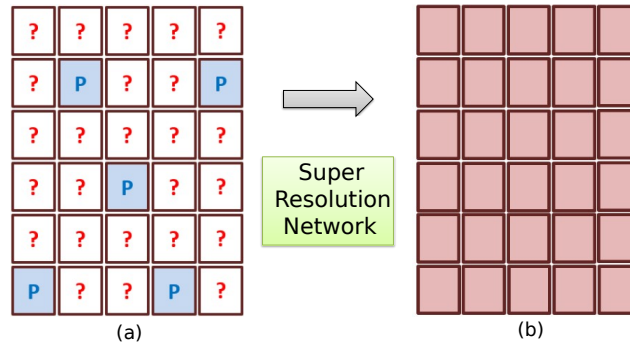


Figure 5 – Super-resolution based CNN, (a) 2D-image which is known only at the pilot positions, (b) estimated channel as a high-resolution
 Рис. 5 – CNN на основе сверхразрешения, (a) 2D-изображение, известное только на позициях пилота, (b) оцениваемый канал высокого разрешения
 Слика 5 – CNN заснован на супер резолуцији, (a) 2D-слика која је позната само на пилот позицијама, (b) процењени канал високе резолуције

- The final layer uses only one filter of size 5×5 to reconstruct the grid channel.

The DnCNN technique in Figure 8 is a residual-learning based network composed of 20 convolutional layers:

- The first layer uses 64 filters of size $3 \times 3 \times 1$ followed by a ReLU,
- Each of the succeeding 18 convolutional layers uses 64 filters of size $3 \times 3 \times 64$ followed by batch-normalization and ReLU, and
- The last layer uses one $3 \times 3 \times 64$ filter to reconstruct the output.

Method 2: channel estimation using a regression method

The approach used for channel estimation is the same as the first method; the channel estimation problem was considered as an image processing problem by viewing the resource grid as a 2D image. A regression method based on deep learning is used in (Banerjee et al., 2022) to estimate a perfect channel. The input to the deep learning model is the LS channel estimated data and the CNN model can be trained against a perfect channel estimate as a reference, based on the statistical information available. CNN operates by applying convolution operations between images and kernels of different sizes to extract feature information. This process occurs in a multilayered system where the output of the convolution opera-

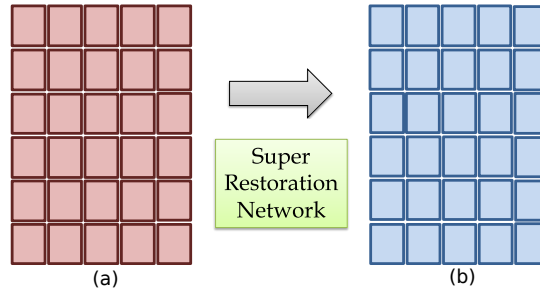


Figure 6 – Denoising based CNN, (a) estimated channel which is considered as a noised image, (b) estimated channel

Рис. 6 – CNN на основе шумоподавления, (a) оценочный канал, который рассматривается как зашумленное изображение, (b) оценочный канал
 Слика 6 – CNN заснован на смањењу шума, (a) процењени канал који се сматра сликом са шумом, (b) процењени канал

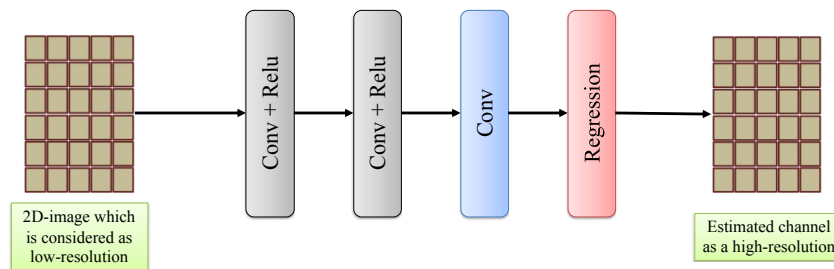


Figure 7 – SRCNN architecture
 Рис. 7 – Архитектура SRCNN
 Слика 7 – Архитектура SRCNN

tion is passed through an activation function, which is a non-linear function that transforms data. In regression problems, the final output layer is a regression layer that calculates the half-mean-squared-error loss. Finally, an optimization function is used to optimize the multilayered system, and the choice of optimization function is determined by the user.

Network architecture for the regression technique

The CNN model consists of 5 hidden layers as shown in Figure 9, where the first four hidden layers are associated with a ReLU activation function.

The fifth layer is associated only with the regression layer, as in regression problems the CNN output does not require an activation function.

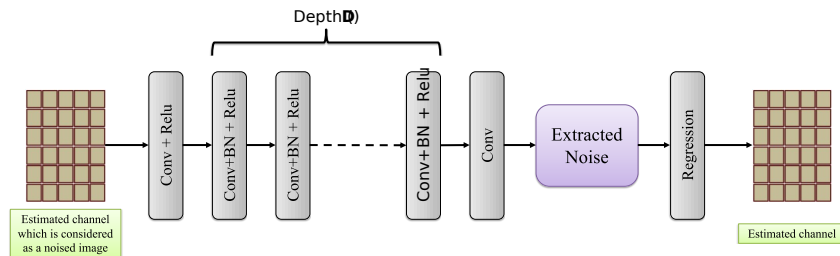


Figure 8 – DnCNN architecture
 Рус. 8 – Архитектура DnCNN
 Слика 8 – Архитектура DnCNN

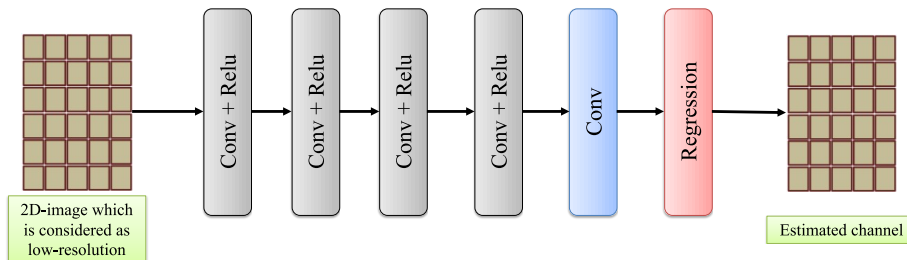


Figure 9 – Regression technique architecture
 Рус. 9 – Архитектура метода регрессии
 Слика 9 – Архитектура технике регресије

The layers are ordered as follows:

- The first convolutional layer uses 64 filters of size 9×9 followed by ReLu activation,
- Each of the succeeding 2 convolutional layers uses 64 filters of size 5×5 followed by ReLu activation,
- The fourth layer uses 32 filters of size 5×5 followed by ReLu activation, and
- The final layer uses only one filter of size 5×5 followed by the regression layer to reconstruct the grid channel.

Method 3: channel estimation using Very Deep Convolutional Networks

The channel estimation problem in this method was also modelled as an image-processing problem, the main difference being that this technique

is using a very deep convolutional network to improve the performance. The SRCNN technique failed to create deeper models for super resolution with superior performance. However, (Kim et al., 2016) presented a method (VDSR: Very Deep Super-Resolution) that utilizes a very deep convolutional network inspired by VGG-net used for ImageNet classification, and it is found that increasing the depth significantly boosts the estimation performances. Given that VDSR shows a highly accurate single-image super-resolution, we want to apply this technique in the channel estimation problem.

Network architecture for VDSR

The VDSR (Kim et al., 2016) technique uses a very deep convolutional network inspired by Simonyan and Zisserman (Simonyan & Zisserman, 2014). The network structure cascades a pair of layers (convolutional and nonlinear) repeatedly. An interpolated low-resolution (CLR) channel goes through the layers and transforms into a high-resolution (HR) channel. The network predicts a residual image and the addition of CLR and the residual gives the desired output.

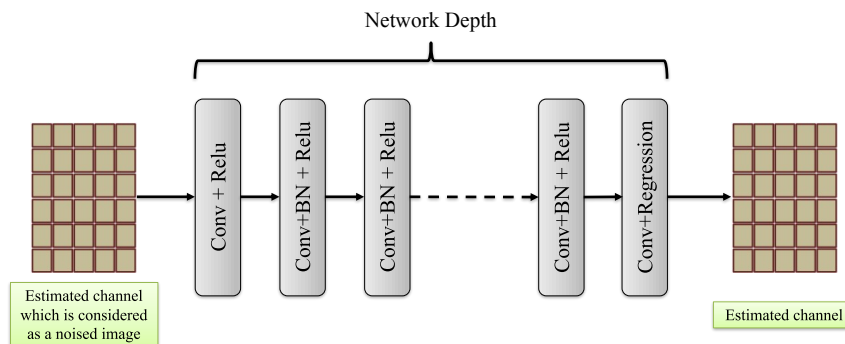


Figure 10 – VDSR architecture
 Рис. 10 – Архитектура VDSR
 Слика 10 – Архитектура VDSR

The VDSR architecture, depicted in Figure 10, consist of 20 layers where layers except the first and the last, are of the same type:

- The first layer operates on the input grid channel,
- Each of the 18 convolutional layers uses 64 filters of size $3 \times 3 \times 64$ followed by ReLU, and

- The last layer, used for grid channel reconstruction, consists of a single filter of size $3 \times 3 \times 64$ followed by the regression layer.

Results and discussion

In this section, all the networks introduced in Section 3 were trained. Following that, the Mean Squared Error (MSE) was evaluated across a range of Signal-to-Noise Ratios (SNRs). The setup involves a single antenna as both the transmitter and the receiver. The 5G Toolbox in Matlab was used for the channel modeling and pilot transmission. The training, testing, and validation sets comprised 40000, 5000, and 5000 channels respectively.

For the purpose of creating test scenarios, a slot period of resource grid consisting of 51 resource blocks was selected to form PDSCH data, forming a matrix of resource elements with dimensions 612 by 14. In order to map the pilots, a slot-wise type A mapping solution was adopted with the DM-RS symbol position set to 2. Furthermore, a single DM-RS symbol was introduced, featuring an additional position of 1. It is worth noting that these parameters and decisions were made in accordance with the rigorous guidelines set forth by the 3GPP standard (3GPP. 2020b).

The parameters used for data generation are presented in Table 1. During this process, a sub-carrier spacing of 30 kHz was maintained, and the actual data symbols were set to zero. Instead, only the DM-RS symbols were embedded in the data as displayed in Figure 11. For the data transmission, a repeated transmission approach was employed. This involved looping through the data of a single slot period, which lasts 0.5 ms. By repeating the transmission within this time frame, the integrity and continuity of the data were effectively maintained. Finally, the collected data was partitioned into the training, validation, and test sets in order to train the CNN models.

Training CNN based channel models

The performance of the neural network-based channel estimation methods relies on the SNR value. Ideally, the weights of the neural network should be optimized for each SNR value to achieve the best performance. However, in practice, this approach is not feasible since the SNR value is continuous, and retraining the network for every possible SNR value is computationally intensive.

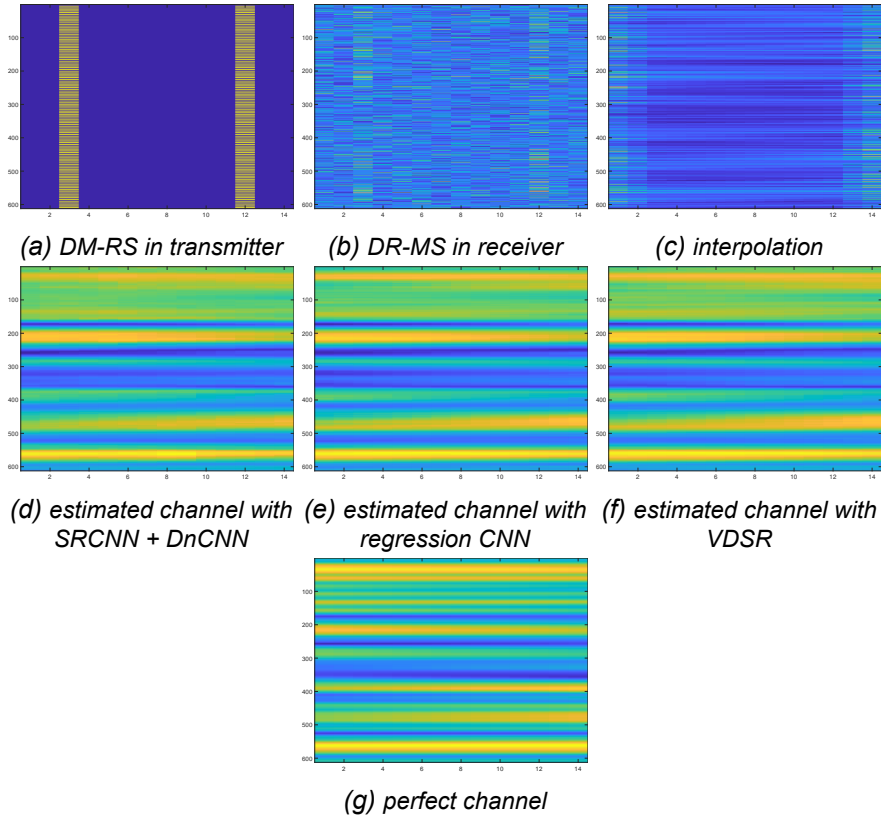


Figure 11 – Resource grid images
 Рис. 11 – Изображения сети ресурсов
 Слика 11 – Сликe мреже ресурса

Fortunately, training the neural network for a few representative SNR values can still yield satisfactory performance. In such cases, the neural network can estimate the channel for SNR values that are close to the ones it was trained on, and can interpolate to SNR values that are not covered in the training. Therefore, in our work, we have selected two ranges of representative SNR values for training the neural network, a range of discrete values $[0, 5]$ for low SNR and $[20, 25]$ for high SNR.

It is worth noting that for each of three methods, two models have been trained, one for low SNR and the other for high SNR values. Also, the models were trained using the parameters specified in Tables 2,3,4,5, for each range of the Signal-to-Noise Ratio (SNR)

Table 1 – Parameters for PDSCH DM-RS data generation
Таблица 1 – Параметры генерации данных PDSCH DM-RS
Табела 1 – Параметри за генерисање PDSCH DMRS података

Parameters	value
PDSCH Mapping Type	Type A
DR-MS TypeA Position	2
DM-RS Additional Position	1
DM-RS Configuration Type	1
Subcarrier Spacing	30 kHz
Cyclic Prefix	Normal
Bandwidth in number of resource blocks	51
Model Channel	TDL
Power Delay Profile	All profiles

Table 2 – Training parameters for the SRCNN method
Таблица 2 – Параметры обучения по методу SRCNN
Табела 2 – Параметри обуке за SRCNN метод

Training Parameters	Value
Solver for training network	Adam (Adaptive Moment Estimation)
Batch Size	128
Initial Learn Rate	0.001
Max Epochs	5

Training progress for low SNR values

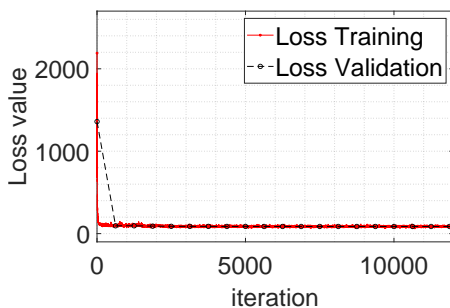
From the Loss graph in figures below (12,13 and 14), we can see that both the training and validation losses decrease steadily over iterations, indicating that the model is learning effectively without over-fitting. The validation loss is consistently similar to the training loss, which suggests that the model is generalizing well to new data.

Table 3 – Training parameters for the DnCNN method
 Таблица 3 – Параметры обучения по методу DnCNN
 Табела 3 – Параметри обуке за DnCNN метод

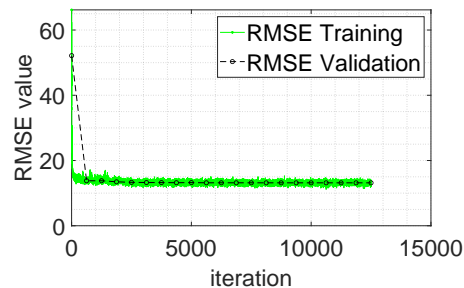
Parameters	Value
Solver for training network	Sgdm (Stochastic Gradient Descent with Momentum)
Momentum	0.9
Initial Learn Rate	0.001
Learn Rate Schedule	piecewise
Gradient Threshold Method	absolute-value
Gradient Threshold	0.005
L2Regularization	0.0001
Batch Size	128
Max Epochs	30

Table 4 – Training parameters for the regression CNN method
 Таблица 4 – Параметры обучения по регрессионному методу CNN
 Табела 4 – Параметри обуке за регресиону CNN методу

Training Parameters	Value
Solver for training network	Adam (Adaptive Moment Estimation)
Batch Size	32
Initial Learn Rate	0.0003
Max Epochs	5



(a) Loss



(b) RMSE

Figure 12 – Training progress for regression model
 Рис. 12 – Прогресс обучения по регрессионной модели
 Слика 12 – Напредак у фази обучавања за регресиони модел

Similarly, from the RMSE graph, we can see that both the training and validation RMSEs displayed a consistent downward trend, indicating good learning and that the models were gradually fitting the training data.

Table 5 – Training parameters for the VDSR method
Таблица 5 – Параметры обучения по методу VDSR
Табела 5 – Параметри обуке за VDSR метод

Parameters	value
Solver for training network	Sgdm (Stochastic Gradient Descent with Momentum)
Momentum	0.9
Initial Learn Rate	0.1
Learn Rate Schedule	piecewise
Learn Rate Drop Period	10
Learn Rate Drop Factor	0.1
L2Regularization	0.0001
Batch Size	32
Max Epochs	100
Gradient Threshold Method	l2norm
Gradient Threshold	0.01

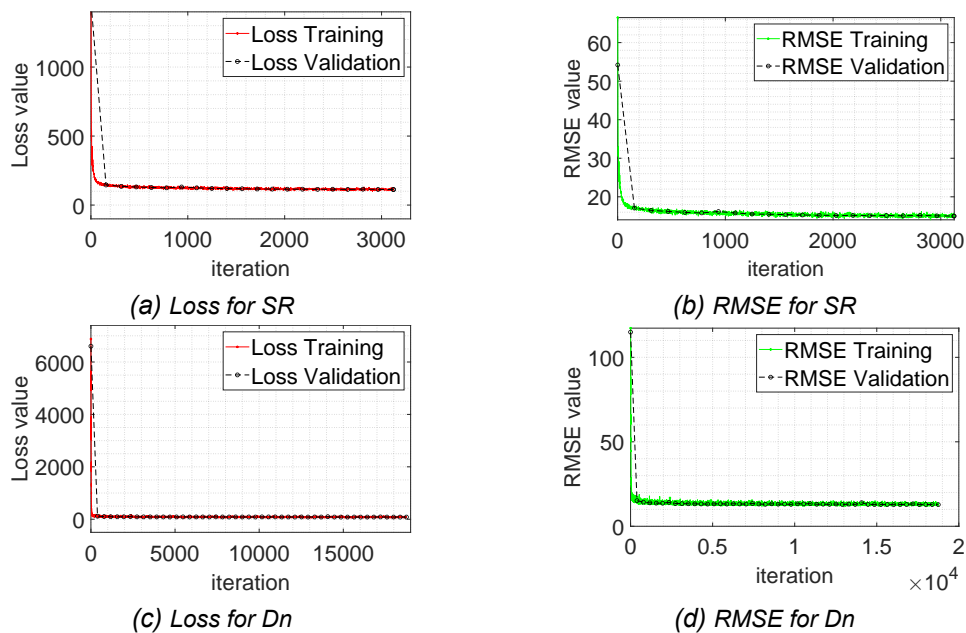


Figure 13 – Training progress for the SRDn model
Рис. 13 – Прогресс в обучении по модели SRDn
Слика 13 – Напредак у фази обучавања за SRDn модел

In the initial epochs, the loss and RMSE for Regression, SRDn and VDSR show a rapid drop, suggesting that the models quickly learned from the training samples. However, after that, the rate of improvement slowed

down, and the training was stopped after the loss and RMSE curve flattened, indicating that the model had reached the limit of learning from data.

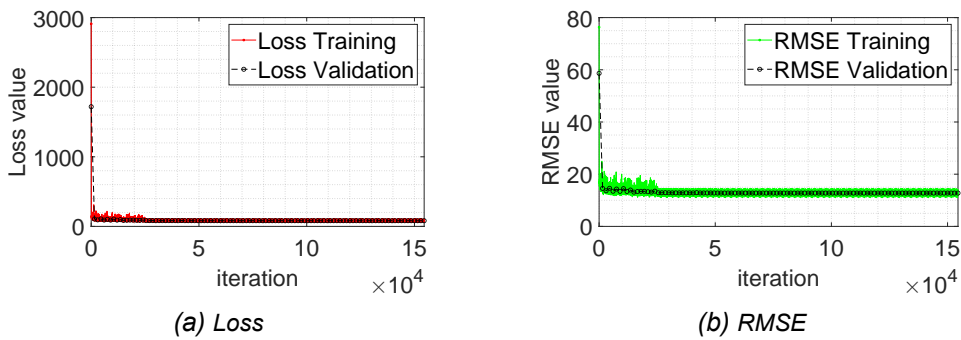


Figure 14 – Training progress for the VDSR model
Рис. 14 – Прогресс в обучении по VDSR
Слика 14 – Напредак у фази обучавања за VDSR модел

It is worth noting that for VDSR, the RMSE curve experienced some fluctuations, which could be attributed to the complexity of the dataset. However, the Regression and SRDn models could not capture this complexity.

Training progress for high SNR values

The figures below (15, 16 and 17) present the Loss and RMSE progress

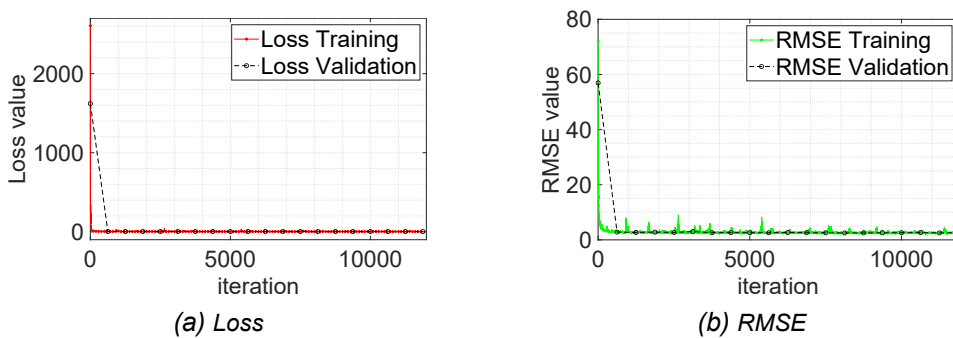


Figure 15 – Training progress for the regression model
Рис. 15 – Прогресс в обучении по регрессионной модели
Слика 15 – Напредак у фази обучавања за регресиони модел

Comparing the Loss and RMSE graphs in the preceding figures (15,16 and 17), it is clear that the trends follow a similar pattern. The models show promising results, with no evidence of over-fitting or under-fitting.

As in the case of the low SNR, the training process presents a downward trend of the loss and RMSE functions, showing that the models were gradually fitting the training data in the same way as in the low SNR.

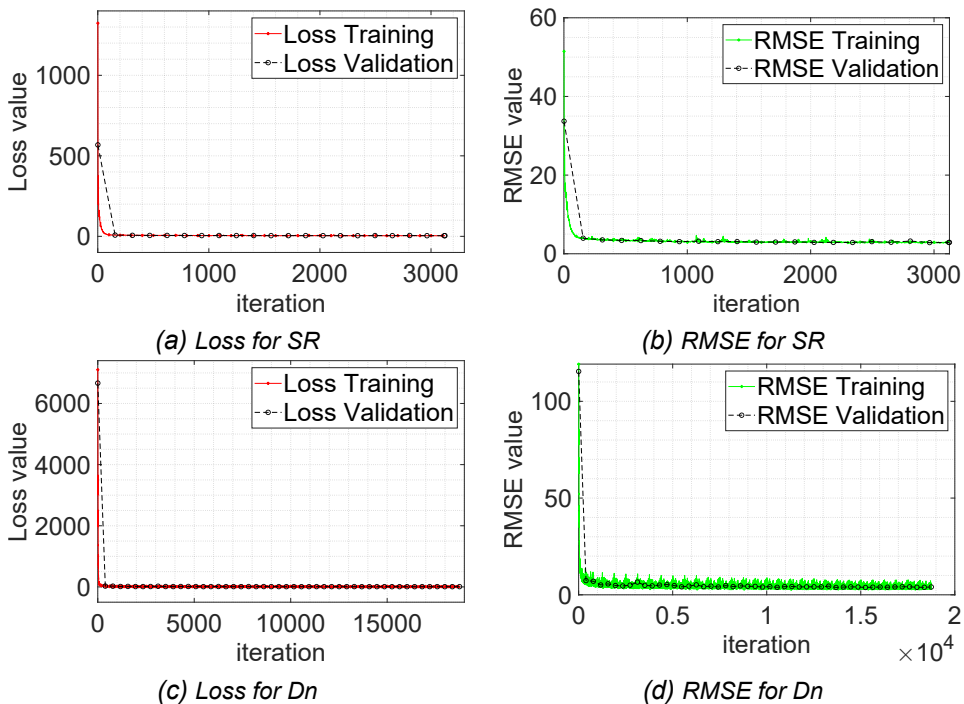


Figure 16 – Training progress for the SRDn model
 Рус. 16 – Прогресс в обучении по модели SRDn
 Слика 16 – Напредак у фази обучавања за SRDn модел

The RMSE curve presents some fluctuations in the cases of Regression, SRDn and VDSR model training, which indicates the ability of models to capture the complexity of the channel in the high SNR.

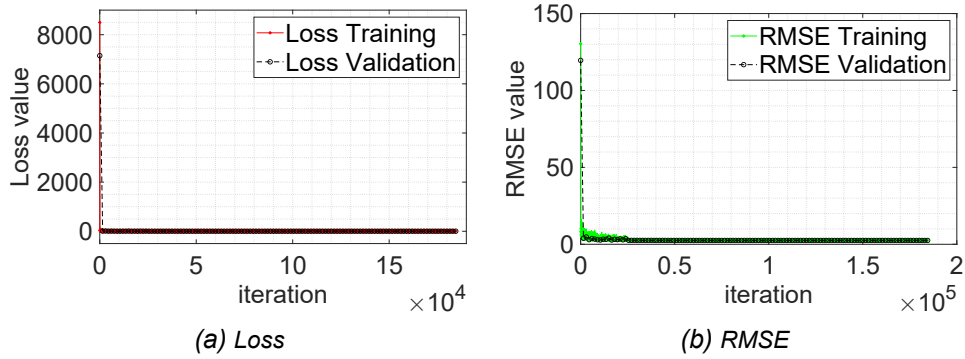


Figure 17 – Training progress for the VDSR model
 Рис. 17 – Прогресс в обучении по модели VDSR
 Слика 17 – Напредак у фази обучавања за VDSR модел

In summary, it could be seen in both low and high SNR values that the VDSR presented fluctuation in RMSE during the training, which indicates a high adaptability to the complexity of the channel.

Performance evaluation of CNN models using test data

The three methods (SRCNN + DnCNN, Regression CNN and VDSR) are evaluated on 5000 random channels in both low and high SNR conditions. Based on the provided RMSE (Root Mean Squared Error) values, their performance can be compared with the traditional method of LS (Least Squares). The results are presented in Table 6.

Table 6 – Performance evaluation of the CNN models
 Таблица 6 – Оценка производительности моделей CNN
 Табела 6 – Процена перформанси CNN модела

Model	RMSE (Low SNR)	RMSE (High SNR)
Least Square	2.0850	0.2425
Method1: SRCNN + DnCNN	0.4776	0.1299
Method2: Regression CNN	0.4942	0.1006
Method3: VDSR	0.4797	0.0968

For the low SNR, the SRCNN + DnCNN method and the VDSR method have similar performances, with the RMSE values of 0.4776 and 0.4797, re-

spectively. The Regression CNN method has a slightly higher RMSE. However, all three methods significantly outperform the Least Square method.

For the high SNR, the VDSR method has the best performance followed by the Regression CNN method and the SRCNN + DnCNN method. Again, all three methods significantly outperform the Least Square method.

In summary, the deep learning-based methods (SRCNN + DnCNN, Regression CNN, and VDSR) are more effective than the traditional Least Square method for channel estimation in both low and high SNR conditions. Among the deep learning-based methods, VDSR appears to be the most effective for high SNR conditions, while SRCNN + DnCNN and VDSR have similar performance for low SNR conditions. The Regression CNN method has slightly lower performance than the other two deep learning-based methods, but is still significantly better than the Least Square method. These results demonstrate the effectiveness of deep learning-based methods for channel estimation in wireless communication systems.

Channel Estimation MSE in terms of SNR for different channel profiles

The accuracy of channel estimation can be evaluated using the mean square error (MSE) metric. The MSE is a measure of the average difference between the estimated channel and the actual channel, and it is commonly used to compare different channel estimation methods. The MSE of channel estimation is affected by several factors, including the channel profile and the signal-to-noise ratio (SNR)

To illustrate the impact of channel profile and SNR on channel estimation for each of the three methods mentioned before, we have calculated the MSE for each of the scenarios, Non-Line-of-Sight NLOS (TDL-A, TDL-B and TDL-C) and Line-of-Sight LOS (TDL-D and TDL-E), in both low and high SNR conditions.

Channel Estimation MSE for NLOS communication

In the context of NLOS communication, where there is no direct line-of-sight between transmitting and receiving antennas, the signal travels along multiple paths to reach the receiver, causing severe signal attenuation, delay spread, and inter-symbol interference. The performance of the three

aforementioned channel estimation methods is impacted by the SNR values.

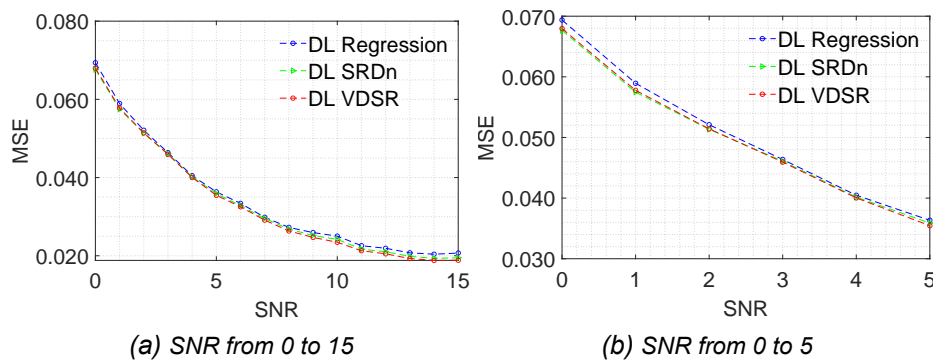


Figure 18 – Channel Estimation MSE in terms of a low SNR for NLOS
 Рис. 18 – Оценка канала MSE с точки зрения низкого SNR для NLOS
 Слика 18 – Процена канала MSE у код ниског SNR за NLOS

In very low SNR conditions (Figure 18), with a high number of multipaths, the SRCNN + DnCNN and VDSR methods outperform the CNN regression method, with VDSR exhibiting slightly better performance. The superior performance of these deep architectures can be attributed to their ability to better capture the complexity of the channel model.

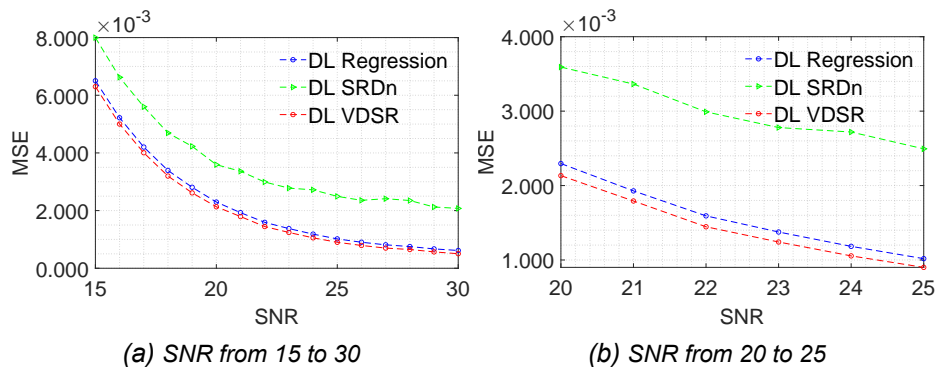


Figure 19 – Channel Estimation MSE in terms of a high SNR for NLOS
 Рис. 19 – Оценка канала MSE с точки зрения высокого SNR для NLOS
 Слика 19 – Процена канала MSE у код високог односа SNR за NLOS

However, as SNR values increase (Figure 19), the performance of the SRCNN + DnCNN method decreases drastically in comparison to the remaining methods. In contrast, the VDSR method continues to outperform all other methods.

Channel Estimation MSE for LOS communication

Line-of-Sight (LOS) scenarios are often preferred due to a clear, unobstructed path between transmitting and receiving antennas. In such scenarios, the signal travels directly between the antennas without being scattered or reflected by obstacles, resulting in minimal attenuation and distortion. As a result, channel estimation in the LOS scenarios is less challenging than in the NLOS scenarios.

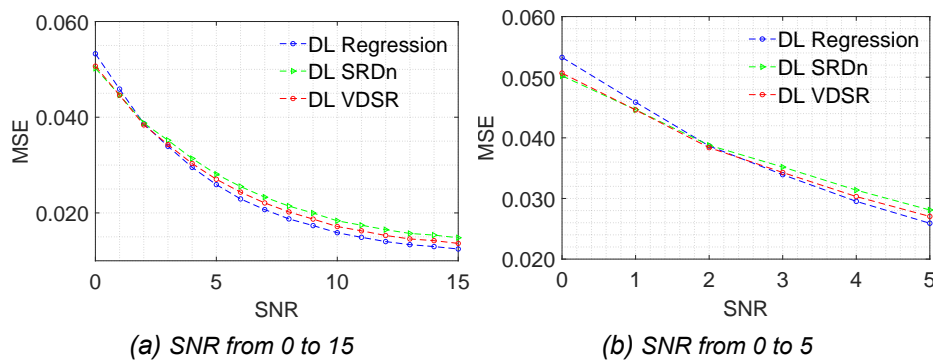


Figure 20 – Channel Estimation MSE in terms of a low SNR for LOS
 Рис. 20 – Оценка канала MSE с точки зрения низкого SNR для LOS
 Слика 20 – Процена канала MSE у смислу ниског SNR за LOS

However, even in the LOS scenarios (Figure 20), the accuracy of channel estimation is still impacted by SNR values. In a very low SNR values (SNR < 2), the deep CNN architectures (SRCNN + DnCNN and VDSR) outperform the simplistic architecture of CNN regression, due to their ability to capture the complexity of the channel model. The SRCNN + DnCNN and VDSR methods are better suited for achieving accurate channel estimation in such scenarios.

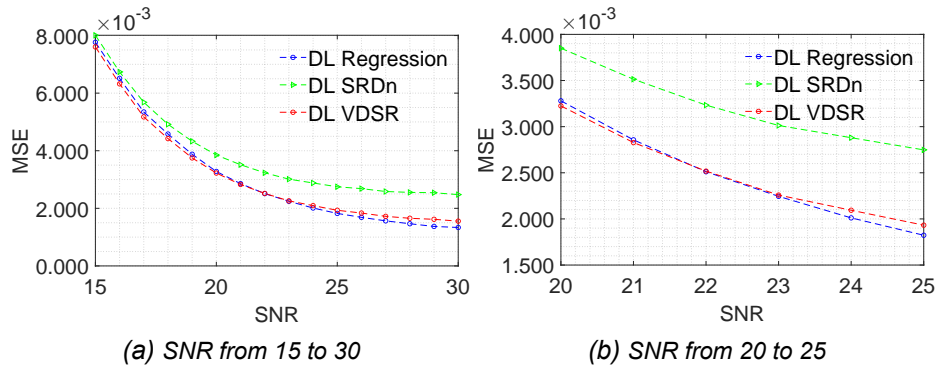


Figure 21 – Channel Estimation MSE in terms of a high SNR for LOS
 Рис. 21 – Оценка канала MSE с точки зрения высокого SNR для LOS
 Слика 21 – Процена канала MSE код високог односа SNR за NLOS

As SNR values increase (Figure 21), the performance of the CNN regression method becomes more favorable, due to its simplistic architecture being well adapted to the low complexity of the channel. On the other hand, the performance of SRCNN + DnCNN decreases significantly due to the negative impact of its deep denoising architecture (DnCNN). The VDSR architecture, however, demonstrates remarkable adaptability to the channel complexity, resulting in stable performance across a range of SNR values.

Conclusion

By leveraging the power of deep learning algorithms such as CNNs, channel estimation in 5G communication systems can be improved significantly. This work has showcased the potential that CNN offers compared to the traditional method of the Least square for an accurate channel estimation.

First, by conducting a comprehensive review of the existing literature on CNN-based channel estimation, two of widely used methods were chosen, namely the super-resolution and denoising method (SRCNN+DnCNN) and the CNN regression method. Besides that, a novel method (VDSR, Very Deep Super Resolution) was proposed in order to improve the accuracy of the state-of-the-art CNN based channel estimation methods. The three CNN models were trained on a large dataset in both low and high SNR conditions.

The trained models were evaluated and the results were compared to the traditional method of Least Square. The compared results have demonstrated the superiority of deep learning-based methods under varying SNR conditions. Moreover, the novel method exhibits the best overall performance in comparison to the two other deep learning-based methods.

Further, the impact of channel complexity on estimation accuracy was investigated in the case of the CNN based methods. The results highlighted the importance of selecting an appropriate channel estimation model based on the specific communication scenario's complexity and SNR values.

In NLOS scenarios with very low SNR values and a high number of multipaths, deep architectures such as SRCNN + DnCNN and VDSR outperform the CNN regression method due to their ability to capture the complexity of the channel model.

In contrast, in LOS scenarios, signal attenuation and distortion are minimal, making channel estimation less challenging. Nonetheless, the accuracy of channel estimation is still heavily impacted by SNR values, and deep CNN architectures such as SRCNN + DnCNN and VDSR remain better suited for achieving accurate channel estimation in very low SNR values.

As the SNR values increase, the CNN regression method exhibits improved performance due to its simplistic architecture that is well-suited to the low complexity of the channel. Conversely, the performance of SRCNN + DnCNN deteriorates significantly due to the adverse impact of its deep denoising architecture (DnCNN).

Notably, the VDSR architecture demonstrates remarkable adaptability to the channel complexity, resulting in consistent performance across all range of SNR values. This makes it a promising method for channel estimation in diverse 5G communication scenarios (NLOS and LOS).

In future work, we propose to extend the evaluation of the proposed method, VDSR (Very Deep Super Resolution), to Single-Input Multiple-Output (SIMO) and Multiple-Input Multiple-Output (MIMO) channel models for 5G wireless communication. The performance of VDSR has shown promising results in our current research, particularly in terms of its adaptability to varying channel complexities and SNR values. The extended evaluation will provide valuable insights into the performance and robustness of VDSR across different wireless communication setups, further enhancing its applicability and potential for real-world 5G deployments. Additionally,

investigating the impact of various system parameters, such as the number of Additional DM-RS and DM-RS configuration types, on the performance of VDSR in SIMO and MIMO models will enable to optimize and tailor the method for specific wireless communication scenarios, paving the way for improved channel estimation techniques in future 5G networks.

References

3GPP. 2018. *5G, NR, Physical layer, General description, Technical specification (3GPP TS 38.201 version 15.0.0 Release 15)* [online]. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3211> [Accessed: 10 August 2023].

3GPP. 2020a. *5G, NR, Physical channels and modulation, Technical Specification (3GPP TS 38.211 version 16.2.0 Release 16)* [online]. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3213> [Accessed: 10 August 2023].

3GPP. 2020b. *5G, Study on channel model for frequencies from 0.5 to 100 GHz, Technical Report (3GPP TR 38.901 version 16.1.0 Release 16)* [online]. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3173> [Accessed: 10 August 2023].

Albreem, M.A.M. 2015. 5G wireless communication systems: Vision and challenges. In: *2015 International Conference on Computer, Communications, and Control Technology (I4CT)*. Kuching, Malaysia, pp.493-497, April 21-23. Available at: <https://doi.org/10.1109/I4CT.2015.7219627>.

Banerjee, B., Khan, Z., Lehtomäki, J.J. & Juntti, M. 2022. Deep Learning Based Over-the-Air Channel Estimation Using a ZYNQ SDR Platform. *IEEE Access*, 10, pp. 60610–60621. Available at: <https://doi.org/10.1109/ACCESS.2022.3180352>.

Dong, C., Loy, C.C., He, K. & Tang, X. 2015. Image Super-Resolution Using Deep Convolutional Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 38(2), pp. 295–307. Available at: <https://doi.org/10.1109/TPAMI.2015.2439281>.

Gizzini, A.K., Chafii, M., Nimr, A., Shubair, R.M. & Fettweis, G. 2021. CNN Aided Weighted Interpolation for Channel Estimation in Vehicular Communications. *IEEE Transactions on Vehicular Technology*, 70(12), pp. 12796–12811. Available at: <https://doi.org/10.1109/TVT.2021.3120267>.

James, A.R., Benjamin, R.S., John, S., Joseph, T.M., Mathai, V. & Pillai, S.S. 2011. Channel estimation for OFDM systems. In: *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*. Thuckalay, India, pp.587-591, July 21-22. Available at: <https://doi.org/10.1109/ICSCCN.2011.6024619>.

Kaur, J., Khan, M.A., Iftikhar, M., Imran, M. & Haq, Q.E.U. 2021. Machine Learning Techniques for 5G and Beyond. *IEEE Access*, 9, pp. 23472–23488. Available at: <https://doi.org/10.1109/ACCESS.2021.3051557>.

Kim, J., Lee, J.K. & Lee, K.M. 2016. Accurate Image Super-Resolution Using Very Deep Convolutional Networks. In: *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. Las Vegas, NV, USA, pp.1646–1654, June 27-30. Available at: <https://doi.org/10.1109/CVPR.2016.182>.

Ma, Z., Zhang, Z., Ding, Z., Fan, P. & Li, H. 2015. Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives. *Science China Information Sciences*, 58(4), pp. 1–20. Available at: <https://doi.org/10.1007/s11432-015-5293-y>.

Morocho-Cayamcela, M.E., Lee, H. & Lim, W. 2019. Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential, Limitations, and Future Directions. *IEEE Access*, 7, pp. 137184–137206. Available at: <https://doi.org/10.1109/ACCESS.2019.2942390>.

Simonyan, K. & Zisserman, A. 2014. Very Deep Convolutional Networks for Large-Scale Image Recognition. *arXiv:1409.1556*. Available at: <https://doi.org/10.48550/arXiv.1409.1556>.

Soltani, M., Pourahmadi, V., Mirzaei, A. & Sheikhzadeh, H. 2019. Deep Learning-Based Channel Estimation. *IEEE Communications Letters*, 23(4), pp. 652–655. Available at: <https://doi.org/10.1109/LCOMM.2019.2898944>.

Wang, C.X., Bian, J., Sun, J., Zhang, W. & Zhang, M. 2018. A Survey of 5G Channel Measurements and Models. *IEEE Communications Surveys & Tutorials*, 20(4), pp. 3142–3168. Available at: <https://doi.org/10.1109/COMST.2018.2862141>.

Ye, H., Li, G.Y. & Juang, B.H. 2017. Power of Deep Learning for Channel Estimation and Signal Detection in OFDM Systems. *IEEE Wireless Communications Letters*, 7(1), pp. 114–117. Available at: <https://doi.org/10.1109/LWC.2017.2757490>.

Zhang, K., Zuo, W., Chen, Y., Meng, D. & Zhang, L. 2017. Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising. *IEEE transactions on image processing*, 26(7), pp. 3142–3155. Available at: <https://doi.org/10.1109/TIP.2017.2662206>.

Оценка канала глубокого обучения в 5G беспроводной связи

Мохамед Зуауи М. Лайдунни, **корреспондент**,
Таки-эддине Ахмед А. Беняхия, Бобан З. Павлович,
Салем-Билал Б. Амокрание, Туати Б. Адли

Университет обороны в г. Белград, Военная академия,
Департамент телекоммуникации и информатики,
г. Белград, Республика Сербия



РУБРИКА ГРНТИ: 49.33.29 Сети связи,
20.23.25 Информационные системы с
базами знаний

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: За последние годы методы глубокого обучения, в частности сверточные нейронные сети (CNN), показали высокую производительность в системах связи 5G, значительно повысив точность оценки канала по сравнению с обычными методами. Целью данной статьи является всесторонний обзор существующей литературы по методам оценки канала на основе CNN. Помимо того, статья нацелена на усовершенствование современных методов оценки канала на основе CNN путем предложения нового метода под названием VDSR (Very Deep Super Resolution), вдохновленного методами изображения Super-Resolution.

Методы: Для того чтобы оценить эффективность различных подходов было проведено всестороннее сравнение с учетом различных сценариев, в том числе с низким соотношением сигнал-шум (SNR) и высоким SNR, а также в условиях прямой видимости (LOS) и вне прямой видимости (NLOS). С помощью сравнительного анализа была произведена оценка эффективности существующих методов и выявлены преимущества предлагаемого метода, основанного на VDSR.

Результаты: Результаты данного исследования показывают значительный потенциал оценки канала, основанного на CNN в системах связи 5G, при этом метод VDSR демонстрирует стабильную производительность во всех сценариях. Данное исследование способствует совершенствованию методов оценки каналов в сетях 5G, прокладывая путь усовершенствованным системам беспроводной связи с повышенной надежностью.

Выводы: Архитектура VDSR прекрасно приспособлена к сложности канала, что обеспечивает стабильную производительность во всем диапазоне значений SNR.

Ключевые слова: глубокое обучение, CNN, системы связи 5G, сверхглубокое сверхвысокое разрешение.

Процена канала дубоког учења за 5G бежичне комуникације

Мохамед Зуауи М. Лаидуни, аутор за преписку,
Таки-еддине Ахмед А. Бенјахија, Бобан З. Павловић,
Салем-Билал Б. Амокроне, Туати Б. Адли

Универзитет одбране у Београду, Војна академија, Катедра
телекомуникација и информатике, Београд, Република Србија

ОБЛАСТ: телекомуникације, рачунарске науке

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Технике дубоког учења, посебно конволуционе неуронске мреже (CNN), последњих година показале су изузетне перформансе у 5G комуникационим системима тако што су значајно побољшале тачност процене канала у поређењу са конвенционалним методама. У овом раду представљен је свеобухватан преглед постојеће литературе о техникама процене канала заснованих на CNN-у. Поред тога, основни циљ рада јесте унапређивање најсавременијих метода за процену канала заснованих на CNN-у, што је резултирало предлагањем нове методе под називом VDSR (Very Deep Super Resolution), инспирисане техникама Super Resolution слике.

Методе: Да би се извршила процена ефикасности различитих приступа, спроведено је свеобухватно поређење различитих сценарија, укључујући низак однос сигнал-шум (SNR) и висок SNR, као и линију оптичке видљивости (LOS) и сценарио без видљивости (NLOS). Кроз ову компаративну анализу процењене су перформансе постојећих метода и истакнуте предности које нуди предложена техника заснована на VDSR.

Резултати: На основу добијених резултата откривен је значајан потенцијал процене канала заснованог на CNN-у у 5G комуникационим системима, при чему VDSR метод показује константну предност у свим сценаријима. Основни циљ истраживања јесте унапређење техника процене канала у 5G мрежама, чиме се дају основе побољшаним бежичним комуникационим системима са већом поузданошћу.

Закључак: VDSR архитектура показује изузетну прилагодљивост различитим врстама канала, што резултира обезбеђењем захтеваних перформанси за све анализиране вредности SNR.

Кључне речи: дубоко учење, CNN, 5G комуникациони системи, веома дубока супер резолуција.

Paper received on / Дата получения работы / Датум пријема чланка: 18.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 27.11.2023.

Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 29.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.srb>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.srb>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.srb>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Anomaly network intrusion detection system based on NetFlow using machine/deep learning

Touati B. Adli^a, Salem-Bilal B. Amokrane^b,
Boban Z. Pavlović^c, Mohammad Zouaoui M. Laidouni^d,
Taki-eddine Ahmed A. Benyahia^e

University of Defence in Belgrade, Military Academy, Department of
Telecommunications and Informatics, Belgrade, Republic of Serbia

^a e-mail: adlitouati94@gmail.com, **corresponding author**,
ORCID ID: <https://orcid.org/0009-0000-2673-6954>

^b e-mail: amokranesalembilal@gmail.com,
ORCID ID: <https://orcid.org/0009-0009-7588-5708>

^c e-mail: bobanpav@yahoo.com,
ORCID ID: <https://orcid.org/0000-0002-5476-7894>

^d e-mail: mohammedz.laidouni@gmail.com,
ORCID ID: <https://orcid.org/0009-0008-6042-0513>

^e e-mail: benyahia.taki@gmail.com,
ORCID ID: <https://orcid.org/0009-0006-6025-6915>

DOI: 10.5937/vojtehg71-46058; <https://doi.org/10.5937/vojtehg71-46058>

FIELD: computer sciences, telecommunications, cybersecurity

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Anomaly detection-based Network Intrusion Detection Systems (NIDSs) have emerged as a valuable tool, particularly in military fields, for protecting networks against cyberattacks, specifically focusing on Netflow data, to identify normal and abnormal patterns. This study investigates the effectiveness of anomaly-based machine learning (ML) and deep learning (DL) models in NIDSs using the publicly available NF-UQ-NIDS dataset, which utilizes Netflow data, with the aim of enhancing network protection.

Methods: The authors Sarhan, M., Layeghy, S., Moustafa, N. and Portmann, M. in the conference paper Big Data Technologies and Applications, in 2021, involve a preprocessing step where 8 features are selected for the training phase out of the 12 available features. Notably, the IP source and destination addresses, as well as their associated ports, are specifically excluded. The novelty of this paper lies in the preprocessing of the excluded features and their inclusion in the training phase, employing various classification ML and DL algorithms such as ExtraTrees, ANN, simple CNN, and VGG16 for binary classification.

Results: The performance of the classification models is evaluated using metrics such as accuracy, recall, etc., which provide a comprehensive analysis of the obtained results. The results show that the ExtraTrees ML model outperforms all other models when using our preprocessing features, achieving a classification accuracy of 99.09%, compared to 97.25% in the reference dataset.

Conclusion: The study demonstrates the effectiveness of anomaly-based ML and DL models in NIDSs using Netflow data.

Key words: Network intrusion detection system (NIDS), Netflow features, Machine/Deep learning, anomaly-based NIDS.

Introduction

As technology progresses, internet networks offer new communication opportunities but also increase vulnerability to intrusions and attacks. This is a significant concern in the military, where technology reliance is growing, and cyber-attacks are becoming more frequent and advanced. To combat these threats, a flexible defense system capable of analyzing large amounts of network traffic is required. Anomaly-based Intrusion Detection System (IDS) offers a valuable methodology for detecting both known and unknown attacks in intrusion detection systems (Van et al., 2017). In the military context, traditional cybersecurity measures such as antivirus software and firewalls are no longer sufficient to protect against advanced threats. To adequately secure military networks against cyber-attacks, an IDS can provide continuous monitoring of the network for potential threats and offer an additional layer of protection (Labonne, 2020).

Network-based Intrusion Detection Systems (NIDSs) are a specific type of IDS that operate at the network layer, analyzing network traffic in real-time for signs of intrusion or malicious activity. In addition to anomaly-based NIDSs, NetFlow is another valuable tool that can be used in the field of NIDSs and attack detection. NetFlow provides network traffic information that can be analyzed to identify patterns and potential threats, allowing for early detection and response to cyber-attacks. By combining the power of anomaly-based NIDSs and NetFlow analysis, military networks can be more effectively protected against a wide range of cyber threats. With the use of advanced technologies such as Deep learning and Machine learning, military networks can become even more resilient against sophisticated attacks.

The paper is structured as follows. Firstly, a comprehensive definition of IDSs, specifically focusing on NIDSs and Anomaly-based NIDSs, is provided. Next, NetFlow is defined, and an overview of the datasets used in the study is presented. The specific ML and DL techniques utilized in the study are presented, along with the results of reproducing the study conducted by (Sarhan et al., 2021) for binary classification. The authors of the original study excluded the IP and port features from the dataset in the training phase, resulting in an 8-features model. The paper introduces a new contribution that involves a preprocessing step applied to the excluded IP and port features, resulting in a 13-features model. This contribution allows us to explore the potential of using these features for improving the performance of the classification in the context of anomaly-based NIDSs with NetFlow data. Then, the NetFlow features for both models were adapted to the input of deep learning techniques by converting the features vector to images.

Finally, the paper presents the results of machine and deep learning for both 8 and 13 feature models and provides recommendations for future research in the field of anomaly-based NIDSs using machine and deep learning techniques with NetFlow data.

Intrusion Detection System (IDS)

Confidentiality, Integrity, and Availability (also known as the CIA triad) are three fundamental concepts of information security. An intrusion or a cyber-attack is defined as all unauthorized activities that compromise one, two, or all of these three components of an information system (Labonne, 2020).

Intrusion detection is the process of monitoring network traffic and computer events to detect unauthorized or malicious activities. An Intrusion Detection System (IDS) is any device or software application that performs this function. An IDS uses its knowledge, including databases, statistics, and artificial intelligence, to transform monitored activities into alerts.

IDSs are sometimes confused with two other security tools: firewalls and Intrusion Prevention Systems (IPSs). Firewalls, IDSs, and IPSs are security tools used to protect network systems but have different methods. Firewalls detect intrusions at the network perimeter and analyze packet headers to filter traffic based on predetermined rules. IDSs monitor network activities and generate alerts, but cannot block suspicious activity on

their own. IPSs function like IDSs but can take proactive action to block threats. IPSs automate the process, while firewalls and IDSs require human intervention to process alerts ([Labonne, 2020](#)).

Types of IDSs

IDSs can be classified into three categories according to the type of activities that are analyzed: host-based IDSs (HIDS) network-based IDSs (NIDSs), and application-based IDSs ([Labonne, 2020](#); [Tufan et al., 2021](#)).

An HIDS is installed on individual computer systems to analyze files, processes, and system logs for suspicious activity. It can detect attacks through indicators like failed logins or high CPU usage. An NIDS analyzes network traffic using sensors placed at various points. It is more scalable and cross-platform than HIDSs, commonly used to protect IT infrastructure. However, a combination of both NIDSs and HIDSs can be used to achieve a higher level of security. For the purpose of this work, the term "IDS" specifically refers to NIDSs. Application-based IDS is a type of HIDS that focuses on monitoring a specific application.

IDSs can be categorized based on the type of detection method they use. There are three main categories: signature-based detection, anomaly-based detection, and hybrid detection. Signature-based detection compares monitored data with a database of attack signatures, detecting known attacks. This method can only detect known attacks, even with the latest updates. Anomaly detection identifies unknown attacks by flagging deviations from normal behavior. This approach does not require a pre-existing database and can identify unknown attacks. However, it can generate a significant number of false positives. Hybrid detection combines both methods to detect known and unknown attacks, reducing false positives and improving accuracy.

Anomaly-based NIDSs

Anomaly detection plays a critical role in network security, as anomalies can indicate rare but serious events. The network-based NIDS analyzes network-related events, such as traffic volume, IP addresses, service ports, protocol usage, etc. It must detect all types of anomalies in the network. In network-based NIDSs, intrusions typically are referred to as anomalous through continuous observation and modeling of normal behavior in the

networks. However, some anomalous behavior may be normal, highlighting the need for anomaly-based NIDSs to adapt to dynamic network environments with new protocols and updated behaviors. Various techniques, such as statistical-based, knowledge-based, and machine learning-based, have been used in anomaly-based NIDSs, but there are still research challenges to improve their performance and suitability with current network data characteristics (Van et al., 2017). Anomaly detection techniques are the most commonly used IDS detection type and are the most investigated topic in the literature among researchers (Bahlali, 2019).

Our work primarily focuses on researching and implementing anomaly detection in network-based NIDSs, commonly referred to as anomaly detection-based NIDSs. Various ML and DL techniques will be explored to enhance the performance of Anomaly detection-based NIDSs in detecting network traffic anomalies using NetFlow features.

NIDS dataset and NetFlow

NIDS Dataset

Acquiring real-world network data flows is difficult due to security and privacy concerns, which make it challenging to access such data (Sarhan et al., 2022). Due to the challenges of obtaining real-world network data flows, many researchers have developed network testbeds as a means to generate synthetic datasets. These NIDS datasets contain labeled network flows that are made up of certain features extracted from network traffic. The features in a dataset are pre-determined by the authors based on their expertise in the relevant domain and the tools used during the extraction process (Sarhan et al., 2022). In recent years, the most widely used NIDS datasets (Sarhan et al., 2021) that have been released within the past five years are shown in Table 1.

These datasets are highly relevant as they capture modern behavioral network attacks. It is important to note that these datasets differ significantly in terms of their feature sets, and therefore, the information they contain varies considerably (Sarhan et al., 2021). This difference in these datasets makes the evaluation of proposed ML-based NIDSs often unreliable when tested on multiple datasets using their original feature sets (Sarhan et al., 2022).

Table 1 – The most relevant NIDS datasets (Sarhan et al., 2021)
 Таблица 1 – Наиболее релевантные наборы данных NIDS (Sarhan et al., 2021)
 Табела 1 – Најрелевантнији NIDS скупови података (Sarhan et al., 2021)

Dataset	Release year	Number of features
UNSW-NB15	2015	49
BoT-IoT	2018	42
CSE-CIC-IDS2018	2018	75
ToN-IoT	2020	44

NetFlow

NetFlow is a network protocol used for network traffic monitoring and analysis. Compared to pcap format, NetFlow data contains less data, making it easier to collect and process. Additionally, NetFlow is less intrusive to privacy, further enhancing its appeal as a preferred network log format (Cao et al., 2022). Rather than focusing on individual packets, flow monitoring analyzes the flow of traffic, making it a more scalable approach to traffic analysis. This process involves observing packets, exporting flows using protocols like NetFlow and IPFIX, collecting data, and analyzing that data in its entirety (Hofstede et al., 2014). Every flow in NetFlow contains network statistics representing a connection between two hosts. These statistics can be utilized to compute performance metrics and to identify any unusual or abnormal network behavior (Cao et al., 2022).

NetFlow version 9 (NetFlow v9) is the most used version of NetFlow. It is a protocol that enables the collection and export of flow records, providing detailed information about network traffic patterns such as source and destination IP address, source and destination port, protocol, etc. (Cisco, 2011).

NetFlow v9 fields play a crucial role in IDSs by providing valuable information for monitoring, analyzing, and tracking network traffic in real-time, enabling the identification of potential security threats.

Anomaly Detection using Machine learning and Deep learning

Machine learning

Machine learning (ML) has proven to be a highly effective approach to solving diverse problems. One area where machine learning models can be applied is NIDSs, which involves categorizing input data into specific classes, such as "benign" or "attack", as well as identifying various types of attacks (Fosić et al., 2023).

Various machine learning algorithms such as decision trees, Extra-Trees, SVM, etc., are employed for classification. For this study, a supervised machine learning approach was adopted using a NetFlow dataset with uniquely labeled records. Benign traffic was labeled as 0 (class 0), while anomalies or network attacks were labeled as 1 (class 1).

An ExtraTrees ensemble classifier was utilized as it belongs to the "trees" family and has demonstrated reliable performance in NIDS datasets, allowing for a valid comparison with (Sarhan et al., 2021).

Artificial Neural Network (ANN)

The ANN is a type of machine learning algorithm consisting of interconnected neurons organized as an input layer, a number of hidden layers, and an output layer. Each layer has a specific number of neurons. The information enters the neural network via the input layer, it is processed in the hidden layers and the result can be retrieved in the output layer (Anitha & Arockiam, 2019; Cahyo et al., 2016).

This study implements an ANN to assess its effectiveness in training NetFlow features, aiming to extract meaningful information and improve the accuracy of NIDSs.

Deep Convolutional Neural Networks (CNNs)

Deep learning (DL) is a sub-field of ML that models the learning process using multiple layers of neurons. DL algorithms offer a more automated solution by allowing models to learn feature representations directly from data. This approach is highly effective as a tool for NIDSs, due to its ability to process and learn the data to discover complex features (Rizvi et al., 2023).



In the context of DL, the convolutional neural networks (CNNs), have shown promise in efficiently selecting features and identifying the latent relationships among them (Liu et al., 2019). Inspired by the success of CNNs in image classification tasks, this work aims to apply CNNs to NIDSs leveraging their ability to extract meaningful NetFlow features and classify data accurately (Liu et al., 2019).

Our work involves transforming NetFlow features into images and utilizing two different architectures for classification. The first architecture utilizes a simple CNN structure, while the second is based on the VGG16 model. The comparative analysis of these two architectures will provide insight into the optimal approach for utilizing neural networks in NIDSs.

Evaluation Metrics

In this study, the selection of appropriate performance metrics was given careful consideration to assess the effectiveness of the NIDS model:

1. **Accuracy**
$$= \frac{TP + TN}{TP + FP + TN + FN}$$
2. **Recall (Detection Rate or TPR)**
$$= \frac{TP}{TP + FN}$$
3. **Precision**
$$= \frac{TP}{TP + FP}$$
4. **F1-Score**
$$= 2 * \frac{Recall * Precision}{Recall + Precision}$$
5. **AUC (Area Under the Curve)**
$$= \int_0^1 TPR(FPR) d_{FPR}$$

where $TPR(FPR)$ is the function that maps each $FPR = \frac{FP}{FP+TN}$ value to the corresponding TPR .

6. **Score time (μ s)** : refers to the duration required for predicting a single test sample.

where prediction **TP** = true positive, **TN** = true negative, **FP** = false positive and **FN** = false negative.

Experiments & results

Hardware and library used

The experimentation phase involved a hardware setup consisting of an 11th Gen Intel(R) Core(TM) i7-11800H processor with 16 virtual CPUs running at a frequency of 2.30GHz. The system was also equipped with 16GB of RAM and an NVIDIA RTX 3060 GPU.

The Python programming language (3.9.16) and the Scikit-learn platform (1.2.1) were utilized for machine/deep learning classification tasks. Additionally, TensorFlow (2.10.1) and Keras (2.10.0) were also used in this study.

NF-UQ-NIDS dataset

The first step of the proposed classification model and methodology is to collect data on traffic flow. The dataset selected for this study is the NF-UQ-NIDS, which is a pre-labeled NetFlow packet containing benign and attack data. This dataset, as published by (Sarhan et al., 2021), was created by merging and converting the four datasets, into NetFlow version 9 format. A total of 12 relevant features were chosen to construct this dataset. The Table 2 shows the descriptions of these features.

The advantage of this dataset is that it offers the advantages of shared datasets and it is more recent than other publicly available datasets which will facilitate a reliable evaluation of proposed learning models across various network settings and attack scenarios.

The NF-UQ-NIDS dataset comprises 11994893 flow records labeled, as either benign or attack. The dataset includes twenty (20) types of attacks, out of which 9208048 (76.77%) are benign flows and 2786845 (23.23%) are attacks. Various types of features, including categorical, numeric (integer, decimal, and binary), and temporal features, are used in the dataset.

Data pre-processing

Data pre-processing involves transforming the raw data into a format that can be used for machine/deep learning tasks. Furthermore, the presence of nominal features or categorical features, and Non-similar scale features can pose a challenge during data pre-processing. To address the first



Table 2 – NetFlow features of NF-UQ-NIDS with brief descriptions
Таблица 2 – Карактеристике NetFlow NF-UQ-NIDS с кратким описанијем
Табела 2 – NetFlow обележја NF-UQ-NIDS-а са кратким описима

Feature	Description
IPV4_SRC_ADDR	IPv4 source address
IPV4_DST_ADDR	IPv4 destination address
L4_SRC_PORT	IPv4 source port number
L4_DST_PORT	IPv4 destination port number
PROTOCOL	IP protocol identifier byte
TCP_FLAGS	Cumulative of all TCP flags
L7_PROTO	Layer 7 protocol (numeric)
IN_BYTES	Incoming number of bytes
OUT_BYTES	Outgoing number of bytes
IN_PKTS	Incoming number of packets
OUT_PKTS	Outgoing number of packets
FLOW_DURATION_MILLISECONDS	Flow duration in milliseconds

challenge, encoding techniques might be required to transform these features into a suitable format. As for the second issue, normalization may be necessary to ensure that all features take the same range of values.

In the case of the NF-UQ-NIDS dataset, the main issues were identified as nominal features and differences in feature value ranges. To address these issues, One-Hot Encoding and Feature Normalization were used.

The authors of ([Sarhan et al., 2021](#)) utilized only eight (8) NetFlow features out of the total twelve (12) features present in the NF-UQ-NIDS dataset. In particular, they excluded the source and destination IP addresses as well as their associated ports during the model training.

However, taking inspiration from ([Figueiredo et al., 2023](#)), our main contribution involves the incorporation of the dropped features (IP source/destination and ports) in our study. This inclusion aims to improve the detection of malicious IP addresses and assess the impact compared to the approach adopted by ([Sarhan et al., 2021](#)).

Source and destination ports pre-processing

In order to make the dataset suitable for ML and DL, the source and destination ports were merged into a unified feature, preserving the net-

work application's corresponding port for each flow. However, having both ports in the dataset would not be useful for an ML model, since one of the ports is typically a dynamic port that is assigned during the network routing process. These dynamic ports are usually found in the higher range of ports (49152 to 65535), whereas the lower port numbers are reserved for specific network applications. A single feature called "port" was created for each flow, consolidating port numbers between 0 and 4096. The process for converting port numbers is outlined in Algorithm 1. Flows with port numbers above 4096 were mapped to the category 4096, which might limit the NIDS's ability to distinguish between different ports beyond this threshold. Nevertheless, this approach still covers the most frequently used ports in both benign and malicious network traffic (Figueiredo et al., 2023).

Algorithm 1 Port number conversion

```

1: for Row in Dataset do
2:    $sp \leftarrow SourcePort$ 
3:    $dp \leftarrow DestinationPort$ 
4:   if  $sp \leq dp$  then
5:      $Port \leftarrow sp$ 
6:   else
7:      $Port \leftarrow dp$ 
8:   end if
9:   if  $Port \geq 4096$  then
10:     $Port \leftarrow 4096$ 
11:  end if
12:   $Row \leftarrow Row + Port$ 
13: end for

```

Source and destination IP pre-processing

The inclusion of source and destination IP addresses and ports in the training phase is a key aspect of this study. An IP address served as an identifier for each system in the network; it is hard to translate into a feature for ML. Two of the most common approaches to solve this problem are (Figueiredo et al., 2023): (a) removing these features altogether as in (Sarhan et al., 2021) which results in the loss of valuable contexts, such as the general network location, or (b) using a dictionary to translate the

IP addresses to a number, which can be reversed in the end to identify a malicious IP address. Although a dictionary can effectively map individual systems and detect patterns such as traffic originating from the same IP address, this method may not work well in a different network context due to high misclassification rates and the increasing dataset size.

To strike a balance between the two prevalent options, a particular approach was applied, involving the conversion of each IP address to a binary feature denoting either Internal or External. (Figueiredo et al., 2023). The assignment of the "Internal" label was based on IP addresses belonging to a private address space (starting with "192.168.", "172.16.", or "10."), while IP addresses outside this range were labeled as "External" (Algorithm 2). Since Internal and External are fundamental characteristics of every network flow, this method yields more contextual information about the network compared to simply removing the source and destination IPs. Moreover, this feature is context-independent, making it easy to apply the model to different networks.

Algorithm 2 IP address conversion

```
1: for Row in Dataset do
2:   if IP starts with "192.168." or "172.16." or "10." then
3:     IP ← Internal
4:   else
5:     IP ← External
6:   end if
7: end for
```

After mapping the IP source and destination addresses into the categories "Internal" and "External," it is necessary to employ data encoding techniques to convert these categorical features into numerical representations.

Encoding data is the process of transforming some input to numbers, usually in a way that is reversible and allows the translation between the resulting output and the original input (Figueiredo et al., 2023).

Assigning a unique number to each category when encoding categorical features can result in an ordinal encoding which may mislead ML models. As such, a binarization technique called One-Hot Encoding was used. This technique converts each category of a specific feature into a new binary

feature with the value one (1) meaning that it belongs to this category and zero (0) otherwise.

After applying this technique to the mapped IP addresses, two new features are obtained for each IP address, as illustrated in Figure 1.

IP Address	One-Hot Encoding	External IP Address	Internal IP Address
External		1	0
Internal	0	1	
Internal	0	1	
External	1	0	

Figure 1 – One-Hot Encoding of an IP address

Рис. 1 – Горячее кодирование IP-адреса

Слика 1 – One-Hot кодирање ИП адресе

Data normalisation

The normalization step is important for the training process since the difference in the feature scales can cause problems during the training. With the normalization, each feature would have an equal impact on the model prediction results.

The Min-Max normalization technique was utilized to scale all values in the dataset between 0 and 1. This technique performs a linear transformation on the original data. The advantage of Min-Max normalization is that it preserves the relationships among the original data values (Labonne, 2020; Bahlali, 2019). The normalized feature is given by:

$$\hat{x}_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)}. \quad (1)$$

where x_i and \hat{x}_i denote the original and the normalized feature value, respectively.

1D NetFlow data to 2D NetFlow images

In this work, two different approaches were explored. The first approach involved constructing an image directly from the features. The second approach involved constructing the image by building a square surrounding correlation matrix (SC matrix), as utilized in (Liu et al., 2019)

First approach: reshaping features image

For the 8 features, constructing an image with a size of 3x3 was insufficient. To address this issue, zeros were added to the missing pixels, as shown in Figure 2.

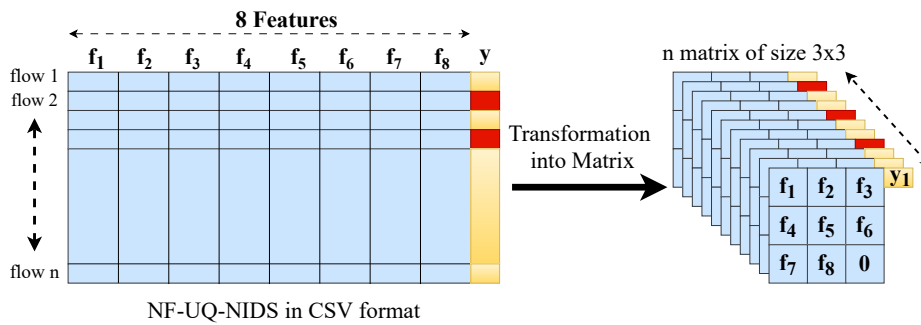


Figure 2 – NetFlow to matrix transformation by reshaping

Рис. 2 – Преобразование NetFlow в матрицу путем изменения формы

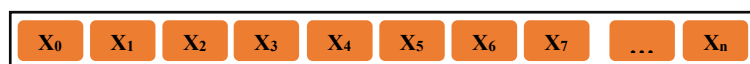
Слика 2 – Преобликовање NetFlow у матричну трансформацију

For the 13-feature scenario, the Recursive Feature Elimination (RFE) technique was employed to select the nine most significant features for the analysis. Following this, a simple reshaping technique was applied to transform the data into images of size 3x3.

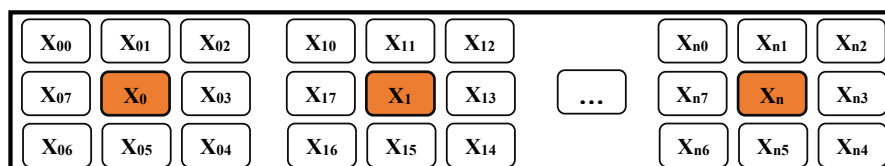
Second approach: using SC matrix

Based on the approach in (Liu et al., 2019) which proposes a localization technique that utilizes the correlation matrix to process NetFlow data, the correlation matrix is used to evaluate the correlations among the features in NetFlow data. In this study, the top-k (k=8) highly correlated features $X_{i0}, X_{i1}, \dots, X_{i7}$, were selected from the Netflow features X_0, X_1, \dots, X_n , for each numeric feature X_i to construct a square SC matrix. For each row of NetFlow data, an image is generated by concatenating the SC matrices of all features. An example of NetFlow images generated using this approach is shown in Figure 3.

This technique provides a powerful approach for extracting meaningful information from NetFlow data and improving the accuracy of NIDSs. In the case of 8 features, the issue of a missing value for the ninth pixel was resolved by substituting it with zero, maintaining the size of the image at



(a)



(b)

Figure 3 – Transformation of 1D NetFlow features to 2D NetFlow

(a) NetFlow features (b) 2D image

Рис. 3 – Преобразование 1D NetFlow в 2D NetFlow

(a) Атрибут NetFlow (b) 2D-изображение

Слика 3 – Трансформација 1D NetFlow обележје у 2D NetFlow

(a) NetFlow обележје (b) слика 2D

3x27 pixels. Similarly, for 13 features, images with dimensions of 3x39 pixels were generated.

Evaluation

The attack detection performance of the NetFlow datasets NF-UQ-NIDS was evaluated, reproducing the results of the authors (Sarhan et al., 2021) for binary classification. The evaluation was conducted using 8 features, and the obtained results were compared with our results using 13 features. The additional features were obtained through data pre-processing, including the IP source and destination and their corresponding ports.

To evaluate the performance of the proposed ML and DL models on the NF-UQ-NIDS dataset, an ExtraTrees ensemble classifier was selected based on its demonstrated success in achieving reliable performance on NIDS datasets (Sarhan et al., 2021). Additionally, a simple ANN model was implemented as an ML classifier. The DL model utilized in this study employed a simple CNN architecture and incorporated transfer learning from the VGG16 model.

ExtraTrees classifier

An ExtraTrees ensemble classifier consisting of 50 randomized decision tree estimators was applied using the sklearn library in Python *Extra-*

TreesClassifier(n_estimators=50, class_weight="balanced"). The option “balanced” is set due to the imbalanced dataset. To ensure the datasets are reliably evaluated, five-fold cross-validation is conducted, and average metrics such as accuracy, Area Under the Curve (AUC), precision, recall, F1-score, and the time required to predict a single test sample in microseconds (μs) are calculated using the *sklearn* library. The results are shown in the [Table 3](#).

Table 3 – Binary classification results using ExtraTrees ML

Таблица 3 - Результаты бинарной классификации с использованием ExtraTrees ML

Табела 3 - Резултати бинарне класификације коришћењем ExtraTrees ML

Metrics	8 features	13 features
Accuracy	0.9744	0.9909
AUC	0.9917	0.9940
Recall	0.9672	0.9861
Precision	0.9632	0.9884
F1-score	0.9459	0.9804
Score time (μs)	5.87	5.03

The results show that the 13-feature model performs better than the 8-feature model across all evaluated metrics.

The 13-feature model has an accuracy of 0.9909, which is higher than the 8-feature model’s accuracy of 0.9744. Additionally, the 13-feature model has a higher AUC (0.9940) than the 8-feature model (0.9917), indicating better overall performance in distinguishing between the two classes. The 13-feature model also shows better recall (0.9861) and precision (0.9884) than the 8-feature model (0.9672, 0.9632, respectively), which means it is able to correctly identify more positive samples (higher recall) and make fewer false positive predictions (higher precision) than the 8-feature model. The F1-score is higher for the 13-feature model (0.9804) than for the 8-feature model (0.9459), indicating that it has a more optimal trade-off between precision and recall.

The 13-feature model has a slightly lower time to predict a single test sample than the 8-feature model, with 5.03 μs for the 13-feature model and 5.87 μs for the 8-feature model.

Our results indicate that the additional features provide valuable information that improves the model's ability to distinguish between benign and attack traffic, and ultimately improve the model's attack detection performance.

ANN model

The summary in [Figure 4](#) provides a detailed description of the proposed ANN model architecture. The ANN is based on an input layer with 8 or 13 inputs for both 8 and 13 feature models.

Model: "sequential"		
Layer (type)	Output Shape	Param #
flatten (Flatten)	(None, 8)	0
dense (Dense)	(None, 256)	2304
dense_1 (Dense)	(None, 256)	65792
dense_2 (Dense)	(None, 256)	65792
dense_3 (Dense)	(None, 256)	65792
dense_4 (Dense)	(None, 256)	65792
dense_5 (Dense)	(None, 20)	514
softmax (Softmax)	(None, 20)	0
Total params: 265,986		
Trainable params: 265,986		
Non-trainable params: 0		

Figure 4 – ANN model summary for the 8 features input
Рис. 4 – Краткое описание модели ANN для ввода 8 функций
Слика 4 – Резиме модела ANN за унос од 8 обележја

The evaluation of the ANN model was conducted using a specific configuration, which included the following parameters: *Adamax* optimizer, the learning rate of 0.001, *categorical cross-entropy* loss function, and 30 epochs of training.

The results shown in [Table 4](#) indicate that the addition of four features has significantly enhanced the model's performance. Both models show promising results, with the 8-feature model achieving an accuracy of 0.9285, and the 13-feature model achieving an accuracy of 0.9673. Furthermore, the AUC increased from 0.9806 to 0.9939, indicating the model's improved ability to distinguish between attack and benign samples. The recall increased from 0.8103 to 0.8810, and the precision improved from



Table 4 – Binary classification results using ANN machine learning
Таблица 4 – Результаты бинарной классификации с использованием ANN ML

Табела 4 – Резултати бинарне класификације коришћењем ANN ML

Metrics	8 features	13 features
Accuracy	0.9285	0.9673
AUC	0.9806	0.9939
Recall	0.8103	0.8810
Precision	0.8729	0.9757
F1-score	0.8404	0.9259
Score time (μs)	115.32	100.38

0.8729 to 0.9757. The F1-score also increased from 0.8404 to 0.9259, indicating an overall improvement in performance. Additionally, the prediction time slightly decreased, which is a positive outcome.

Discussion: ExtraTrees Vs ANN

The ExtraTrees with 13 features outperformed the 8-feature model from (Sarhan et al., 2021) with an accuracy of 0.9909 compared to 0.9744.

The ExtraTrees for 8 and 13 features, outperformed the ANN in all the evaluation metrics. However, it is noteworthy that the ANN still achieved a high level of accuracy and showed significant improvement after incorporating the four additional features. The ExtraTrees show better accuracy than the ANN for both the 8 and 13 features. Moreover, both models performed well in terms of the AUC, indicating their ability to distinguish between attack and benign flow. In terms of recall, the ExtraTrees outperformed the ANN for both the 8 and 13-feature models, with consistently better performance observed for the 13-feature model. When it comes to precision, the ExtraTrees using 13 features exhibited better precision metrics. The ExtraTrees using 13 features achieved the highest F1-score, surpassing all other models in performance.

The ExtraTrees model demonstrated a slightly faster score time compared to the ANN model for both the 8 and 13 features.

The results obtained from both the ExtraTrees and ANN models indicate that incorporating the excluded features was more effective in detecting attacks compared to utilizing only 8 features.

CNN model based-NIDS

The process for training a CNN model on NetFlow data involves two key steps: 1) converting 1D NetFlow features into 2D NetFlow images, and 2) inputting the NetFlow image data into the CNN model using both direct training and transfer learning techniques. Transforming 1D NetFlow features into 2D images enables the utilization of the powerful image classification capabilities of CNNs, leading to improved accuracy in NIDSs (Liu et al., 2019).

In this study, two different CNN models were employed. The first model is a simple CNN composed of three convolutional layers. The second model utilized is the widely recognized VGG16, known for its significant contributions to CNN models.

Simple CNN

The summary in Figure 5 provides a detailed description of our simple CNN model architecture, including the arrangement and specifications of each layer. The proposed CNN model is based on an input layer with an input size of (32,32,1).

For the evaluation of the simple CNN model, a specific configuration was employed, incorporating the following parameters: the *Adamax* optimizer, a learning rate of 0.001, the use of *categorical cross-entropy* as the loss function, and training for a total of 30 epochs. The performance results of the proposed simple CNN model for both cases with 8 and 13 features are presented in Table 5.

Based on the obtained results, for the Simple CNN model, using the 13 features with an image size of 3x3 provides the best overall performance, as it achieved the highest accuracy (0.9884), AUC (0.9970), recall (0.9648), Precision (0.9850) and F1-score (0.9747) compared to the other models, suggesting that the additional features contribute valuable information for the classification of the attacks. Accuracy increased from 0.9508 to 0.9884 going from 8 to 13 features with a 3x3 image. It increased further to 0.9686 with a 3x39 image compared to 0.9657 for 3x27 image.

Model: "sequential"		
Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 32, 32, 16)	160
max_pooling2d (MaxPooling2D)	(None, 16, 16, 16)	0
conv2d_1 (Conv2D)	(None, 16, 16, 32)	4640
max_pooling2d_1 (MaxPooling 2D)	(None, 8, 8, 32)	0
conv2d_2 (Conv2D)	(None, 8, 8, 64)	18496
max_pooling2d_2 (MaxPooling 2D)	(None, 4, 4, 64)	0
flatten (Flatten)	(None, 1024)	0
dense (Dense)	(None, 128)	131200
dense_1 (Dense)	(None, 2)	258
Total params: 154,754		
Trainable params: 154,754		
Non-trainable params: 0		

Figure 5 – A Simple CNN model summary
Рис. 5 – Краткое описание модели Simple CNN
Слика 5 – Једноставан резиме CNN модела

The score time tends to increase as the image size grows larger. Among the different image sizes evaluated, the 3x39 image size exhibited the highest score time (178.34 μ s). On the other hand, using 8 features with 3x3 images demonstrated the fastest score time, with a minimal difference compared to the 13 features using the same 3x3 image size.

Among the tested configurations, it seems that utilizing 13 features with a 3x3 image size offers the optimal balance of accuracy, AUC, recall, precision, and F1-score. The inclusion of the four features, combined with the reshaping approach, leads to enhanced performance for NIDSs.

VGG16 model

VGG16 has a relatively straightforward architecture compared to other deep learning models. VGG16 has a hierarchical structure that gradually increases the complexity of feature extraction, allowing it to capture both low-level and high-level features in images. (Van et al., 2017).

In the study, a 32x32x3 input layer is utilized. Two strategies are employed: transfer learning with a pre-trained model on the ImageNet dataset and training the VGG16 model from-scratch. The structure of the adapted

Table 5 – Binary classification results using a simple CNN model
 Таблица 5 – Результаты бинарной классификации с использованием простой модели CNN
 Табела 5 – Резултати бинарне класификације коришћењем једноставног CNN модела

Metrics	8 features		13 features	
	Image 3x3	Image 3x27	Image 3x3	Image 3x39
Accuracy	0.9508	0.9657	0.9884	0.9686
AUC	0.9889	0.9889	0.9970	0.9932
Recall	0.8933	0.8989	0.9648	0.8882
Precision	0.8947	0.9508	0.9850	0.9743
F1-score	0.8940	0.9241	0.9747	0.9293
Score time (μs)	80.89	108.6 3	81.13	178.34

VGG16 model, specifically designed for the binary classification between benign and attack instances, is shown in Figure 6.

Model: "Adapted VGG16"		
Layer (type)	Output Shape	Param #
vgg16 (Functional)	(None, 1, 1, 512)	14714688
flatten (Flatten)	(None, 512)	0
dense (Dense)	(None, 256)	131328
dropout (Dropout)	(None, 256)	0
dense_1 (Dense)	(None, 2)	514
Total params: 14,846,530		
Trainable params: 131,842		
Non-trainable params: 14,714,866		

Figure 6 – Adapted VGG16 model summary
 Рис. 6 – Краткое описание адаптированной модели VGG16
 Слика 6 – Прилагођени резиме VGG16 модела

The evaluation of the adapted VGG16 model involved a specific configuration with the following parameters: *Adamax* optimizer, a learning rate of 0.001, *categorical cross-entropy* as the loss function, and training for 30

epochs. The performances of the VGG16 model trained on both 8 and 13 features are presented in [Table 6](#).

Table 6 – Binary classification results using the VGG16 model

Таблица 6 – Результаты бинарной классификации с использованием модели VGG16

Табела 6 – Резултати бинарне класификације коришћењем VGG16 модела

Metrics	8 features				13 features			
	Image 3x27		Image 3x3		Image 3x39		Image 3x3	
	Pre Trained	From scratch	Pre Trained	From scratch	Pre Trained	From scratch	Pre Trained	From scratch
Accuracy	0.9026	0.9505	0.9012	0.9750	0.9536	0.9670	0.9532	0.9665
AUC	0.9609	0.9875	0.9577	0.9924	0.9885	0.9925	0.9896	0.9930
Recall	0.7739	0.8911	0.7729	0.9162	0.8668	0.9199	0.8693	0.8855
Precision	0.8002	0.8953	0.7958	0.9749	0.9285	0.9369	0.9248	0.9674
F1-score	0.7868	0.8932	0.7842	0.9446	0.8966	0.9283	0.8962	0.9246
Score time (μ s)	346.32	1062.95	363.30	568.34	431.23	876.50	342.89	888.771

Comparing pre-trained and from-scratch models, the results suggest that the from-scratch models tend to achieve superior performance in terms of accuracy, AUC, recall, and F1-score. However, the pre-trained models have lower score time compared to the from-scratch models.

For the 8 feature, the VGG16 model trained from-scratch with a 3x3 image size achieves the highest accuracy (0.9750), AUC (0.9924), Recall (0.9162), Precision (0.9749) and F1-score (0.9446). In the case of the 13 features trained from-scratch, the results show that both image sizes produce comparable outcomes, particularly in terms of accuracy and AUC.

In conclusion, the from-scratch VGG16 models display superior performance in terms of evaluation metrics, while the pre-trained models excel in computational efficiency. This can be attributed to the fact that pre-trained models are not optimized for the specific task of network intrusion detection, as the VGG16 model was originally pre-trained on the ImageNet dataset, which has a different set of features.

Overall, the VGG16 model gives very good results for this network intrusion detection task, with accuracy and AUC over 0.95. This shows that the model has learned the patterns in the NetFlow data very well for detecting network intrusions.

Result summary and discussion

This part presents an overview of the results obtained from various tests of anomaly-based NIDSs. The results show that the ExtraTrees model outperformed all other models for 13 feature inputs. It also showed relatively high recall and precision, which indicates a good balance between identifying true positives and avoiding false positives. Moreover, it had the lowest prediction time (5.03 μ s) among all models, which makes it a good choice for real-time applications. Additionally, using ExtraTrees with 13 features has shown better results than the one of (Sarhan et al., 2021) with the highest accuracy of 0.9909.

The ANN model also demonstrates a good performance with 13 features, but its score time is significantly higher than the ExtraTrees model, at 100.38 μ s.

As for the deep learning models, the VGG16 from-scratch outperformed the pre-trained model in most cases, especially in terms of precision and recall. However, it had a significantly higher prediction time, which could be a disadvantage in some real-time applications. Regarding the proposed simple CNN model, it showed relatively good performance, especially for image 3x3 in both 8 and 13 features input. However, its performance was not as good as the ExtraTrees but is better than VGG16 models, and its prediction time was higher than ExtraTrees but lower than VGG16.

In conclusion, among the tested models, the ExtraTrees model utilizing 13 features demonstrates superior performance in terms of accuracy, AUC, F1-score, and score time. However, for the DL models, the simple CNN model provides better performance compared to the VGG16 models.

Conclusion

This study presents ML and DL models based-NIDSs using Netflow features. The ML models utilized are ExtraTrees and ANN, while the DL models employed include VGG16 and a simple CNN model proposed in this study. The models were trained on the NF-UQ-NIDS dataset.



Our main contribution is the inclusion of the excluded features in the binary classification process, based on the work by (Sarhan et al., 2021). This enhancement aims to improve the performance of the binary classification model in NIDSs to classify the flow data as either "attack" or "benign", resulting in two training datasets: one with the original 8 features and another with the enriched 13 features by using the technique proposed in (Figueiredo et al., 2023). Additionally, both the proposed ML and DL models were evaluated using appropriate performance metrics such as accuracy, recall, precision, and F1-score.

The results demonstrate that the ExtraTrees model outperformed other methods in binary classification using the 13 features and shows better results compared to the one presented in (Sarhan et al., 2021).

These findings suggest that the inclusion of the four excluded features in (Sarhan et al., 2021) contributed to the improved performance of the classifier. The results of this study have practical implications for the development of more efficient and accurate NIDS systems for detecting network attacks.

In future work, the second version of the NF-UQ-NIDS dataset, known as NF-UQ-NIDS-v2, proposed in (Sarhan et al., 2022), will be considered for further investigation. This dataset is advantageous as it contains a larger number of records, totaling 75987976, and includes 43 features. Training machine learning and deep learning models on this dataset can improve their accuracy and robustness due to a larger number of features. This dataset has the potential to enhance the performance of NIDS systems in detecting network attacks.

References

Anitha, A.A. & Arockiam, L. 2019. ANNIDS: Artificial Neural Network based Intrusion Detection System for Internet of Things. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(11), pp. 2583–2588. Available at: <https://doi.org/10.35940/ijitee.K1875.0981119>.

Bahlali, A.R. 2019. *Anomaly-Based Network Intrusion Detection System: A Machine Learning Approach*. Ma thesis, Biskra, Algeria: University of Mohamed Khider, Faculty of Exact, Natural and Life Sciences, Computer Science Department. Available at: <https://doi.org/10.13140/RG.2.2.29553.84325>.

Cahyo, A.N., Hidayat, R. & Adhipta, D. 2016. Performance comparison of intrusion detection system based anomaly detection using artificial neural

network and support vector machine. *AIP Conference Proceedings*, 1755(1, art.number:070011), pp. 1–7. Available at: <https://doi.org/10.3969/j.issn.1002-6819.2015.01.028>.

Cao, C., Panichella, A., Verwer, S., Blaise, A. & Rebecchi, F. 2022. ENCODE: Encoding NetFlows for State-Machine Learning. *arXiv:2207.03890*. Available at: <https://doi.org/10.48550/arXiv.2207.03890>.

Cisco. 2011. *NetFlow Version 9 Flow-Record Format* [online]. Available at: https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html [Accessed: 10 August 2023].

Figueiredo, J., Serrão, C. & de Almeida, A.M. 2023. Deep Learning Model Transposition for Network Intrusion Detection Systems. *Electronics*, 12(2, art.number:293). Available at: <https://doi.org/10.3390/electronics12020293>.

Fosić, I., Žagar, D., Grgić, K. & Križanović, V. 2023. Anomaly detection in NetFlow network traffic using supervised machine learning algorithms. *Journal of Industrial Information Integration*, 33, art.number:100466. Available at: <https://doi.org/10.1016/j.jii.2023.100466>.

Hofstede, R., Čeleda, P., Trammell, B., Drago, I., Sadre, R., Sperotto, A. & Pras, A. 2014. Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX. *IEEE Communications Surveys and Tutorials*, 16(4), pp. 2037–2064. Available at: <https://doi.org/10.1109/COMST.2014.2321898>.

Labonne, M. 2020. *Anomaly-based network intrusion detection using machine learning*. Ph.D. thesis, Institut polytechnique de Paris. [online]. Available at: <https://theses.hal.science/tel-02988296> [Accessed: 10 August 2023].

Liu, X., Tang, Z. & Yang, B. 2019. Predicting Network Attacks with CNN by Constructing Images from NetFlow Data. In: *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. Washington, DC, USA, pp.61–66, May 27-29. Available at: <https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00022>.

Rizvi, S., Scanlon, M., McGibney, J. & Sheppard, J. 2023. Deep Learning Based Network Intrusion Detection System for Resource-Constrained Environments. In: *Goel, S., Gladyshev, P., Nikolay, A., Markowsky, G. & Johnson, D. (Eds.) Digital Forensics and Cyber Crime. ICDF2C 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Boston, MA, 508, pp.355–367, November 16-18. Cham: Springer. Available at: https://doi.org/10.1007/978-3-031-36574-4_21.

Sarhan, M., Layeghy, S., Moustafa, N. & Portmann, M. 2021. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. In: *Deze, Z., Huang, H., Hou, R., Rho, S. & Chilamkurti, N. (Eds.) Big Data Technologies and Applications. BDTA WiCON 2020 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Virtual Event, 371, pp.117–135, December 11. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-72802-1_9.



Sarhan, M., Layeghy, S. & Portmann, M. 2022. Towards a Standard Feature Set for Network Intrusion Detection System Datasets. *Mobile Networks and Applications*, 27, pp. 357–370. Available at: <https://doi.org/10.1007/s11036-021-01843-0>.

Tufan, E., Tezcan, C. & Acartürk, C. 2021. Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network. *IEEE Access*, 9, pp. 50078–50092. Available at: <https://doi.org/10.1109/ACCESS.2021.3068961>.

Van, N.T., Tinh, T.N. & Sach, L.T. 2017. An anomaly-based network intrusion detection system using Deep learning. In: *2017 International Conference on System Science and Engineering (ICSSE)*. Ho Chi Minh City, Vietnam, pp.210-214, September 11. Available at: <https://doi.org/10.1109/ICSSE.2017.8030867>.

Аномальная система обнаружения вторжений в сеть на основе NetFlow с использованием машинного/глубокого обучения

Туати Б. Адли, **корреспондент**, Салем-Билал Б. Амокране, Бобан З. Павлович, Мохамед Зуауи М. Лаидуни, Таки-эддине Ахмед А. Беняхия

Университет обороны в г. Белград, Военная академия, Департамент телекоммуникаций и информатики, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 20.23.25 Информационные системы с базами знаний,
49.33.29 Сети связи

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Системы обнаружения аномалий на основе сетевого обнаружения вторжений (NIDS) стали ценным инструментом, особенно в области военного применения, для защиты сетей от кибератак, с фокусом на данных Netflow для идентификации нормальных и аномальных паттернов. В данной статье исследуется эффективность моделей машинного обучения (ML) и глубокого обучения (DL) на основе аномалий в NIDS с использованием общедоступного набора данных NF-UQ-NIDS, использующего данные Netflow, с целью повышения защиты сети.

Методы: Авторы Sarhan, M., Layeghy, S., Moustafa, N. и Portmann, M. в своем докладе на конференции «Big Data Technologies and Applications», проведенной в 2021 году использовали этап предобработки, на котором выбираются 8 признаков для фазы обучения из доступных 12 признаков. Были исключены IP-адреса исходных и целевых узлов, а также связанные с ними порты. Новизна данной статьи заключается во включении всех доступных функций на этапе обучения с использованием различных алгоритмов классификации ML и DL, таких как ExtraTrees, ANN, простая модель CNN и VGG16 при бинарной классификации.

Результаты: Производительность моделей классификации оценивается с использованием метрик, таких как точность, полнота и т. д., что обеспечивает комплексный анализ полученных результатов. Результаты показывают, что модель ML ExtraTrees превосходит все остальные модели при использовании признаков на этапе предобработки и достигает 99,09% точности классификации, по сравнению с 97,25% в эталонном наборе данных.

Выводы: Исследование показало высокую эффективность различных алгоритмов классификации моделей ML и DL в NIDS с использованием базы данных Netflow.

Ключевые слова: сетевые системы обнаружения вторжений (NIDS), характеристики Netflow, машинное/глубокое обучение, аномальный NIDS.

Систем откривања аномалија у мрежи на бази NetFlow протокола применом машинског/дубоког учења

Туати Б. Адли, **аутор за преписку**, Салем-Билал Б. Амокрание, Бобан З. Павловић, Мохамед Зуауи М. Лаидуни, Таки-еддине Ахмед А. Бенјахија

Универзитет одбране у Београду, Војна академија, Катедра телекомуникација и информатике, Београд, Република Србија

ОБЛАСТ: рачунарске науке, телекомуникације, сајбер безбедност

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад



Сажетак:

Увод/циљ: Проналажење мрежних аномалија, базирано на примени система за детекцију злонамерних упада у мрежу (NIDS), представља изузетно вредан алат, посебно у војним применама, за заштиту мрежа од сајбер напада, са посебним фокусом на Netflow податке ради идентификације нормалних и инцидентних ситуација. У овом раду је спроведено истраживање које анализира ефикасност у борби против аномалија применом модела машинског учења (ML) и дубоког учења (DL) у NIDS-у коришћењем јавно доступне базе података NF-UQ-NIDS која садржи Netflow податке, ради побољшања заштите мреже.

Метод: Аутори Sarhan, M., Layeghy, S., Moustafa, N. и Portmann, M. у раду са конференције Big Data Technologies and Applications, из 2021. године, користили су предобраду у којој се 8 обележја издваја за фазу тренинга од укупно 12 доступних обележја. Посебно су изузете изворне и одређене IP адресе, као и њихови припадајући портови. Главни допринос овог рада односи се на укључивање свих доступних обележја у фазу тренинга, коришћењем различитих алгоритама класификације ML и DL, као што су ExtraTrees, ANN, једноставни CNN и VGG16 за бинарну класификацију.

Резултати: Перформансе анализираних класификационих модела евалуиране су помоћу неколико метрика (тачност, одзив, прецизност и друго), чиме је омогућена свеобухватна компарација добијених резултата. У завршној анализи резултати показују да ML модел ExtraTrees надмашује све остале моделе користећи предложену предобраду свих доступних обележја, постигавши тачност класификације од 99,09%, у поређењу са 97,25% у референтном скупу података.

Закључак: Спроведено истраживање анализира ефикасност различитих алгоритама класификације ML и DL модела у NIDS-у коришћењем базе Netflow.

Кључне речи: систем откривања упада у мрежу (NIDS), Netflow обележја, машинско учење (ML), дубоко учење (DL).

Paper received on / Дата получения работы / Датум пријема чланка: 18.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 01.12.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 02.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier
(<http://vtg.mod.gov.rs>, <http://втр.мо.унп.срб>). This article is an open access article distributed under
the terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier" (<http://vtg.mod.gov.rs>, <http://втр.мо.унп.срб>). Данная статья в открытом доступе
и распространяется в соответствии с лицензией "Creative Commons"
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(<http://vtg.mod.gov.rs>, <http://втр.мо.унп.срб>). Ово је чланак отвореног приступа и дистрибуира се
у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).





Cybersecurity attacks: which dataset should be used to evaluate an intrusion detection system?

Danijela D. Protić^a, Miomir M. Stanković^b

^a Serbian Armed Forces, General Staff, Department for Telecommunication and Informatics, Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia,
e-mail: danijelaprotic318@gmail.com, **corresponding author**,
ORCID iD: <https://orcid.org/0000-0003-0827-2863>,

^b Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Republic of Serbia,
e-mail: miomirdanijela@gmail.com,
ORCID iD: <https://orcid.org/0009-0002-8504-6966>

DOI: 10.5937/vojtehg71-46524; <https://doi.org/10.5937/vojtehg71-46524>

FIELD: computer sciences, electronics, telecommunications

ARTICLE TYPE: original scientific paper

Abstract:

Introduction: Analyzing the high-dimensional datasets used for intrusion detection becomes a challenge for researchers. This paper presents the most often used data sets. ADFA contains two data sets containing records from Linux/Unix. AWID is based on actual traces of normal and intrusion activity of an IEEE 802.11 Wi-Fi network. CAIDA collects data types in geographically and topologically diverse regions. In CIC-IDS-2017, HTTP, HTTPS, FTP, SSH, and email protocols are examined. CSE-CIC-2018 includes abstract distribution models for applications, protocols, or lower-level network entities. DARPA contains data of network traffic. ISCX 2012 dataset has profiles on various multi-stage attacks and actual network traffic with background noise. KDD Cup '99 is a collection of data transfer from a virtual environment. Kyoto 2006+ contains records of real network traffic. It is used only for anomaly detection. NSL-KDD corrects flaws in the KDD Cup '99 caused by redundant and duplicate records. UNSW-NB-15 is derived from real normal data and the synthesized contemporary attack activities of the network traffic.

Methods: This study uses both quantitative and qualitative techniques. The scientific references and publicly accessible information about given dataset are used.

Results: Datasets are often simulated to meet objectives required by a particular organization. The number of real datasets are very small compared to simulated dataset. Anomaly detection is rarely used today.

Conclusion: The main characteristics and a comparative analysis of the data sets in terms of the date they were created, the size, the number of features, the traffic types, and the purpose are presented.

Key words: ADFA, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA, ISCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD, UNSW-NB15.

Introduction

With the increase in computer applications and large amounts of data being processed around the world, the need for data protection has multiplied in recent years. Intrusion detection systems (IDSs) are the primary line of defense that protects networks from malicious attacks. The IDS is generally classified into three installation types: host-based, network-based, and hybrid (Protić & Stanković, 2020). The network-based intrusion detection systems can also be divided into signature-based and anomaly-based, both of which are inspired by the human immune system. The signature-based (misuse-based) IDS protects the network by proactively detecting the presence of known attacks by comparing unknown network traffic against a database of known attack signatures. It detects malicious software based on the knowledge gathered through known attacks. The main advantage of signature-based IDSs is their high detection speed. The main disadvantage of signature-based IDSs is the difficulty in detecting unknown attacks. Anomaly-based IDSs detect unusual network behavior by detecting deviations from a statistical model of normal network behavior and by looking for activities that deviate from the created model. The main advantage of anomaly-based IDSs is the detection of unknown attacks. The main challenge in anomaly detection is determining what is identified as normal.

The main problem in intrusion detection is the huge amount of data. Since the type of features and the number of instances determine the applicability of IDSs, analyzing high-dimensional datasets becomes a challenge for researchers. Simulated datasets or datasets obtained from real network traffic differ in size, number of features, purpose, type of attacks, etc. (Omar et al, 2013; Jie et al 2018). A number of authors examine, describe and compare various datasets such as ADFA-LF, ADFA-WD, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA 98, SCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD and UNSW-NB15 data sets, which differ in the number of features, type of attacks and purpose (Protić, 2018; Bohara et al, 2020; Borisniya & Patel, 2015; Thakkar &

Lohiya, 2020; Khraisat et al, 2019; Ferriyan et al, 2021; Serkani et al, 2019; Mighan & Kahani, 2021; Soltani et al, 2021).

In this paper, we present the main characteristics and a comparative analysis of the given data sets in terms of the date they were created, their size, attacks/anomalies, the number of their features, their traffic types, and their purpose.

Data sets

A list of ADFA-LF, ADFA-WD, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA 98, ISCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD, and UNSW-NB15 data sets, with comprehensive descriptions, is given in the text that follows.

ADFA-LD and ADFA-WD datasets

In 2013, the Australian Defense Force Academy (ADFA) developed two data sets containing records from Linux/Unix (ADFA-LD) and Windows (ADFA-WD) systems, respectively. The datasets are free to use for research purposes only. The datasets are evaluated by the host-based IDS (HIDS) (system-call-based). The ADFA-LD consists of system call traces obtained from a temporary local Linux server, and six cyberattacks (Xie et al, 2014). The ADFA-WD is a set of DLL access requests and system calls from a variety of hacking attacks (2015). Both ADFA datasets are the benchmarks for evaluating IDS based on system calls.

ADFA-LD

System call traces are used by HIDS to detect attacks on target systems. ADFA-LD consists of 833 normal training traces, 4372 normal validation traces, and 746 attack traces, all collected under the Linux system, namely: Adduser (91), Hydra_FTP (162), Hydra_SSH (176), Java_Meterpreter (124), Meterpreter (75), and Web Shell (118). Each system call is represented by an integer (Zhang et al, 2020).

ADFA-WD

ADFA-WD is high-quality collection of DLL access requests and system calls for a variety of hacking attacks. The dataset was gathered on a Windows XP SP2 host. The default firewall was enabled, and Norton AV 2013 was installed to detect only sophisticated attacks and ignore low-level attacks. The operating system environment allowed for sharing and the configuration of network printers. It was running applications like webserver, database server, FTP server, streaming

media server, PDF reader, and so on. A total of 12 known vulnerabilities for installed applications were exploited using the Metasploit framework and other custom approaches. ADFA-WD is composed of 355 normal training traces, 1827 normal validation traces, and 5542 attack traces (Borisniya & Patel, 2015).

AWID

The Aegean Wi-Fi Intrusion Detection (AWID) data set is a publicly available labeled data set that was created in 2016 and is based on actual traces of normal and intrusion activity of an IEEE 802.11 Wi-Fi network (Natkaniec & Bednarz, 2023). Character data and imbalance between attack and normal data characterize AWID, which may influence IDS evaluation (Chen et al, 2021). The dataset contains 155 distinct features and 14 simulated existing attacks (Sudaroli Vijayakumar & Ganapathy, 2018).

Table 1 – AWID attack classes
Таблица 1 – Классы кислотны атак
Табела 1 – AWID класе напада

Attack class		Description
Flooding	Deauthentication	Sending a large number of deauthentication management frames with specific destination MAC address. Results in the connection loss of a client with MAC address or disconnection of all clients that receive the frame.
	Disassociation	Similar to a deauthentication flood, uses disassociation management frames.
	Block Acknowledge	The attacker sends a fake ADDBA message on behalf of a real client with high sequence numbers, causing the AP to not accept frames.
	Authentication request	Involves sending a large number of authentication request frames; AP overloads can cause it to shut down and drop the wireless network.
	Fake Power Saving	Takes advantage of the Power Saving mechanism by sending a null frame on behalf of the victim with the power saving bit set to 1.
	Clear-to-Send	Relies on the Request-to-Send/Clear-to-Send mechanism; causes STA to wait for a transmission that never occurs;
	Request-to-Send	Similar to a CTS flood, involves sending a large number of RTS frames, which prevents other clients from accessing the medium.
	Beacon	Involves sending multiple beacon frames with different SSIDs; causes confusion for end users attempting to connect to the correct network.
	Probe Request	Drain resources from the AP; sends large number of probe request frames.
Probe Response	Involves flooding a victim with a large number of probe response frames.	
Impersonation	HoneyPot	Wireless network created by an attacker designed to attract unsuspecting victims.
	Evil Twin	Wireless network created by an attacker that is an exact replica of an existing network used by the victim.
	Caffe Latte	Attacking wireless networks where direct access to the access point is not necessary.
	Hirte	Extension of the Caffe Latte attack in which ARP packets are fragmented to collect more IVs from the connected device; easier to crack WEP key.
Injection	ARP Injection	Injecting a fake ARP Request into the wireless network
	Fragmentation	The attacker first performs a fake authentication with the Access Point and then receives at least one frame. Attacker can guess the first 8 bytes of the keystream. Then constructs a frame with a known payload, breaks it into fragments.
	Chop-Chop	Dropping the last byte of the encrypted frame and then guessing a valid Integrity Check Value (ICV).

IEEE 802.11i, also known as WPA2, was an improvement to the original IEEE 802.11 standard that aimed to improve protocol security. It significantly augments and expands the well-known AWID2 corpus by capturing and analyzing traces of wide range of IEEE 802.1X Wi-Fi network attacks. AWID3 is expected to be a great improvement in the design and evaluation of IDSs. Attacks from the wireless MAC layer to higher ones that are common to IEEE 802.3 networks.

CAIDA

Center of Applied Internet Data Analysis (2002-2016) created the CAIDA data set and made it widely available to the research community who provide data or network access. CAIDA contains three datasets: CAIDA OC48 (contains various types of data observed on an OC48 link in San Jose), CAIDA DDoS (contains one hour of DDoS attack traffic divided into 5-minute pcap files), and CAIDA Internet Traces 2016 (CAIDA Equinix-Chicago High-speed Internet backbone passive traffic traces) are three datasets contained in CAIDA. CAIDA datasets collect a variety of data types in geographically and topologically diverse regions. Because of numerous flows, these benchmarking are ineffective (Proebstel, 2008).

CAIDA OC48

The CAIDA OC48 Peering Point Traces Dataset (2002-2003) contains anonymized passive traffic traces collected from large ISP's west coast OC48 peering point from 2002 to 2003. The payload is removed and IP addresses anonymized using CryptoPAN prefix-preserving anonymization tool with the same key for all traces in this dataset. The CAIDA OC48 data is useful for research on the internet traffic characteristics such as application breakdown, security events, topological distribution, and flow volume and duration. These traces can be read by any program that supports the pcap (tcpdump) format (CAIDA, 2020a).

CAIDA DDoS

This dataset contains the traffic traces of a flooding DDoS attack over a one-hour period. The attack's goal was to consume the computing resource of the targeted server. IP addresses have been pseudonymized, and their payloads and non-attack traffic have been removed from the dataset for security reasons, limiting its usability. This dataset found its application in detecting low rate stealthy as well as high-rate flooding DDoS attacks (Behal & Kumar, 2016). This type of DoS attack attempts to prevent access to the targeted server by consuming

computing resources on the server and by consuming all computing resources on the server as well as all network bandwidth connecting the server to the Internet. The one-hour trace is divided into 5-minute pcap files. Only attack traffic to the victim and responses to the attack from the victim are included in the traces. Traces in this dataset are anonymized using CryptoPan prefix-preserving anonymization using a single key. The payload has been removed from all packets (CAIDA, 2020b).

CAIDA Internet Traces

The CAIDA Internet Traces dataset contains three subsets:

- 2008-2014: contains anonymized passive traffic traces from CAIDA's equinix-chicago and equinix-sanjose high-speed Internet backbone connections.
 - o the first available traffic trace is an hourly traffic trace collected during the DITL 2008 measurement event;
 - o contains anonymized packet headers in pcap format for a single direction of the bidirectional OC129 link at the equinix-chicago monitors;
 - o a one-hour recording resulted in 83GB compressed pcap files;
 - o a monthly one-hour trace is collected;
 - o traffic traces are anonymized using CryptoPan prefix-preserving anonymization;
 - o during recording, packets are truncated to a specified length (64-96 B) to avoid excessive packet loss due to disk I/O overload.
 - o payload is removed from all packets; only header information at the transport layer is retained;
 - o the Endace network cards used to record these traces provide timestamps with nanosecond precision;
- 2015-2016: contains anonymized passive traffic traces from CAIDA's equinix-chicago monitors on high-speed Internet backbone links.
- 2018-2019: contains anonymized passive traffic traces from CAIDA's equinix-nyc monitor.

Starting with the 2010 traces, the original nanosecond timestamps are provided as separate ascii files alongside the pcap files. The traces can be read with any software that can read pcap (tcpdump) files (CAIDA, 2019).

CIC-IDS-2017

In 2018, the Canadian Institute for Cybersecurity (CIC) created the CIC-IDS-2017 dataset. The dataset consists of ~2.8 million benign and malicious records with 77 features and ~128 thousands current common attack covering 11 criteria (see Table 2) with 14 types of attacks (Sharafaldin et al, 2018). For this dataset, the authors examined the abstract behavior of 25 users based on HTTP, HTTPS, FTP, SSH, and email protocols. The attacks implemented include brute-force FTP, brute-force SSH, DoS, Heartbleed, web attack, Infiltration, Botnet and DDoS (UNB University of New Brunswick: Canadian Institute for Cybersecurity, 2018).

Table 2 – CIC-IDS-2017 criteria and description
Таблица 2 – CIC-IDS-2017 критериуми и описание
Табела 2 – CIC-IDS-2017 критеријуми и опис

No	Criteria	Description
1	Complete Network configuration	A complete network topology includes Modem, Firewall, Switches, Routers, and presence of a variety of operating systems such as Windows, Ubuntu and Mac OS X.
2	Complete Traffic	By having a user profiling agent and 12 different machines in Victim-Network and real attacks from the Attack-Network.
3	Labelled Dataset	Section 4 and Table 2 show the benign and attack labels for each day. Also, the details of the attack timing will be published on the dataset document.
4	Complete Interaction	As Figure 1 shows, we covered both within and between internal LAN by having two different networks and Internet communication as well.
5	Complete Capture	Because we used the mirror port, such as tapping system, all traffics have been captured and recorded on the storage server.
6	Available Protocols	Provided the presence of all common available protocols, such as HTTP, HTTPS, FTP, SSH and email protocols.
7	Attack Diversity	Included the most common attacks based on the 2016 McAfee report, such as Web based, Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot and Scan covered in this dataset.
8	Heterogeneity	Captured the network traffic from the main Switch and memory dump and system calls from all victim machines, during the attacks execution.
9	Feature Set	Extracted more than 80 network flow features from the generated network traffic using CICFlowMeter and delivered the network flow dataset as a CSV file. See our PCAP analyzer and CSV generator.
10	MetaData	Completely explained the dataset which includes the time, attacks, flows and labels in the published paper.
11	Day, Date, Description, Size	Days of normal network activity and attacks.

CSE-CIC-2018

A joint project between the Communication Security Establishment (CSE) and the CIC produced the CSE-CIC-2018 dataset, which included detailed descriptions of intrusions along with abstract distribution models for applications, protocols, or lower-level network entities.

The final data set included seven different attack scenarios: Brute-Force, Hearth Bleed, Botnet, DoS, DDoS, Web Attacks and Infiltration (see Table 3). The attack infrastructure consists of 50 machines and the victim organization consists of 5 departments and includes 420 machines and 30 servers (Kali Linux).

Table 3 – CSE-CIC-2018 attacks and tools
Таблица 3 – CSE-CIC-2018 атаки и инструменты
Табела 3 – CSE-CIC-2018 напади и алати

Attack	Tools	Victim
Bruteforce (1 day)	FTP – Patator; SSH – Patator	Ubuntu 16.4 (Web Server)
DoS (1 day)	Hulk, GoldenEye, Slowloris, Slowhttptest	Ubuntu 16.4 (Apache)
DoS (1 day)	Heartleech	Ubuntu 12.04 (Open SSL)
Web (2 days)	Damn Vulnerable Web App (DVWA); In-house selenium framework (XSS, Brute-force);	Ubuntu 16.4 (Web Server)
Infiltration (2 days)	First level: Dropbox download in a windows machine; Second Level: Nmap and portscan;	Windows Vista & Macintosh
Botnet (1 day)	Ares: remote shell, file upload/download, capturing screenshots and key logging	Windows Vista, 7, 8.1, 10 (32-bit) and 10 (64-bit)
DDoS & PortScan (2 days)	Low Orbit Ion Canon for UDP, TCP, HTTP requests	

The dataset includes the captured network traffic and the system logs of each machine, as well as 80 features extracted from the captured traffic using CICFlowMeter-V3. CICFlowMeter is a network traffic flow generator that produces bidirectional flows (Biflow), where the first packet determines the forward (source to destination) and reverse (destination

to source) directions, hence the 83 statistical features such as Duration, Number of packets, Number of bytes, Length of packets, etc.

The application output is in the CSV file format with six columns labeled for each flow, namely FlowID, SourceIP, DestinationIP, SourcePort, DestinationPort, and Protocol with more than 80 network traffic features. Normally, TCP flows are terminated when the connection is broken (by the FIN packet), while UDP flows are terminated by a flow timeout. The flow timeout value can be set arbitrarily according to the particular scheme, e.g. 600s for TCP and UDP. A list of extracted features can be found at (UNB University of New Brunswick: Canadian Institute for Cybersecurity, 2017).

The dataset shows class imbalance as about 17% of the instances contain abnormal traffic. The data set is not used as a treasure trove for signature-based IDS, but to promote anomaly-based intrusion detection (Levy & Khoshgoftar, 2020).

1998/1999 DARPA intrusion detection evaluation dataset

The DARPA dataset was produced by the Lincoln Laboratory of the Massachusetts Institute of Technology (MIT) in 1998 and 1999. The dataset consists of two parts: online and offline. All network traffic including the total payload of each packet, was recorded in tcp dump format and made available for analysis. In these evaluations, the data was in the form of sniffed network traffic, Solaris BSM audit data, Windows NT audit data (1999 DARPA), and file system snapshots, and an attempt was made to identify intruders that had penetrated a test network during the data collection period. The IDSs are tested in an offline evaluation using network traffic and audit logs collected from a simulated network (Lippmann et al, 2000). The test network consisted of a mixture of real and simulated machines; background traffic was artificially generated by the real and simulated machines while attacks were carried out against the real computers.

The DARPA dataset is used to measure the detection rate and false alarm rate for network traffic consisting of four types of attacks: Denial of Service (DoS), probing (Probe/Scan attacks), and two types of privilege escalation attacks – User to Root (U2R) and Remote to Local (R2L). The 1998 DARPA Intrusion Detection Evaluation Dataset (1998 DARPA) contains 41 features and a class. In total, there are 409021 records with classes labeled as either normal or one of the 22 attack types. However, only 409020 records can be used, primarily because of errors in the records within the dataset (see Table 4) (Khor et al, 2009).

Table 4 – 1998 DARPA record types
 Таблица 4 – 1998 DARPA виды записи
 Табела 4 – 1998 DARPA класе записа

Record type	Number of records
Normal	97277
Denial of Service	391458
Probe	4107
Remote to Local	1126
User to Root	52

The DARPA 1999 consists of weeks 1-3 of training data and weeks 4-5 of testing data. Weeks one and three contain normal traffic and week two contains labeled attacks (Thomas et al, 2008). The descriptions of the attacks are listed in Table 5.

Table 5 – DARPA attack classes and descriptions
 Таблица 5 – DARPA классы атак и описание
 Табела 5 – DARPA класе напада и опис

Attack class	Attack type	Description
Probe	ipsweep, lsdomain, mscan	Scans a computer network or a DNS server to find valid IP addresses
	portsweep, mscan	Scans a computer network or a DNS server to find active ports
	queso, mscan	Scans a computer network or a DNS server to find hostoperating system types
	satan	Scans a computer network or a DNS server to find known vulnerabilities
DoS (Designed to disrupt a host or network service)	selfping	Solaris operating system crash
	tcpreset	Active termination of all TCP connections to a specific host
	arpoison	Corruption of ARP cache entries for a victim not in others' caches
	crashiis	Crashes the Microsoft Windows NT web server
	Dosnuke	Crashes Windows NT
R2L (Attacker who does not have an account on a victim machine)	quest, dict	Gains local access to the machine
	ppmacro	Exfiltrates files from the machine
	framespoof	Modifies data in transit to the machine
	ppmacro	NT power point macro attack
	framespoof	Man-in-middle web browser attack
	netbus	NT trojan-installed remote administration tool
	sshtrojan	Linux trojan SSH server
U2R (Local user on a machine is able to obtain privileges)	ncftp	Linux FTP file access-utility with a bug that allows remote commands to run on a local machine
	nftsdos, sqlattack	Secret attacks, where a user who is allowed to access the special files exfiltrates them

Protić. D. et al, Cybersecurity attacks: which dataset should be used to evaluate an intrusion detection system? 970-995

The DARPA 1999 test data consisted of 190 instances of Probe (37), DoS (63), R2L (53) and U2R (37) attacks. The following types of attacks were added to the training set (see Table 6).

*Table 6 – DARPA attack types
Таблица 6 – DARPA классы атак
Табела 6 – DARPA класе напада*

Attack class	Attack type
DoS	apache2, back, land, mailbomb, neptune, pod, processtable, teardrop, smurf, syslogid, udpstorm, warexzlient
Probe	ntinfoscan, iligal-sniffer
R2L	ftpwrite, httptunnel, imap, named, netcat, phf, sendmail, snmpget, xlock, xsnoop
U2R	casesen, eject, fdformat, flbconfig, loadmodule, nukewp, perl, ppmacro, ps, secret, srchole, xterm, yaga

The main criticisms of the DARPA data relate to: (1) the software used to generate traffic on the testbed, which is not publicly available, (2) the evaluation criteria do not take into account the system resources used, (3) the ease of use, (4) the type of system it is on, (5) the procedures used in building the dataset and performing the evaluation, (6) the background data does not include background noise such as packet storms, (7) strange packets, (8) anomalous Internet traffic that is not caused by malicious behavior, etc.

ISCX 2012

The ISCX 2012 dataset has two profiles. Alpha performs various multi-stage attacks, and Beta generates actual network traffic with background noise. The dataset contains network traffic for HTTP, SMTP, SSH, IMAP, POP3, and FTP protocols but no HTTPS traces. The distribution of simulated attacks is not based on real world statistics (Sharafaldin et al, 2018).

The dataset shows realistic network behavior and includes various intrusion scenarios. It is shared as a complete network capture with all internal traces to evaluate the payloads for a deep data packet analysis. In addition, the dataset includes seven days of both normal and malicious network traffic activity.

The dataset was created using profiles that contain abstract representations of network traffic actions and behaviors. ISCX-IDS 2012 contains two different profiles to create network traffic behaviors and scenarios (Table 7) (Khan et al, 2019).

Table 7 – ICSX 2012 criteria
 Таблица 7 – ICSX 2012 критериуми
 Табела 7 – ICSX 2012 критеријуми

No	Criteria	Description
1	Realistic network traffic	Ideally, a dataset should not exhibit any unintended properties, both network and traffic wise. This is to provide a clearer picture of the real effects of attacks over the network and the corresponding responses of workstations. For this reason, it is necessary for the traffic to look and behave as realistically as possible. This includes both normal and anomalous traffic. Any artificial post-capture trace insertion will negatively affect the raw data and introduce possible inconsistencies in the final dataset. Consequently, all such adjustments are highly discouraged.
2	Labelled Dataset	A labeled dataset is of immense importance in the evaluation of various detection mechanisms. Hence, creating a dataset in a controlled and deterministic environment allows for the distinction of anomalous activity from normal traffic; therefore, eliminating the impractical process of manual labeling.
3	Total interaction capture:	The amount of information available to detection mechanisms are of vital importance as this provides the means to detect anomalous behaviour. In other words, this information is essential for post-evaluation and the correct interpretation of the results. Thus, it is deemed a major requirement for a dataset to include all network interactions, either within or between internal LANs.
4	Complete Capture	Privacy concerns related to sharing real network traces have been one of the major obstacles for network security researchers as data providers are often reluctant to share such information. Consequently, most such traces are either used internally, which limits other researchers from accurately evaluating and comparing their systems, or are heavily anonymized with the payload entirely removed resulting in decreased utility to researchers. In this work, the foremost objective is to generate network traces in a controlled testbed environment, thus completely removing the need for any sanitization and thereby preserving the naturalness of the resulting dataset.
5	Diverse intrusion scenarios	Attacks have increased in frequency, size, variety, and complexity in recent years. The scope of threats has also changed into more complex schemes, including service and application-targeted attacks. Such attacks can cause far more serious disruptions than traditional brute force attempts and also require a more in-depth insight into IP services and applications for their detection. Through executing attack scenarios and applying abnormal behaviour, the aim of this objective is to perform a diverse set of multistage attacks; each carefully crafted and aimed towards recent trends in security threats. This objective often labels many of the available datasets as ineffective and unfit for evaluating research results.
6	Day, Date, Description, Size	7 days of normal network activity and attacks

Protić. D. et al, Cybersecurity attacks: which dataset should be used to evaluate an intrusion detection system? 970-995

The ISCX IDS 2012 dataset is publicly available for researchers at (UNB University of New Brunswick: Canadian Institute for Cybersecurity, 2012).

KDD Cup '99

The KDD Cup '99 dataset is a collection of data transfer from a virtual environment and used for 5th Knowledge Discovery and Data Mining Tools competition. It is a subset of the 1998 DARPA dataset collected by simulating network traffic in a medium sized U.S. Air Force LAN (TCP dump data) over a nine-week period.

The dataset was collected and distributed at the Massachusetts Institute of Technology (MIT) Lincoln Laboratory. The KDD Cup '99 consists of the full KDD Cup '99 dataset, which includes simulation of normal connections and four attack classes (Probe, DoS, R2L, U2R), a 10% KDD dataset for training the classifiers, and a KDD test dataset intended for testing (Gifty Jeya et al, 2012, pp.28-32).

The structure of the full dataset is given in Table 8.

Table 8 – KDD Cup '99 file content
Таблица 8 – KDD Cup '99 содержание файлов
Табела 8 – KDD Cup '99 садржај фајлова

File	File content
kddcup.names	List of features
kdd.data.gz	Full data set (uncompressed)
kdd.cup.data_10_percent.gz	10% subset (compressed)
kddcup.newtestdata_10_percent_unlabeled.gz	1.4M, 45M uncompressed
kddcup.testdata.unlabeled.gz	11.2M, 430M uncompressed
kddcup.testdata.unlabeled_10_percent.gz	1.4M, 45M uncompressed
corrected.gz	Test data with corrected labels
training_attack_types	List of attack types
typo-correction.txt	Short description of corrections to the data set

The full KDD Cup '99 dataset contains 4,898,431 single connection records, each of which consists of 41 features labeled as normal or attacks (Tavallaee et al, 2009).

The number of instances is given in Table 9. The attack classes are described in Table 10.

Table 9 – KDD Cup '99 instance number
 Таблица 9 – Номер случая в базе KDD Cup '99
 Табела 9 – Број инстанци у KDD Cup '99 бази

Attack class	Training set	10% Training set	Test set
Normal	492,708	97,278	60,593
Probe	41,102	4,107	4,166
DoS	3,883,370	391,458	229,853
R2L	1,126	1,126	16,347
U2R	52	52	70

Table 10 – KDD Cup '99 attack classes
 Таблица 10 – Классы атак в базе KDD Cup '99
 Табела 10 – Класе напада у бази KDD Cup '99

Attack class	Attack type
Probe	ipsweep, nmap, portsweep, satan
DoS	back, land, neptune, pod, smurf, teardrop
R2L	fpwrite, spy, phf, guesspasswd, imap, warezclient, warezmaster, multihop
U2R	rootkit, perl, loadmodule, bufferoverflow

The features describing the connections can be classified into four categories:

- *Basic features* – determined from the packet header without examining the contents of the packet.
- *Content features* – determined by analyzing the content of the TCP packet (number of unsuccessful attempts to login to the system).
- *Time features* – determine the duration of the connection from a source IP address to a destination IP address. The connection is a sequence of data packets that begin and end at predefined times.
- *Traffic features* – are based on a window that has an interval of a certain number of connections (suitable for describing attacks that last longer than the interval of the specific time features).

The features are listed in Table 11.

Table 11 – KDD Cup '99 features
Таблица 11 – Атрибуты базы KDD Cup '99
Табела 11 – Атрибуту у бази KDD Cup '99

No	Feature	Description
1.	duration	length of connection
2.	protocol type	type of protocol (TCP, UDP...)
3.	service	destination service (ftp, telnet...)
4.	flag	status of connection
5.	source bytes	No. of B from source to destination
6.	destination bytes	No. of B from destination to source
7.	land	If the source=destination address are the same land=1/if not, 0
8.	wrong fragments	No. of wrong fragments
9.	urgent	No. of <i>urgent</i> packets
10.	hot	No. of <i>hot</i> indicators
11.	failed logins	No. of unsuccessful attempts at login
12.	logged in	If logged in=1/if login failed 0
13.	# compromised	No. of <i>compromised</i> states
14.	root shell	If a command interpreter with a root account is running root shell=1/if not, then 0
15.	su attempted	If <i>su</i> command is attempted=1, otherwise=0
16.	# root	No. of <i>root</i> accesses
17.	# file creations	No. of operations that create new files
18.	# shells	No. of active command interpreters
19.	# access files	No. of file creation operations
20.	# outbound cmds	No. of outbound commands in an ftp session
21.	is host login	is host login=1 if the login is on the <i>host login</i> list/if not 0
22.	is guest login	If a guest is logged into the system = 1 otherwise 0
23.	count	No. of connections to the same host as the current connection at a given interval
24.	srv count	No. of connections to the same service as the current connection at a given interval
25.	serror rate	% of connections with SYN errors
26.	srv error rate	% of connections with SYN errors
27.	rerror rate	% of connections with REJ errors
28.	srv rerror rate	% of connections with REJ errors
29.	same srv rate	% of connections to the same service
30.	diff srv rate	% of connections to different services
31.	srv diff host rate	% of connections to different hosts
32.	dst host count	No. of connections to the same destination
33.	dst host srv count	No. of connections to the same destination that use the same service
34.	dst host same src rate	% of connections to the same destination that use the same service
35.	dst host srv rate	% of connections to different hosts on the same system
36.	dst host same srv port rate	% of connections to a system with the same source port
37.	dst host srv diff host rate	% of connections to the same service coming from different hosts
38.	dst host serror rate	% of connections to a host with an S0 error
39.	dst host srv serror rate	% of connections to a host and specified service with an S0 error
40.	dst host rerror rate	% of connections to a host with an RST error
41.	dst host srv rerror rate	% of connections to a host and specified service with an RST error

The main criticism is that the KDD Cup '99 dataset is not an authentic simulation of real network traffic. Other problems include complexity of the training and test sets, the impact of duplicates to machine learning algorithms, the number of attack instances of attack is too high relative to the number of instances of normal traffic, the relationship between each attack category is not realistic, the instances of individual attacks are similar to the instances of normal traffic for the R2L attack types, etc.

Kyoto 2006+

The Kyoto 2006+ dataset contains records of real network traffic data collected from November 2006 to December 2015 on five different computer networks inside and outside Kyoto University (Protić, 2018, pp.587-589). The first part of the dataset contains records collected from ~350 honeypots, including two darknet sensors with ~300 unused IP addresses and other IDSs (Song et al, 2011; Singh et al, 2015; Najafabadi et al, 2016). To generate traffic, the authors developed a server that was deployed on the same network as the honeypots. The first part of the Kyoto 2006+ dataset recorded from 2006 to 2009 consists of 24 features containing ~90 million instances. Fourteen statistical features were derived from the KDD-Cup '99 dataset (KDD, 1999; Ashok Kumar & Venugopalan, 2018). The authors also added 10 additional features that were used exclusively to detect anomalies. In the observation period, more than 50 million sessions with normal traffic, 43 million sessions with known attacks and 425,000 sessions with unknown attacks were recorded. As a part of the Kyoto 2006+ dataset, a total of 20GB of data was collected from November 2009 to December 2015 (Park et al, 2018). The IDS Bro was used to convert packet-based traffic into a session format. (Demertzis, 2018; McCarthy, 2014). IDS Bro is a behavioral and signature-based analysis framework that provides detailed information about the hypertext transfer protocol (HTTP), the domain name system (DNS), the secure shell (SSH) communication protocol, and irregular network behavior (Song et al, 2011). It is suitable for high-performance network monitoring, protocol analysis, and real-time application layer status reporting. The Bro event engine is responsible for receiving and converting the internet protocol (IP) packets into events that are passed to the policy script interpreter that generates the output. DoS, exploits, malware, port scans and shell code attacks were recorded with no additional information about a specific attack. The Kyoto 2006+ dataset does not provide detailed information on attacks parameters.

Instead, the feature Label determines whether the session is normal or not (Ting, 2011). Table 12 presents the Kyoto 2006+ dataset.

Table 12 – Kyoto 2006+ dataset
 Таблица 12 – Киото 2006+ база данных
 Табела 12 – Киото 2006+ база података

No	Feature	Description
1	Duration – basic	Length of the connection (in seconds)
2	Service – basic	Connection's server type (dns, ssh, other)
3	Source bytes – basic	No of data bytes sent by the source IP address
4	Destination bytes – basic	No of data bytes sent by the destination IP address
5	Count	No of connections whose source IP address and destination IP address are the same to those of the current connection in the past two seconds
6	Same_srv_rate	% of connections to the same service in the Count feature
7	Srv_rate	% of connections that have 'SYN' errors in the Count feature
8	Srv_serror_rate	% of connections that have 'SYN' errors in Srv_count
9	Dst_host_count	No of connections whose source IP address is also the same to that of the current connection
10	Dst_host_srv_count	No of connections whose service type is also the same to that of the current connection
11	Dst_host_same_src_port_rate	% of connections whose source port is the same to that of the current connection in the Dst_host_count feature
12	Dst_host_serror_rate	% of connections that have 'SYN' errors in the Dst_host_count feature
13	Dst_host_srv_serror_rate	% of connections that have 'SYN' errors in the Dst_host_srv_count feature
14	Flag	The state of the connection at the time of connection was written (tcp, udp)
15	IDS_detection	Reflects if IDS triggered an alert for the connection
16	Malware_detection	Indicates if malware was observed at the connection
17	Ashula_detection.	Means if shellcodes and exploit codes were used in the connection
18	Label	Indicates whether the session was attack or not
19	Source_IP_Address	Source IP address used in the session
20	Source_Port_Number	Indicates the source port number used in the session
21	Destination_IP_Address	It was also sanitized
22	Destination_Port_Number	Indicates the destination port number used in the session
23	Start_Time	Indicates when the session was started
24	Duration	Indicates how long the session was being established

NSL-KDD

The NSL-KDD dataset is created from the KDD Cup '99 dataset. It corrects flaws in the KDD Cup '99 dataset caused by redundant records in the training set and duplicate records in the test set. Furthermore, the number of records in both the training set and the test sets is appropriate (Protic, 2018, pp.587-589). The training set contains 21 different attack types, while the test set contain 37 different attack types. The known attacks are those presented in the training set, while the additional 16

attacks are only available in the test set (see Table 13) (Nkiama et al, 2016). Normal traffic in the training set contains 67,343 instances, while normal traffic in the test set contains 9,711 instances.

Table 13 – Kyoto 2006+ attack classes
 Таблица 13 – Классификация атак в базе Kyoto 2006+
 Табела 13 – Класе напада у бази Kyoto 2006+

Attack class	Attack type – Training set	Attack type – Test set
Probe	ipsweep, nmap, portsweep, satan	ipsweep, nmap, portsweep, satan
DoS	back, land, neptune, pod, smurf, teardrop	apache2, back, land, mailbomb, neptune, pod, processtable, smurf, teardrop, udpstorm, worm
R2L	guess_passwd, ftp_write, imap, multihop, phf, spy, warezmaster, warezclient	guess_passwd, ftp_write, imap, httptunnel, phf, multihop, named, snmpguess, snmpgetattack, sendmail, warezmaster, xlock, xsnoop
U2R	buffer_overflow, loadmodule, perl, rootkit	buffer_overflow, loadmodule, rootkit, perl, ps, sqlattack, xterm

UNSW-NB-15

In 2015, Moustafa et al introduced a hybrid academic intrusion detection UNSW-NB-15 dataset derived from real normal data, and the synthesized contemporary attack activities of network traffic. The dataset consists of raw network packets containing nine different attacks (Moustafa & Slay, 2015). Raw network packets from the UNSW-NB 15 dataset are generated by the IXIA PerfectStorm tool at the Cyber Range Lab of UNSW Canberra. The tcpdump tool was used to capture 100 GB of raw traffic (Pcap files).

This dataset contains nine types of attacks, namely Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. The Argus and Bro-IDS tools are used and twelve algorithms are developed to generate a total of 49 features with the specified class label (UNSV Sydney, 2021). The total number of records is two million and 540,044 stored in the four CSV files:

- The ground truth table and the list of event files.
- One partition from this dataset was configured as a training and test set.
- The number of records in the training set is 175,341 records and the test set consists of 82,332 records of different attack and normal types.

This dataset is a collection of network packets exchanged between hosts (see Table 14) (Ahmad et al, 2022).

Table 14 – UNSW-NB-15 data type
 Таблица 14 – Виды данных в базе UNSW-NB-15
 Табела 14 – Врсте података у базу UNSW-NB-15

No	Data type	Description
1	Normal	Natural transaction data
2	Analysis	An attack targets web applications through emails, ports, or web scripts
3	Backdoor	Using backdoor to secure remote access
4	DoS	Attacks computer memory
5	Exploits	An instruction that takes advantage of bugs/errors caused by unintentional behavior on the network
6	Fuzzers	An attack to crash the system by inputting a lot of random data
7	Generic	A technique to clash the block-cipher configuration by using hash functions
8	Reconnaissance	A probe to evade network security controls by collecting relevant information
9	Shellcode	Code is used to exploit software vulnerabilities
10	Worms	A set of virus codes can be added to a computer system or other programs

Conclusion

The researchers worldwide investigate various cybersecurity issues, such as malicious attacks on computer networks. The main challenges in evaluating intrusion detection and intrusion prevention are the massive amounts of data in well-known and publicly available datasets. The majority of the datasets presented in this paper are simulations of real network traffic. Several are hybrid, and one is based on real network traffic. The size, number of features, purpose and type of attacks of each dataset vary.

We presented datasets primarily used for intrusion detection, namely ADFA-LF, ADFA-WD, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA 98, SCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD and UNSW-NB15. The main characteristics and the comparative analysis are provided. The authors' main goal is to assist researchers in selecting datasets that best meet their needs.

References

Ahmad, I., Haq, Q.E.U., Imran, M., Alassafi, M.O. & AlGhamdi, R.A. 2022. An efficient network intrusion detection and classification system. *Mathematics*, 10(3), art.number:530. Available at: <https://doi.org/10.3390/math10030530>.

Ashok Kumar, D. & Venugopalan, S.R. 2018. A Novel algorithm for Network Anomaly Detection using Adaptive Machine Learning. In: Saeed, K., Chaki, N., Pati, B., Bakshi, S. & Mohapatra, D. (Eds.) *Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing*, 564. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-10-6875-1_7.

Behal, S. & Kumar, K. 2016. Trends in validation of DDoS research. *International Conference on Computational Modeling and Security. Procedia Computer Science*, 85, pp.7-15. Available at: <https://doi.org/10.1016/j.procs.2016.05.170>.

Bohara, B., Bhuyan, J., Wu, F. & Ding, J. 2020. A Survey on the Use of Data Clustering for Intrusion Detection System in Cybersecurity. *International Journal of Network Security & Its Applications (IJNSA)*, 12(1), pp.1-18. Available at: <https://doi.org/10.5121/ijnsa.2020.12101>.

Borisniya, B. & Patel, D.R. 2015. Evaluation of Modified Vector Space Representation Using ADFA-LD and ADFA-WD Datasets. *Journal of Information Security*, 6(3), 250-264. Available at: <https://doi.org/10.4236/jis.2015.63025>.

-CAIDA. 2019. The CAIDA Anonymized Internet Traces Dataset (April 2008 - January 2019). *Caida.org*, December 3 [online]. Available at: https://www.caida.org/catalog/datasets/passive_dataset/ [Accessed: 10 June 2023].

-CAIDA. 2020a. The CAIDA "DDoS Attack 2007" Dataset. 2020. *Caida.org*, June 24 [online]. Available at: https://www.caida.org/catalog/datasets/ddos-20070804_dataset/ [Accessed: 10 June 2023].

-CAIDA. 2020b. The CAIDA OC48 Peering Point Traces. 2020. *Caida.org*, June 24 [online]. Available at: https://www.caida.org/catalog/datasets/passive_oc48_dataset/ [Accessed: 10 June 2023].

Chen, J., Yang, T., He, B. & He, L. 2021. An analysis and research on wireless network security dataset. In: *2021 International Conference on Big Data Analysis and Computer Science (BDACS)*, Kunming, China, pp.80-83, June 25-27. Available at: <https://doi.org/10.1109/BDACS53596.2021.00025>.

Demertzis, K. 2018. The Bro Intrusion Detection System. *Research Gate*. Available at: <https://doi.org/10.13140/RG.2.2.35333.40168>.

Ferriyan, A., Thamrin, A.H., Takeda, K. & Murai, J. 2021. Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic. *Applied Sciences*, 11(17), art.number:7868. Available at: <https://doi.org/10.3390/app11177868>.

Jie, C., Jiawei, L., Shulin, W. & Sheng, Y. 2018. Feature selection in machine learning: A new perspective. *Neurocomputing*, 300, pp.70-79. Available at: <https://doi.org/10.1016/j.neucom.2017.11.077>.

Khan, M.A., Karim, Md.R. & Kim, Y. 2019. A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network. *Symmetry*, 11(4), art.number:583. Available at: <https://doi.org/10.3390/sym11040583>.

Khraisat, A. Gondal, I., Vamplew, P. & Kamruzzaman, J. 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(art.number:20). Available at: <https://doi.org/10.1186/s42400-019-0038-7>.

Khor, K.-C., Ting, C.-Y. & Amnuaisuk, S.-P. 2009. A Feature Selection Approach for Network Intrusion Detection. In: *2009 International Conference on Information Management and Engineering*, Kuala Lumpur, Malaysia, pp.133-137, April 3-5. Available at: <https://doi.org/10.1109/ICIME.2009.68>.

-KDD. 1999. SIGKDD-KDD Cup: KDD Cup 1999: Computer network intrusion detection. *Kdd.org* [online] Available at: <https://kdd.org/kdd-cup/view/kdd-cup-1999> [Accessed: 10 June 2023].

Levy, J.L. & Khoshgoftaar, T.M. 2020. A survey and analysis of intrusion detection models based on CSE-CIC IDS 2018 Big Data. *Journal of Big Data* 7(art.number:104). Available at: <https://doi.org/10.1186/s40537-020-00382-x>.

Lippmann, R.P., Cunningham, R.K., Fried, D.J., Graf, I., Kendal, K.R., Webster, S.E. & Zissman, M.A. 2000. Results of DARPA 1998 Offline Intrusion Detection Evaluation. In: *Recent Advances in Intrusion Detection, RAID 99 Conference*, West Lafayette, Indiana, USA. September 7-9. [online] Available at: https://archive.ll.mit.edu/ideval/files/RAID_1999a.pdf [Accessed: 10 June 2023].

McCarthy, R. 2014. Network analysis with the Bro Network Security Monitor. *ADMIN Network & Security*, 24 [online] Available at: [https://www.admin-magazine.com/Archive/2014/24/Network-analysis-with-the-Bro-Network-Security-Monitor/\(language\)/eng-US](https://www.admin-magazine.com/Archive/2014/24/Network-analysis-with-the-Bro-Network-Security-Monitor/(language)/eng-US) [Accessed: 10 June 2023].

Mighan, S.N. & Kahani, M.A. 2021. A novel scalable intrusion detection system based on deep learning. *International Journal of Information Security*, 20, pp.387-403. Available at: <https://doi.org/10.1007/s10207-020-00508-5>.

Moustafa, N. & Slay, J. 2015. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, Australia, pp.1-6, November 10-12. Available at: <https://doi.org/10.1109/MilCIS.2015.7348942>.

Najafabadi, M.N., Khoshgoftaar, T.M. & Selyia, N. 2016. Evaluating Feature Selection Methods for Network Intrusion Detection with Kyoto Data. *International Journal of Reliability, Quality and Safety Engineering*, 23(1), art.number:1650001. Available at: <https://doi.org/10.1142/S0218539316500017>.

Natkaniec, M. & Bednarz, M. 2023. Wireless Local Area Networks Threat Detection Using 1D-CNN. *Sensors*, 23(12), art.number:5507. Available at: <https://doi.org/10.3390/s23125507>.

Nkiama, H., Mohd Said, S.Z. & Saidu, M. 2016. A Subset Feature Elimination Mechanisms for Intrusion Detection System. *International Journal of Advanced Computer Science and Application*, 7(4), pp.148-157. Available at: <https://doi.org/10.14569/IJACSA.2016.070419>.

Omar, S., Ngadi, A. & Jebur, H.H. 2013. Machine Learning Techniques for Anomaly Detection: An Overview. *International Journal of Computer Applications*, 79(2), pp.33-41 [online] Available at:

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0278bbaf1db5df036f02393679d485260b1daeb7> [Accessed: 10 June 2023].

Park, K., Song, Y. & Cheong, Y. 2018. Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm. In: *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*, Bamberg, Germany, pp.282-286, March 26-29. Available at: <https://doi.org/10.1109/BigDataService.2018.00050>.

Proebstel, E.P. 2008. *Characterizing and Improving Distributed Network-based Intrusion Detection Systems (NIDS): Timestamp Synchronization and Sampled Traffic*. Master thesis. Davis: University of California [online]. Available at:

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ee123bb36e6d16ac9b70507e7ac614791dd8f759> [Accessed: 10 June 2023].

Protić, D. 2018. Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets. *Vojnotehnički glasnik/Military Technical Courier*, 66(3), pp.580-596. Available at: <https://doi.org/10.5937/vojtehg66-16670>.

Protić, D. & Stanković, M. 2020. Anomaly-Based Intrusion Detection: Feature Selection and Normalization Influence to the Machine Learning Models Accuracy. *European Journal of Formal Sciences and Engineering*, 3(1), pp.1-9. Available at: <https://doi.org/10.26417/ejef.v2i3.p101-106>.

Serkani, E., Gharaee, H. & Mohammadzadeh, N. 2019. Anomaly Detection Using SVM as Classifier and Decision Tree for Optimizing Feature Vectors. *The ISC International Journal of Information Security (ISecure)*, 11(2), pp.159-171 [online]. Available at: https://www.isecure-journal.com/article_91592_e825e0139e75d44a6b543ad437c18379.pdf [Accessed: 10 June 2023].

Sharafaldin, I., Lashkari, A.H. & Ghorbani, A.A. 2018. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy ICISSP*, Funchal, Madeira, Portugal, 1, pp.108-116, January 22-24. Available at: <https://doi.org/10.5220/0006639801080116>.

Singh, R., Kumar, H. & Singla, R.K. 2015. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Systems with Applications*, 42(22), pp.8609-8624. Available at: <https://doi.org/10.1016/j.eswa.2015.07.015>.

Soltani, M., Siavoshani, M.J. & Jahangir, A.H. 2021. A content based deep intrusion detection system. *International Journal of Information Security*, 21, pp.547-562. Available at: <https://doi.org/10.1007/s10207-021-00567-2>.

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D. & Nakao, K. 2011. Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation. In: *EuroSys '11: Sixth EuroSys Conference: BADGERS '11 - Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, Salzburg, Austria, pp.29-36, April 10-13. Available at: <https://doi.org/10.1145/1978672.1978676>.



Sudaroli Vijayakumar, D. & Ganapathy, S. 2018. Machine Learning Approach to Combat False Alarms in Wireless Intrusion Detection System. *Computer and Information Science* 11(3), pp.67-81. Available at: <https://doi.org/10.5539/cis.v11n3p67>.

Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A. 2009. A Detailed Analysis of the KDD Cup '99 dataset. In: *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, pp.1-6, July 8-10. Available at: <https://doi.org/10.1109/CISDA.2009.5356528>.

Thakkar, A. & Lohiya, R. 2020. A Review of the Advancement in Intrusion Detection Datasets. *Procedia Computer Science*, 167, pp.636-645. Available at: <https://doi.org/10.1016/j.procs.2020.03.330>.

Thomas, C., Sharma, V. & Balakrishnan, N. 2008. Usefulness of DARPA dataset for intrusion detection system evaluation. In: *Proceedings: Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security*, 6973, pp.1-8, March 16. Available at: <https://doi.org/10.1117/12.777341>.

Ting, K.M. 2011. Confusion Matrix. In: Sammut, C. & Webb, G.I. (Eds.) *Encyclopedia of Machine Learning*. Boston, MA: Springer. Available at: https://doi.org/10.1007/978-0-387-30164-8_157.

-UNB University of New Brunswick: Canadian Institute for Cybersecurity. 2018. *CSE-CIC/IDS2018 on AWS* [online] Available at: <https://www.unb.ca/cic/datasets/ids-2018.html> [Accessed: 10 June 2023].

-UNB University of New Brunswick: Canadian Institute for Cybersecurity. 2017. *Intrusion Detection Evaluation Dataset (CIC-IDS2017)* [online]. Available at: <https://www.unb.ca/cic/datasets/ids-2017.html> [Accessed: 10 June 2023].

-UNB University of New Brunswick: Canadian Institute for Cybersecurity. 2012. *Intrusion Detection Evaluation Dataset (ISCXIDS2012)* [online] Available at: <https://www.unb.ca/cic/datasets/ids.html> [Accessed: 10 June 2023].

-UNSV Sydney. 2021. The UNSW-NB15 Dataset. 2021. *UNSV Sydney*, June 02 [online] Available at: <https://research.unsw.edu.au/projects/unsw-nb15-dataset> [Accessed: 10 June 2023].

Xie, M., Hu, J., Yu, X. & Chang, E. 2014. Evaluating Host-Based Anomaly Detection Systems: Application of the Frequency-Based Algorithms to ADFA-LD. In: Au, M.H., Carminati, B. & Kuo, C.C.J. (Eds.) *Network and System Security. NSS 2015. Lecture Notes in Computer Science*, 8792. Cham: Springer. Available at: https://doi.org/10.1007/978-3-319-11698-3_44.

Zhang, S., Xie, X. & Xu, Y. 2020. A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity. *IEEE Access*, 8, pp.128250-128263. Available at: <https://doi.org/10.1109/ACCESS.2020.3008433>.

Угрозы кибербезопасности: Какой набор данных следует использовать для оценки системы обнаружения атак?

Даниела Д. Протич^а, Миомир М. Станкович^б

^а Вооруженные силы Республики Сербия, Генеральный штаб,
Управление информатики и телекоммуникаций (J-6),
Центр прикладной математики и электроники,
г. Белград, Республика Сербия, **корреспондент**

^б Математический институт Сербской академии наук и искусств,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 20.23.25 Информационные системы с базами знаний
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Анализ многомерных наборов данных, используемых для обнаружения вторжений, становится настоящим вызовом для исследователей. В данной статье представлены самые используемые наборы данных. ADFA включает два набора данных, содержащих записи из Linux/Unix. AVID основан на фактических нормальных действиях и следах вторжений в Wi-Fi сеть стандарта IEEE 802.11. CAIDA собирает географические и топологические данные различных регионов. CIC-IDS-2017 основана на протоколах: HTTP, HTTPS, FTP, SSH и электронной почте. CSE-CIC-2018 включает абстрактные модели распространения для приложений, протоколы или сетевые модели нижнего уровня. DARPA содержит данные о сетевом трафике. Набор данных ISCX 2012 содержит различные виды многоэтапных атак и фактический сетевой трафик с фоновым шумом. KDD Cup '99 представляет собой смоделированную базу данных виртуальной сетевой среды. Kyoto 2006+ содержит записи о реальном сетевом трафике. Он используется исключительно для обнаружения аномалий. NSL-KDD корректирует недостатки в KDD Cup '99, вызванные избыточными и дублирующимися записями. UNSW-NB-15 создан путем объединения реального и синтезированного трафика, который описывает атаки на сетевой трафик.

Методы: В данном исследовании использованы количественные и качественные методы. Рассматриваются научные референсы и общедоступная информация о вышеперечисленных базах данных.

Результаты: Наборы данных часто моделируются для достижения целей конкретной организации. Количество реальных наборов данных намного меньше количества моделируемых наборов данных. Обнаружение аномалий редко используется в современном мире.

Выводы: Представлены основные характеристики и сравнительный анализ наборов данных с точки зрения даты их создания, размера, количества атрибутов, видов трафика и назначения.

Ключевые слова: ADFA, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA, ISCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD, UNSW-NB15.

Напади на сајбер безбедност: који скуп података треба користити за евалуацију система за детекцију упада?

Данијела Д. Протић^а, Миомир М. Станковић^б

^а Војска Србије, Генералштаб, Управа за телекомуникације и информатику (Ј-6), Центар за примењену математику и електронику, Београд, Република Србија, **аутор за преписку**

^б Математички институт Српске академије наука и уметности, Београд, Република Србија

ОБЛАСТ: рачунарске науке, електроника, телекомуникације
КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод: Анализа великих скупова података који се користе за детекцију упада постаје истраживачки изазов. У раду су представљени најчешће коришћени скупови података. ADFA садржи два скупа података са записима из Linux-а и Unix-а. AWID је заснован на реалној нормалној активности и активности упада у IEEE 802.11 Wi-Fi мрежу. CAIDA садржи податке са географских и тополошки различитих региона. CIC-IDS-2017 је базирана на протоколима: HTTP, HTTPS, FTP, SSH и email. CSE-CIC-2018 укључује апстрактне моделе дистрибуције за апликације, протоколе и мрежне ентитете нижег нивоа. DARPA садржи податке о мрежном саобраћају. ISCX 2012 је скуп података различитих вишестепених напада и стварног мрежног саобраћаја са позадинским шумом. KDD Cup '99 је симулирана база података виртуалног мрежног окружења. Kyoto 2006+ садржи записе реалног мрежног саобраћаја који се искључиво за детекцију аномалија. NSL-KDD коригује проблеме из KDD Cup '99 изазване редундантним записима и дупликатима. UNSW-NB-15 настаје комбинацијом реалног и синтетизованог саобраћаја који описује активности типа напада на мрежни саобраћај.

Методе: Овај рад користи квалитативну и квантитативну технологију. Разматране су научне референце и јавно доступне информације о датим базама података.

Резултати: Базе података се често симулирају да би били испуњени циљеви које захтева одређена организација. Број реалних база података је веома мали у поређењу са симулираним базама података. Детекција аномалија данас се ретко користи.

Закључак: Приказане су главне карактеристике и компаративна анализа скупова података у погледу датума настанка, величине, броја атрибута, врсте саобраћаја и намене.

Кључне речи: ADFA, AWID, CAIDA, CIC-IDS-2017, CSE-CIC-2018, DARPA, ISCX 2012, KDD Cup '99, Kyoto 2006+, NSL-KDD, UNSW-NB15.

Paper received on / Дата получения работы / Датум пријема чланка: 13.06.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 30.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 01.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



eHealthcare system data privacy concept based on Blockchain technology

Dejan B. Cizelj^a, Tomislav B. Unkašević^b, Zoran Đ. Banjac^c

Institute VLATACOM, Belgrade, Republic of Serbia

^a e-mail: dayantcizela@gmail.com,

ORCID ID: <https://orcid.org/0009-0003-9785-2524>

^b e-mail: tomislav.unkasevic@vlatacom.com, **corresponding author**,

ORCID ID: <https://orcid.org/0000-0002-6456-9250>

^c e-mail: zoran.banjac@vlatacom.com,

ORCID ID: <https://orcid.org/0000-0001-8195-8576>

DOI: 10.5937/vojtehg71-45589; <https://doi.org/10.5937/vojtehg71-45589>

FIELD: IT, cryptography, computer sciences

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Advances in information and communication technologies have enabled the creation of a symbiotic environment of humans and machines in which humans interact with machines to get better quality of everyday life. In that interaction, environment problems of information security and in particular data privacy are at the forefront. In many countries, there is legal regulation that regulates this problem in terms of securing the goals that must be realized when manipulating private data, and the technology itself is the choice of the creators of information systems. Blockchain technology is one of the methods of choice to ensure the integrity of data and undeniable transactions while digital certificates in conjunction with it enable the realization of data privacy of patients.

Methods: The cryptographic methods of asymmetric cryptography apply blockchain technology and reliable methods of identification in cyberspace, which enables the preservation of data privacy at a high level.

Results: This paper describes the method of patient health data privacy protection in a healthcare system based on digital certificates as an identification method in cyberspace and Blockchain technology as a method for preserving the integrity of transactions and a healthcare information system. The proposed concept enables the separation of private and medical data in such a way that with the accepted principle of patient ownership of medical data, it is possible to achieve primary and secondary use of healthcare data without compromising the patient's privacy.

Conclusions: The concept of identity assignment to every element in the healthcare information system and the organization/storage of data in ac-

cordance with the principles of Blockchain technology proposed in this paper enable the realization of a high level of data privacy in accordance with the European Union General Data Protection Regulation at the international level. In addition, the proposed concept enables the detection of unregistered devices or entities in the system and thus preserves the integrity of the system and increases its overall information security.

Key words: information security, healthcare IS, medical data, primary and secondary usage, asymmetric cryptography, digital signature, Blockchain organization, block structure.

Introduction

Blockchain technology is a mechanism designed to ensure the integrity of large data sets. This technology has experienced its full promotion and affirmation with the launch of the financial system Bitcoin, the first reliable decentralized digital currency in the electronic world. Bitcoin is essentially a digital value/money generation system that uses purpose-designed procedures and communication protocols to manage and exchange the created digital value, Bitcoin. It is important to understand that Bitcoins are digital data, not a physical entity. The developed Bitcoin generation and exchange protocols are based on asymmetric cryptographic systems to ensure the reliability of transactions, their immutability and integrity. The application of electronic signatures and hash functions ensures the reliability of creating Bitcoin and transactions that make payments and exchanges of Bitcoin. Transactions change the ownership of Bitcoin from one entity to another. In this virtual cash transaction, control mechanisms based on electronic signatures and verification of the possession of appropriate private cryptographic keys enable the correct realization of transactions and exchange of values. Defined control mechanisms also prevent the spending of non-existent money or the multiple use of existing money (double spending). The rules on establishing a consensus regarding the correctness of transactions and the ways of their realization establish mutual trust of individual Bitcoin owners. The basics of the Bitcoin system were first described in the paper (Nakamoto, 2008) in 2008. Bitcoin is the first virtual digital currency system to successfully solve the problem of double spending and establishing trust in a network of mutually distrustful entities.

The model of functioning of the financial system is not unique in everyday life. In the abstract sense, it can be applied to any system in which entities interact with each other and there is no a priori confidence in the correct



behaviour, accuracy of the data presented, their integrity during the transaction and later in time. With the advent of Bitcoin and the blockchain technology described in it, for the first time, there was technology that provides a satisfactory solution to this type of problem. This is particularly important for environments where accuracy, consistency, integrity and transparency must be achieved while preserving the privacy of the data of transaction participants.

In this way, by ensuring the integrity and credibility of the data, blockchain technology has enabled the automation of many life and business processes and thus permeates everyday life and the entire reality. In addition to initial applications in finance ([Hines, 2020](#); [Smith, 2020](#); [Lee & Deng, 2018](#)), blockchain technology is massively applied in surveillance and management systems based on complex systems of devices with various processing capabilities such as the Internet of Things ([Balamurugan et al., 2023](#); [Kumar et al., 2022](#)) and Smart cities ([Kumar et al., 2022](#)). In this context, the possibilities of applying blockchain technology in healthcare information systems are particularly emphasized ([Shoniregun et al., 2010](#); [Bhushan et al., 2022, 2023](#)). The dominant examples of the application of blockchain technology in information systems of this type relate to:

- Protecting patients' privacy and managing their healthcare data, using various identification, authentication and authorization techniques in patients' private data management procedures (personal identification data, medical data, etc.) in blockchain technology are included in a certain way to ensure the credibility and integrity of the data to the process of its sharing and storage.
- Monitoring supply chains for medical devices and pharmaceutical products has a significant role in healthcare systems. Counterfeiting products and their origin (medical devices and pharmaceuticals) has a significant prevalence in the world. In addition to the consequences of the use of uncertified devices and drugs in the treatment of people and the consequences for their health, financial losses of companies in the healthcare industry are also significant. Therefore, concepts and labeling systems of medical devices and pharmaceutical products have been developed and data on them is stored in appropriate blockchain structures. Each entity in the supply chain can verify

the origin and credibility of each individual product, see for example (Stawicki, 2023).

- For clinical research, it is very important that the data obtained during the research is credible, that during the research data is collected in accordance with current legislation and that the data is stored in such a way that it cannot be changed and its integrity can always be verified. Blockchain technology is enabling these challenges to be overcome and is widely applied in this segment. Some of possible approaches can be seen in (Stawicki, 2023).

Protecting and managing patients' privacy and their data is one of the key challenges in healthcare information systems. This paper presents a concept for solving this problem based on the synergistic application of digital certificate and blockchain technology.

Blockchain technology

The diversity and disparity of terminology in the field of digital currencies makes Blockchain technology equate the digital currency Bitcoin. That is not quite right. Bitcoin technology is more complex and contains Blockchain technology as one of its building blocks. Also, Blockchain technology in the academic literature is defined and described in different ways. For our approach, the most suitable definition is the one based on the Data Structure Theory which defined a blockchain as a linked list of data blocks. Copies of a blockchain list are stored on different computers and the number of copies is not limited. Synchronization between the data contents of list copies and data integrity is realized by execution proprietary designed protocols for blockchain blocks management. Blockchain blocks management assumes rules for new block construction and their registration in the blockchain list. Block construction and management rules are based on cryptographic methods dedicated for data integrity preserving and consequently have the property that the registration of an unverified data block in the blockchain list is an intractable task. Every attempt to falsify the blockchain list by entering an unverified block is easily detectable by applied mechanisms. A high level of data integrity protection in blockchains is achieved by a specific application of hash functions and the cryptographic method of digital signature for digital data.

Such a powerful integrity protection mechanism has experienced its full promotion in data distribution systems in unsafe peer-to-peer (P2P) networks, but a complete solution had to go a few more steps further:

- How to construct a decentralized mechanism for confirming the accuracy of the data included in the candidate block for registration in the blockchain list such that mutually distrustful members of the network have a high degree of confidence in its correctness.
- How to ensure synchronization of blockchain lists stored in different places/devices and the consistent use of data.

Solving these two problems opens the door for the construction of a reliable decentralized system, regarding the correctness and integrity of data blocks, for storing data. Nowadays, decentralized data management provides autonomy for data owners/users and independence from third parties. One of the reasons that speaks in favour of decentralized organization of data and their use lies in the fact that this increases the reliability of the functioning of the system because the cessation of work of one blockchain list holder does not prevent others from participating in business processes that include a blockchain list. In the case of centralized storage, the situation is exactly the opposite. The integrity, decentralization and public availability of a blockchain list are the key characteristics of the immutability of a blockchain list.

These properties are due to the application of the cryptographic mechanisms in Blockchain technology and therefore we will briefly describe the cryptographic mechanisms Blockchain technology is based on.

Blockchain technology and cryptographic mechanisms

In this section, we will briefly describe the cryptographic mechanisms on which Blockchain technology and its power rest. A detailed overview of cryptographic mechanisms, their characteristics and theoretical explanations can be found in ([Menezes et al., 1997](#); [Zheng, 2022](#); [Zheng et al., 2023](#)). Additional information and explanation regarding the application of cryptographic techniques in identification and authentication can be found in ([Todorov, 2007](#); [Boonkrong, 2021](#)) and ([Mamdouh et al., 2021](#)).

Cryptographic hash functions

Informally speaking, hash functions are a class of functions that map data of an arbitrary length in essence to data of a fixed length in bits. The hash function is usually denoted by H , a given data by m and its hash value is denoted by h_m ,

$$H(m) = h_m.$$

Interest in this class of functions was expressed in the late 1960s and early 1970s in the context of large data set searches, see (Knuth, 1998), and later found widespread use in cryptology in which numerous researchers dealt with their nature and properties. For cryptology, hash functions which have the following properties are of particular importance:

- For a given value h , it is computationally intractable to find a value, some $H(m) = h$.
- For a given value m_1 , it is computationally intractable to find the value m_2 so that $H(m_1) = H(m_2)$.
- It is computationally intractable to find two values m_1, m_2 so that $H(m_1) = H(m_2)$.

The standardized hash functions are, for example, SHA256, SHA2 and SHA3.

Cryptographic transformations

Cryptography deals with the problem of protecting the transmission of messages between two parties in communication, let us call them Alice and Bob, so that the information they exchange is available only to them and to no one else. This is achieved by corresponding message transformations called cryptographic algorithms and the parameters on which the transformation depends are the message being protected, m , and the cryptographic key or keys if there are more than one. The process of transformation by which a message is prepared for sending through a communication channel is called encryption and the result of that transformation is data called a cipher text. The fact that the cipher text that we denote with c is obtained by the transformation of the message m using the cryptographic algorithm E and the cryptographic key k_1 is denoted by

$$E_{k_1}(m) = c.$$

The transformation by which the receiving side is transforming a message c , the cipher text, into its original form by applying the cryptographic key k_2 is called decryption and it is denoted with D

$$D_{k_2}(c) = m.$$

When a $k_1 = k_2$, a cryptographic system is called symmetric and when it is $k_1 \neq k_2$, a system is called asymmetric. A graphical representation of a symmetric cryptographic transformation is shown in Figure 1 and a graphical asymmetric cryptographic transformation is shown in Figure 2.

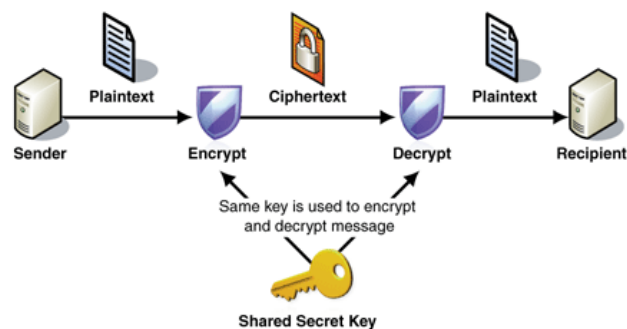


Figure 1 – Symmetric cryptographic transformation

Рис. 1 – Симметричное криптографическое преобразование

Слика 1 – Симетрична криптографска трансформација

Asymmetric cryptographic algorithms

Asymmetric cryptographic algorithms were first described in the work of Diffie and Hellman in 1976 (Diffie & Hellman, 1976) and have revolutionized the cryptographic world. Before the seminal paper of Diffie and Hellman in order to protect the message, the sender and the recipient must securely exchange the cryptographic key they intend to use, otherwise anyone who is able to access their key can find out the contents of the exchanged message. As a consequence, it is not easy to organize the distribution and management of cryptographic keys in symmetric cryptographic systems and especially if the communication networks in which they are applied consist of a large number of participants.

In the case of asymmetric cryptographic algorithms, the encryption and decryption keys are different and the encryption key is usually denoted with p and the decryption key with d . For such systems, the following facts are characteristic:

- When only the encryption key is known, it is not possible to reconstruct the decryption key, and vice versa, and
- Although the decryption key is known, it is not possible to reconstruct the encryption key.

This has brought new possibilities to the cryptographic world.

Let us show this giving one example.

Let Alice want to send Bob a protected message by applying an asymmetric cryptographic algorithm with the encryption and decryption functions E, D , respectively. The procedure proceeds as follows, Figure 2:

- For a given system, Bob constructs his encryption key p_B and the decryption key d_B in the prescribed way.
- On some public directory, Bob publishes his encryption key p_B .
- Alice takes over p_B from the public directory and constructs a cipher c for her message m as

$$c = E_{p_B}(m)$$

- Bob gets c and by applying the deciphering operation D and the key d_b gets

$$m = D_{d_B}(c)$$

Due to the fact that the encryption key can be made publicly known, the name public key is still used in the literature and, for the purpose of keeping the communication secret, the decryption key must be kept secret and therefore it is called a secret or private key.

The security of communication stems from the fact that on the basis of the knowledge of the public key it is not possible to obtain a secret key and decrypt the cipher.

Asymmetric cryptographic algorithms are based on difficult-to-solve mathematical problems:

- The problem of factorization of natural numbers, and
- The problem of discrete logarithms in finite groups.

With this in mind, it follows that asymmetric algorithms by the degree of security they provide fall into the class of practically secure cryptographic

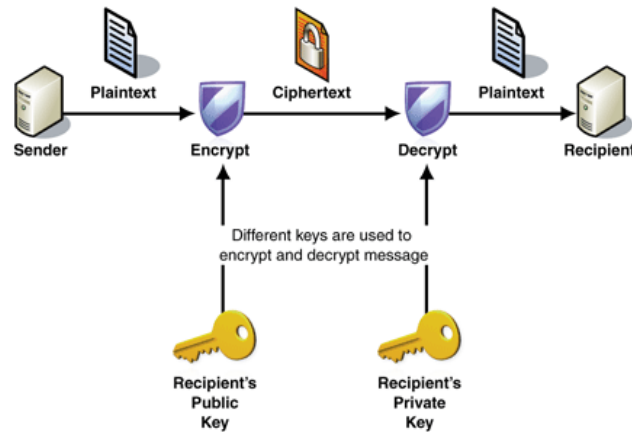


Figure 2 – Asymmetric cryptographic transformation
 Рис. 2 – Асимметричное криптографическое преобразование
 Слика 2 – Асиметрична криптографска трансформација

algorithms. The methods to compromise them are known, but it is not possible to provide the required resources for the successful execution of these algorithms (Galbraith, 2012).

In today's practice, the most common ones are asymmetric cryptographic algorithms RSA, El Gamal, and Diffie-Hellman as well as the algorithms derived from the arithmetic of points on elliptical curves.

Electronic signature

In addition to advances in the solution for distribution of cryptographic keys, asymmetric algorithms have enabled the definition of the identity of objects involved in transactions in the electronic world as well as verifying the origin and integrity of data involved in transactions. In this way, it is possible to unambiguously identify interactions and their participants in the electronic world.

Declaring the origin of electronic data/documents is carried out by the data/document electronic signature procedure and the verification of the integrity and origin of the document by the verification of the electronic signature procedure. These procedures are based on appropriate asymmetric cryptographic algorithms. Let us call the actors of this process Alice and Bob. Alice has a pair of asymmetric keys appropriate for the electronic signature generation and the verification procedures (p_A, d_A) and wants to

send Bob a message m but so that Bob can be sure, upon receipt, that the message was sent by Alice and that the message on the transmission path has not been changed. Alice creates a digital signature for the message m using the procedure for creating an electronic signature

$$\text{Sign}(m, d_A) = \text{sig}(m)$$

and she sends Bob a message $(m, \text{sig}(m), p_A)$. Bob conducts an electronic signature check for the message he received,

$$\text{Verify}(m, \text{sig}(m), p_A)$$

and if he gets the result that the verification is successful, he knows that the message comes from Alice because it is verified by her public key, the electronic signature verification key, and that the message has not been changed on the transmission path. Bob's belief regarding the origin and integrity of the received message rests on the mathematical fact that the probability of successful verification of an electronic signature created by a certain private key is infinitely small if an inadequate public key is used. The consequence of this fact is that the electronic signature algorithm and its corresponding key pair, in this case, represent a unique set of data and can serve to create Alice's identity in the electronic world. Alice proves her identity to Bob by verifying her electronic signature for the agreed document. This is the basic principle, but there are still many technical details whose considerations are not the subject of this text.

Electronic signature algorithms can be constructed in different ways, to use entire messages or just their hash values. Today, algorithms standardized in (Chen et al., 2023) are most commonly used in practice. The graphical representation of the creation of the electronic signature and its verification is given in Figure 3.

Creation of the Blockchain list

Conceptually, Blockchain is, as we previously stated, a linked list and as such has its beginning, a generic block (the Genesis block), and some number of blocks between the Genesis and the last block added to the list. Each block has a predefined structure.

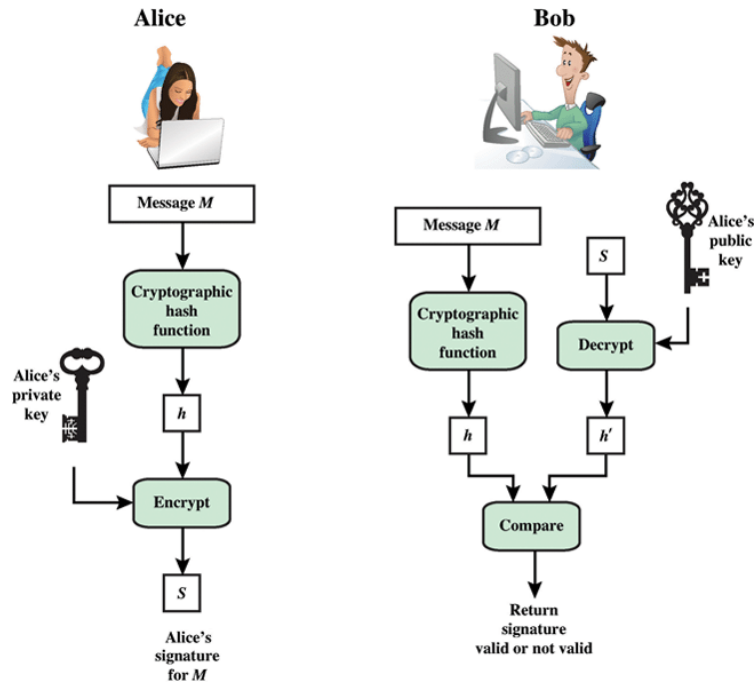


Figure 3 – Generation and verification of the digital signature procedure
 Рис. 3 – Процедура генерации и проверки ЭЦП
 Слика 3 – Генерисање и провера дигиталног потписа

Block structure

A graphical representation of Blockchain and its block structure is shown in Figure 4.

At the abstract level, every block has two clearly separated parts. The transaction part consists of the digital representation of the transactions between the community members, data are named transactions and each one is electronically signed by the data holder. The block header part consists of the following fields:

- Merkle hash is data calculated over the entire dataset that a block carries but constructed in a specific way that enables fast checking whether or not a piece of data is contained in the transaction part of the block. The details of the construction of Merkle hash value for a single block and its properties can be seen in more detail in (Summers, 2022). One of the key features is that even minimal changes in the

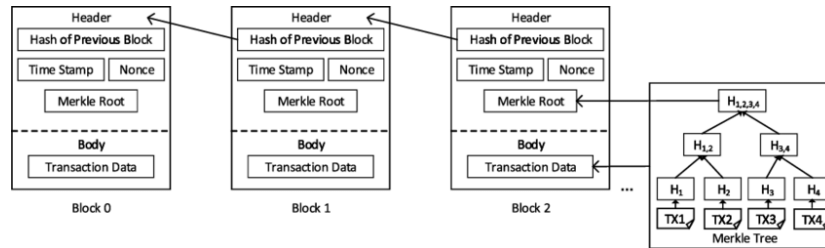


Figure 4 – Blockchain and the block structure, (Liang, 2019)
 Рис. 4 – Блокчейн и блочная структура, (Liang, 2019)
 Слика 4 – Блокчејн и структура блока, (Liang, 2019)

data result in the newly constructed Merkle hash not matching the previous one, the one that corresponds to the data before the change, and this is evidence of a violation of data integrity within the block.

- Immediate predecessor block header is processed by the defined hash function and the calculated value is entered in the appropriate data field. That value represents the control data for the immediate predecessor block data integrity.
- A timestamp is a data evidence for the block existence in the quoted time that is electronically signed by the time stamp authority.
- The weight-factor, defined in the system, is a random time variant value. It is used for the decision whether the candidate block for registering in the block chain is formed in an appropriate way. Namely, if the block hash value is below the weight-factor value, the block is well formatted and qualified for entering the blockchain. In the opposite case, the registration of the block is rejected.

Creating qualified block for entry in the blockchain list

The data involved in the formation of blocks and transactions may be different in its nature. For the purpose of this description, we will consider that there is a single data source from which to form blocks and pool of transactions, and, eventually, upon a successful procedure, to register a block in a blockchain list.

The pool of transactions is accessible by all entities in the community. Entities that want to try to form a block for registering in the blockchain cre-



ate the block candidate are usually called miners. The protocol proceeds as follows:

1. The miner selects some number of transactions from the transaction pool and includes them in the transaction part of the block. After that, the miner computes the Merkle hash of the selected transactions, obtains a timestamp as evidence about the time of construction and fills in the timestamp field.
2. From the last block in the blockchain, the miner computes its hash value and fills in the computed value in the Hash Value of Previous Block field.
3. The miner fills in the weight factor field by the current system weight-factor value.
4. Using some random number generator, the miner obtains some value and writes it into a field labelled Nonce.
5. After that, using the defined hash function and the candidate block header, the miner computes the hash value. In the case that the calculated value is lower than the current system weight factor, the miner successfully constructs the eligible block and broadcasts it for verification. In the opposite case, he/she goes back to step 4.

Upon new block candidate broadcasting, the recognition of its novelty procedure for its admission to the blockchain starts by the members of the blockchain community. The community members conduct the eligibility verification procedure as follows:

1. First, the verifier checks whether the Hash Value of Previous Block field contains the hash value of the last block registered in the blockchain. By this check, the verifier prevents incorrect copies of blockchain usage. The negative result assumes that the candidate is rejected for registration.
2. After that, the verifier checks the existence of each individual transaction from the block transaction part in the transaction pool. The absence of any of the selected transactions assumes the rejection of the candidate for registration in the blockchain.
3. The Merkle hash value for the transaction part is calculated by the verifier and compared with the Merkle hash field in the block candidate. If the values are equal, the verification continues; otherwise, the block candidate is rejected.

4. At this stage, the verifier uses a defined hash function over the block candidate header data to obtain the hash value. The obtained value is compared with the system weight factor at the time written in the timestamp field. If the computed value is lower than the appropriate system value, the check is positive; if it is not, the check is negative. If the check is negative, the candidate is discarded.
5. In the case that all checks are fulfilled, the validation of the candidate is successful, the block is entered and registered into the blockchain and the transactions from the transaction part of the block are deleted from the transaction pool.

In the previously described procedure, the criterion for the block candidate eligibility is that its hash value is lower than the current system weight factor. This criterion is the evidence of the effort made by the miner to find a convenient nonce to achieve the declared relation regarding the system defined weight factor, and it is named Proof-of-Work. In digital currency systems, miners obtain financial benefits for successfully created blocks. For different applications of Blockchain technology, various mechanisms are applied to create credible blocks, see ([Summers, 2022](#)).

Security of electronic health systems

The turbulent development of technology in the last few decades has led to tremendous advances in the field of Information and Communication Technologies and the possibility of interactive communication between humans and machines. This created a symbiotic community of humans and machines called cyberspace. The new technological environment has brought the possibility of automating many life and business processes and has significantly changed everyday life. One of the areas of everyday life and work that has undergone a significant change by applying technological capabilities is the health care system.

By creating complex information systems connected with various medical devices and means of monitoring the condition of patients, mobile and stationary, and networking of all actors in systemic processes has led to a major change in the way of operation, protocols and treatment. The consequence of these changes is a significant improvement in the quality of services and their results while reducing costs and increasing efficiency. But like any new technology, this one, in addition to its great benefits, also



brings significant challenges, especially in the field of managing patients' medical data and preserving their privacy.

Essentially, these problems have their origin in the technology itself and represent the translation of the existing security challenges into a real existing living environment.

Security challenges in information systems

The security of information systems is a complex and extensive issue (Stamp, 2011). Basically, on an abstract level, the challenges that information systems security addresses can be roughly classified into three groups:

- Ensuring the confidentiality of data relating to data protection in such a way that its content is available only to those entities for which it is intended. This applies to all processes of manipulation, processing and transfer of data.
- Ensuring the integrity of the system and data. This includes the ability to detect unauthorized changes to the architecture and structure of the system in relation to the defined structure of the system, when it comes to the system itself, or to detect unauthorized changes in data in relation to its initial correct content.
- Ensuring undeniability for activities in the system. This implies that for each action in the system, it can be unambiguously determined which entity performed it as well as when and what exactly was done.

The previously described information security challenges in the literature are known as the CIA Information Security Triad.

If one looks closely at the requirements of the CIA triad, it is easy to see that for their realization it is necessary that the entities that make up the system, whether passively providing specific functionality or having an active role in it, must be identifiable in a unique way. In other words, each of them must be assigned a unique identity within the system - electronic identity.

Electronic identity

From the very beginning of the development of computer systems, there was a need to distinguish users who use the system by their identification.

Over time, techniques for identifying users in information systems were developed so that today they can be classified into one of three groups. User identification is based on:

- What the user knows (username and password, etc.)
- What the user owns (electronic certificate, etc.)
- What the user is (fingerprint, iris, other biometric data, etc.)

With the advent of asymmetric cryptography ([Diffie & Hellman, 1976](#)), conditions were created for the formation of a system for the unique identification of objects in the digital world through digital certificates and the public key infrastructure (PKI), ([Buchmann et al., 2013](#); [Vacca, 2004](#)). The identity of each object is determined by a pair of cryptographic keys, a public one and a secret one, for a chosen asymmetric cryptographic algorithm. The nature of the facility (people, devices, software) and its associated public key within the existing public key infrastructure generates a digital certificate associated with that object. A specific body, the registration authority, within the given PKI infrastructure guarantees for the accuracy of the information included in the digital certificate and, in the case that the application for the issuance of the certificate is correct, forwards it to the competent authority for issuing digital certificates, the Certification Body. A certification body creates a digital certificate for the entity that has requested the issuance of the certificate and guarantees the accuracy of the information contained therein by its digital signature. The architecture, mode of operation and guarantees regarding the issued digital certificates of the certification body are given in the documents of the certification policy, practical rules of operation and internal rules of operation. In order to achieve interoperability in the application of digital certificates as expressions of digital identity, their format and content are standardized through the document of the International Telecommunication Union and the World Organization for Standardization ITU-T X.509, ISO / IEC 9594-8, ([Cooper et al., 2008](#)). The main characteristics of certificates generated in accordance with X509 Standard are:

- By their structure, they can be very complex due to recursive definitions in the standard and the analysis of the correctness of the structure and content can be resource demanding.



- Their size, expressed in bytes, is about two kilobytes, in average, which can cause problems while working in resource-limited environments.

For the purpose of creating and using electronic identity in resource-limited environments, Lightweight X.509 Digital Certificates Standard has been created (Forsby et al., 2018) that goes beyond the above-mentioned features and enables the application of digital certificates as methods of identification in resource-limited environments. In Figure 5, the structure and the content of both certificate profiles are presented.

Standard X.509 certificate profile		
Field	Content description	
Version	X.509 Version of certificate	
Serial Number	Serial number of the certificate	
Signature Algorithm ID	Identification of the signature algorithm	
Issuer (CA) name	X.500 Name of the certificate issuer	
Validity Period	(beginning date, ending date)	
Subject name	Certificate owner X.500 name	
Subject Public Key Info	Algorithm ID	Public key algorithm ID
	Public Key Value	Value of the public key
Issuer Unique ID	Identification of the certificate issuer	
Subject Unique ID	Identification of the certificate owner	
Extension	Additional information	
CA Digital Signature	Digital signature of the certificate by CA	

CBOR X.509 certificate profile for IoT		
Field	Content description	
Version	Fixed to 3	
Serial Number	Unsigned integer	
Signature Algorithm	ECDSA With SHA256	
Issuer (CA) name	EUI-64 as UTF8 String	
Validity Period	UTCTime	
Subject name	EUI-64 as UTF8 String	
Public Key Value	ecPublicKey followed by secp256r1 and 64-byte uncompressed ECC public key	
	Not present	
Issuer Unique ID	Not present	
Subject Unique ID	Not present	
Extension	Additional information	
CA Digital Signature	ECDSA With SHA256 Sig value	

Figure 5 – X.509 certificate profiles
 Рус. 5 – Профили сертификатов X.509
 Слика 5 – Профили сертификата X.509

e-Healthcare information security

Health information systems by their nature are very complex in architecture due to heterogeneity of devices that make them up and their functionality. The information security of such systems includes many different aspects of which in this section we will consider the security of medical data.

The introduction of information and communication technologies in health systems resulted in the creation of e-Healthcare systems. They are by their nature network-oriented in the sense that they provide the creation and rapid exchange of health information in order to increase the quality

and efficiency of medical services and treatment results. At the heart of any such system there is medical data of patients which can be, by its nature, multimedia, text, image and sound. The user's acceptance of such systems depends largely on patients' confidence in the protection of privacy, integrity and undeniability in the management of their medical data (Singh & Zhou, 2022; Murphy, 2015). Medical data of patients is collected and used by a number of medical professionals from the health care system. This use can be classified as:

1. Primary – when this data is used in the treatment of patients.
2. Secondary – when this data is used for other purposes; for example, for medical research purposes, medical and pharmaceutical statistics, various business and economic records.

The nature of the right to use medical data has changed over time and today it is accepted that the owner of the medical data is the patient from whom the data was collected and that any use of that data, which in terms of scope and content includes the ability to recognize the patient's real identity, requires his explicit consent, (Singh & Zhou, 2022). Therefore, many legislations pay close attention to protecting patient privacy through various legal solutions, e.g. the General Data Protection Rule (GDPR) in the European Union or the Data Privacy Protection Act in the Republic of Serbia.

e-Healthcare data privacy concept based on Blockchain technology

As we mentioned earlier, the security of information systems rests on the ability to know, for every activity undertaken in the system, who and when did it, and this applies to each entity in the system (people, devices, software). Regarding medical information in this system, the basic unit is the electronic health record (EHR) (Shoniregun et al., 2010). The data contained in the EHR is primarily used for medical procedures of the patient to whom the data belong and secondary for medical research needs, medical and pharmaceutical statistics, various business, administrative and economic needs. The need for a strict control of access to the identity of the patient to whom the medical data belongs further emphasizes the requirements for strong and reliable security mechanisms in such systems especially in the management of this data. In order to implement appropriate



identification and authorization techniques, it is necessary to establish unambiguous and reliable identification mechanisms.

Identification of entities in the system

In many countries, the transition towards a digitalized society is being implemented and legal solutions define the identification of persons in the electronic world for administrative and business purposes. Consequently, in health insurance, it is customary for persons to be joined by qualified electronic certificates in accordance with X.509v3 Standard which confirms the link between personal and electronic identity. The personal certificate is issued in accordance with the legislation governing this area.

It is common for users to have a smart card in the health insurance system that serves for personal identification in the system, an electronic health-care patient identification document (eHPID). In addition to a digital certificate whose public key represents the electronic identity of the patient, a personal health number (LZB) is also assigned to serve as an identification element in health procedures. The relationship between the public key contained in the electronic certificate and the LZB is such that it is in no way possible to obtain another from one piece of data; for example, an LZB is generated in a random way. Public key pairs and LZBs are kept in a cryptographically protected form in databases with restrictive access rights. The access to this database is possible only with the explicit consent of the patient, which can be expressed by providing the ePHID for inspection and typing the PIN to access this data.

Professional members of the e-Healthcare system possess identification smart cards - the employee electronic healthcare identification card (eEHID).

Issued digital certificates are placed on these identification cards (eHID, ePHID).

For devices, digital certificates are issued in accordance with the Lightweight X.509 Digital Certificates description that is compatible with X509v3 Standard.

Procedure of medical examination, generation and preservation of results

In order to present the security concept of an electronic health system based on blockchain technology and the PKI infrastructure, we will use a simplified scenario of medical examination, creation of medical data and records in the system:

1. Upon arrival at the doctor's office, the patient is identified with the system with his ePHID card and the doctor is identified with his eHID card.
2. If the system does not recognize the patient or the doctor as legitimate entities, the health system issues a report containing the reason for not holding the examination and generates a report that is recorded in the blockchain system records.
3. If the system recognizes both the patient and the doctor as legitimate entities in the health care system, the doctor is allowed to create a new medical report with a system-generated identification ordinal number in which the patient's identity is represented by an LBZ number. The doctor writes in the report anamnesis, ailments, diagnosis and conclusion about medical treatment. The electronic form of the report is digitally signed by the doctor and the system places it in the blockchain for medical reports.
4. If the diagnostic process ended at this level, the physician prescribes the necessary therapy and medications, and the system determines the prescription identification number and forms an electronic form of the prescription that the doctor electronically signs. According to the electronic signature of the prescription, it is placed in the prescription blockchain.
5. If the process of medical care of the patient requires additional examinations or medical interventions, the doctor generates a request with the necessary medical data to which the system assigns an identification number and whose electronic form is digitally signed. The request generated in this way is placed in the blockchain for medical instructions.
6. Each request for additional healthcare examinations is individually digitally signed by the issuing doctor and constitutes a unit medical transaction.

7. The identification numbers of prescriptions, instructions and medical procedures are written into the blockchain, which represents the patient's healthcare history. This blockchain has unique numerical identification and connection with patient's identity and this identification is stored in a specially protecting database.

The described concept of creation and storage of electronic healthcare reports and their usage makes medical data separate from the data on the identity of the patient. The actual identity of the patient can only be obtained by knowing the identification parameter of the user's medical data, which is not feasible because this data is stored in the register of users of the health system, which is a highly protected database with restrictive access policy. A graphical representation of the system is given in Figure 6.

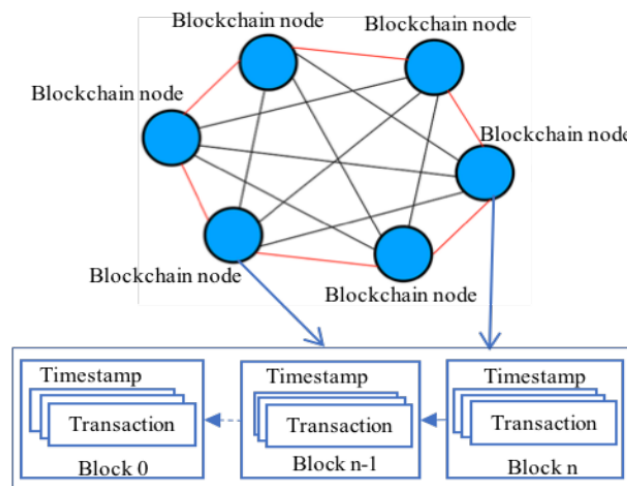


Figure 6 – Graphical presentation of the system structure, (Salman et al., 2019)

Рис. 6 – Графическое изображение структуры системы (Salman et al., 2019)

Слика 6 – Графички приказ структуре система (Salman et al., 2019)

Security analysis

The processes of digital transformation of society and the transition of life processes towards cyberspace inevitably highlight the issues of information security and the preservation of privacy of personal data. Unauthorized access to any individual's personal data can have serious adverse

consequences for him or her. The damages can be personal, psychological, business, material and social. By identity theft and access to health data, an individual can be subjected to damage in terms of obtaining employment, premiums of insurance companies and bank loans, and the like. These examples show the importance of preserving the privacy of medical data for an individual in each community.

As we have previously stated, the first and basic element of security is the establishment of a reliable identification system in the electronic health insurance system.

In the proposed concept, each entity that makes up the system (people, devices) has a defined electronic identity in the form of a digital certificate. Digital certificates for persons are issued in the form of a qualified digital certificate in accordance with the legislation of the community in which the system operates. Digital certificates for devices are issued in the Lightweight X.509 Digital Certificates format, which is compatible with X509 Standard and which allows installation on devices with very limited processing resources. This reliable method of identification enables reliable tracking of events in the system and prevents any activities that are inconsistent with the role assigned to the system by the entity. This enables efficient and up-to-date monitoring of the functioning of the system, which brings as an additional benefit the reliability of the functioning of the system as a whole. Additionally, identifying each individual entity in the system makes it possible to verify the integrity of the system and disable access to the system to devices that are not logged as its elements.

The main activity in the health system, including the eHealthcare system, is data collection, its analysis, use and preservation. The system must be designed and implemented in such a way as to enable relatively easy primary and secondary use of this data in accordance with legal regulations. The mechanisms for managing this data must be such as to protect the privacy of the data.

In the proposed concept, this goal is achieved by separating the patient's identification data and his/her medical data. The patient's identification data is stored in a highly secured database with strictly defined and restricted access rights. As identification data in this database, the identification number of the blockchain containing the patient's medical data is stored. The medical data block contains identifiers of the patient's medical procedures and through them a connection among the patient's physical

identity and medical data is established. In this way, the separation of identity and content of medical data is achieved.

The primary use of patient data requires access to a secure database to identify a blockchain containing the identifiers of medical procedures and their results for a given patient. This approach requires the patient's explicit consent and can be realized, for example, by physically using an ePHID card and entering a PIN value that testifies that the patient has willingly used the card to access medical data. Regarding to its content, electronic medical data does not contain any references to the identity of the patient, but the connection is established through their randomized numerical identifiers. In this way, the anonymity of the patient is achieved in relation to the content of medical reports.

The integrity of medical data is guaranteed by the electronic signature of the initiator of the medical procedure or the implementer of the procedure and the creator of the results. This guarantees the integrity and immutability of the data at the time of its creation. The integrity and credibility of data over time is guaranteed by storing it in a way that is provided by blockchain technology.

Relationship of the proposed solution concept with some other solutions

Blockchain technology has strongly supported the transformation of healthcare businesses towards paperless business and the cyber world. As in all business and life processes in cyberspace, information security is essential in this segment as well. However, in this sense, Blockchain technology in itself represents one of the building blocks and support for building a data privacy mechanism, but not its essential part. Different concepts for the protection and privacy of health data are applied in the implemented systems of electronic health care with the application of blockchain technology. An exhaustive overview of the solutions described in the literature regarding the methods of identification and authentication of entities in the healthcare information system as well as the protection of privacy in the management of their data can be found in ([Fernández-Alemán et al., 2013](#); [Jayabalan & O'Daniel, 2016](#)). In the following paragraphs we will look at two solutions that are based on similar ideas as the solution proposed in this paper, but the ways of realization are different.

The concept described in (Wang et al., 2019) is based on blockchain and cloud technologies. The security of medical data and EHR is ensured by their creator (medical institution + authorized person) encrypting them and additionally encrypting them before placing them in the appropriate space at the storage location in the cloud . The indexes of the generated EHR records are stored in the corresponding blockchain. Encryption mechanisms are such that they enable keyword searches over encrypted data. This concept enables the secondary use of health data, but the mechanism is relatively complex. The owner of the medical data is still the person whose examination created the record and who fully controls the access to that data. The right of access is obtained only with the explicit consent of the data owner. The procedure for accessing the desired data is as follows.

The interested entity sends a list of keywords that relevant records must contain to the EHR creator. The creator sends to the entity a digital pattern to search the EHR record space. After finding the requested records, the interested entity addresses the owner of the data, whose identifier it receives after finding the indexes that match the set of keywords, for consent to access the data. If access is granted, the operation of decrypting the EHR data and sending it securely to the interested entity is undertaken.

Theoretically, the weakness of this concept lies in the fact that the patient's privacy is not fully protected. It is possible to create a targeted set of queries by keywords in order to analyze the situation whether a specific patient has a certain type of health problem. The problem lies in the fact that this information is obtained before the right of access to specific medical data.

The concept formulated in (Omar et al., 2019) proposes a solution based on Blockchain technology and cryptographic mechanisms. Cryptographic mechanisms are used to protect privacy and Blockchain technology to store health data. The application of cryptographic methods ensures the anonymity of patients, and Blockchain technology ensures data integrity and immutability .

The solution described in this paper uses usernames and passwords as a method of user identification and authorization. The allowed activities in the system are defined based on the roles assigned to users. Patients have the role of data source and they pass their personal health data to the system in an encrypted form. Entities that use data in the system, data users, require access to data in the system, which is allowed only after



successful authentication. The registration authority is responsible for the authentication process. Access and exchange of health data are protected by special cryptographic mechanisms. Each transaction of data stored in the blockchain is marked with a special blockchain identifier, on the basis of which the data contained in the transaction is accessed and this identifier is forwarded to the initiator of the block generation.

In order for the data user to access the data contained in one block of a patient, he/she must have the identifier of that block, which is owned only by the patient as a source of data, so this protocol also implicitly requires the patient's consent to access the data. When the user knows the desired number, he/she turns to the registration authority for the authorization of access to the requested data. If the user's authentication is successful, he/she receives the desired private data of the patient whose data he/she requested.

In relation to the described concept of EHR data management, the concept proposed in this paper has certain security and functional advantages. It refers to the applied identification and authentication mechanism. The method based on digital certificates is organizationally and functionally, in our opinion, less complex in terms of scalability and interoperability. From the functionality point of view, the concept proposed in this work with its data organization, equally easily enables primary and secondary use of medical data without endangering the disclosure of the patient's identity in case of secondary use. In this way, the proposed concept of EHR data organization enables the implementation of an electronic healthcare system in legislative systems with different approaches to the ownership of medical data.

Conclusion

The processes of digital transformation of society and the transition of life processes towards cyberspace inevitably highlight the issues of information security and the preservation of privacy of personal data. Unauthorized access to an individual's personal data can have serious adverse consequences for him or her. The damages can be personal, psychological, business, material and social. Identity theft and access to health data can inflict harm to the person in question in terms of obtaining employment, insurance premiums, bank loans, and the like. These examples show the

importance of maintaining the privacy of medical data for the individual in each community and the community as a whole.

This paper presents the concept of object identification and privacy protection based on blockchain technology and the PKI infrastructure. The application of these technologies helps the concept achieve the following goals:

- The use of digital certificates as carriers of electronic identity enables a unique distinction of entities in the system. The application of Lightweight X.509 Digital Certificates enables the identification of devices with limited process capacities, which is significant from the point of view that devices with limited processing capacities (sensors, mobile and wearable devices) also participate in such systems.
- The system of registering events in the system and preserving the history of the system is such that for each activity it is known who did it, and when it was undertaken. This enables the detection of incidents, the analysis of their causation and the definition of prevention procedures.
- The mechanism of separation of identification and medical data enables the primary and secondary use of medical data in accordance with the data privacy regulations.
- Digital signature and blockchain technology enable the integrity of medical data to be preserved both at the time of its creation and over time.

The enumerated security features of the proposed concept enable the implementation of electronic health systems as zero trust information systems (Rais et al., 2024; Kudrati & Pillai, 2022; Garbis & Chapman, 2021) and at the same time ensure compliance with the EU GDPR.

References

Balamurugan, B., Poongodi, T., Manu, M.R., Karthikeyan, S. & Sharma, Y. 2023. *Convergence of Blockchain, AI and IoT: A Digital Platform, 1st Edition*. New York, NY: Chapman & Hall/CRC. ISBN 9780367495305.

Bhushan, B., Rakesh, N., Farhaoui, Y., Nand, P. & Unhelkar, B. 2022. *Blockchain Technology in Healthcare Applications: Social, Economic, and Technological Implications, 1st Edition*. Boca Raton: CRC Press. Available at: <https://doi.org/10.1201/9781003224075>.

Bhushan, B., Sharma, S.K., Saračević, M. & Boulmakoul, A. 2023. *Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems: A volume in Cognitive Data Science in Sustainable Computing*. Academic Press. Available at: <https://doi.org/10.1016/C2021-0-01904-0>.

Boonkroong, S. 2021. *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress Berkeley, CA. Available at: <https://doi.org/10.1007/978-1-4842-6570-3>.

Buchmann, J.A., Karatsiolis, E. & Wiesmaier, A. 2013. *Introduction to Public Key Infrastructures*. Heidelberg: Springer Berlin. Available at: <https://doi.org/10.1007/978-3-642-40657-7>.

Chen, L., Moody, D., Regenscheid, A. & Robinson, A. 2023. Digital Signature Standard (DSS). *Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology*. Available at: <https://doi.org/10.6028/NIST.FIPS.186-5>.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. & Polk, W. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Standards Track. Tech. rep.* [online]. Available at: <https://www.rfc-editor.org/rfc/rfc5280.html> [Accessed: 15 July 2023].

Diffie, W. & Hellman, M. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), pp. 644–654. Available at: <https://doi.org/10.1109/TIT.1976.1055638>.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. & Toval, A. 2013. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), pp. 541–562. Available at: <https://doi.org/10.1016/j.jbi.2012.12.003>.

Forsby, F., Furuhed, M., Papadimitratos, P. & Raza, S. 2018. Lightweight X.509 Digital Certificates for the Internet of Things. In: *Fortino, G. et al (Eds.) Proceedings of Interoperability, Safety and Security in IoT, Third International Conference, InterIoT 2017, and Fourth International Conference, SaSelot*. Valencia, Spain, vol. 242. pp.123-133, November 6-7. Cham: Springer. Available at: https://doi.org/10.1007/978-3-319-93797-7_14.

Galbraith, S.D. 2012. *Mathematics of Public Key Cryptography, 1st Edition*. Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9781139012843>.

Garbis, J. & Chapman, J.W. 2021. *Zero Trust Security: An Enterprise Guide*. Apress Berkeley, CA. Available at: <https://doi.org/10.1007/978-1-4842-6702-8>.

Hines, B. 2020. *Digital finance: Security tokens and unlocking the real potential of blockchain*. Hoboken, New Jersey: Wiley. ISBN 978-1119756309.

Jayabalan, M. & O'Daniel, T. 2016. Access control and privilege management in electronic health record: a systematic literature review. *Journal of Medical Systems*, 40, art.number:261. Available at: <https://doi.org/10.1007/s10916-016-0589-z>.

Knuth, D.E. 1998. *The art of computer programming, volume 3: (2nd ed.) sorting and searching*. Redwood City, CA: Addison-Wesley Pub. Co. ISBN 978-0-201-89685-5.

Kudrati, A. & Pillai, B. 2022. *Zero Trust Journey Across the Digital Estate, 1st Edition*. Boca Raton: CRC Press. Available at: <https://doi.org/10.1201/9781003225096>.

Kumar, V., Jain, V., Sharma, B., Chatterjee, J.M. & Shrestha, R. 2022. *Smart City Infrastructure: The Blockchain Perspective, 1st Edition*. Hoboken, NJ: Willey. ISBN 978-1119785385.

Lee, D. & Deng, R.H. 2018. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*. San Diego, CA: Academic Press. Available at: <https://doi.org/10.1016/C2015-0-04334-9>.

Liang, Y.C. 2019. Blockchain for Dynamic Spectrum Management. In: *Dynamic Spectrum Management*. pp.121-146. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-15-0776-2_5.

Mamdouh, M., Awad, A.I., Khalaf, A.A.M. & Hamed, H. 2021. Authentication and Identity Management of IoT Devices: Achievements, Challenges, and Future Directions. *Computers & Security*, 111, art.number:102491. Available at: <https://doi.org/10.1016/j.cose.2021.102491>.

Menezes, A.J., van Oorschot, P.C. & Vanstone, S.A. 1997. *Handbook of Applied Cryptography*. Boca Raton: CRC Press. Available at: <https://doi.org/10.1201/9780429466335>.

Murphy, S. 2015. *Healthcare Information Security and Privacy, 1st Edition*. New York, NY: McGraw-Hill. ISBN 978-0071831796.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN*, 21 August, pp. 1-9. Available at: <https://doi.org/10.2139/ssrn.3440802>.

Omar, A.A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S. & Rahman, M.S. 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, 95, pp. 511–521. Available at: <https://doi.org/10.1016/j.future.2018.12.044>.

Rais, R., Morillo, C., Gilman, E. & Barth, D. 2024. *Zero Trust Networks, 2nd Edition*. O'Reilly Media. ISBN 9781492096597.

Salman, T., Zolanvari, M., Erbad, A., Jain, R. & Samaka, M. 2019. Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys and Tutorials*, 21(1), pp. 858–880. Available at: <https://doi.org/10.1109/COMST.2018.2863956>.

Shoniregun, C.A., Dube, K. & Mtenzi, F. 2010. *Electronic Healthcare Information Security*. New York, NY: Springer. Available at: <https://doi.org/10.1007/978-0-387-84919-5>.

Singh, A.K. & Zhou, H. 2022. *Medical Information Processing and Security: Techniques and applications*. Institution of Engineering and Technology. Available at: <https://doi.org/10.1049/PBHE044E>.

Smith, S.S. 2020. *Blockchain, Artificial Intelligence and Financial Services: Implications and Applications for Finance and Accounting Professionals*. Cham: Springer. Available at: <https://doi.org/10.1007/978-3-030-29761-9>.

Stamp, M. 2011. *Information Security: Principles and Practice*. Hoboken, NJ: Wiley. Available at: <https://doi.org/10.1002/9781118027974>.

Stawicki, S.P. 2023. *Blockchain in Healthcare: From Disruption to Integration*. Cham: Springer. Available at: <https://doi.org/10.1007/978-3-031-14591-9>.

Summers, A. 2022. *Understanding Blockchain and Cryptocurrencies: A Primer for Implementing and Developing Blockchain Projects, 1st Edition*. Boca Raton: CRC Press. Available at: <https://doi.org/10.1201/9781003187165>.

Todorov, D. 2007. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management, 1st Edition*. New York, NY: Auerbach Publications. Available at: <https://doi.org/10.1201/9781420052206>.

Vacca, J.R. 2004. *Public Key Infrastructure: Building Trusted Applications and Web Services, 1st Edition*. New York, NY: Auerbach Publications. Available at: <https://doi.org/10.1201/9780203498156>.

Wang, Y., Zhang, A., Zhang, P. & Wang, H. 2019. Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*, 7, pp. 136704–136719. Available at: <https://doi.org/10.1109/access.2019.2943153>.

Zheng, Z. 2022. *Modern Cryptography Volume 1: A Classical Introduction to Informational and Mathematical Principle*. Singapore: Springer. Available at: <https://doi.org/10.1007/978-981-19-0920-7>.

Zheng, Z., Tian, K. & Liu, F. 2023. *Modern Cryptography Volume 2: A Classical Introduction to Informational and Mathematical Principle*. Singapore: Springer. Available at: <https://doi.org/10.1007/978-981-19-7644-5>.

Концепция конфиденциальности данных в электронной системе здравоохранения на основе технологии Блокчейн

Деян Б. Цизель, Томислав Б. Ункашевич, Зоран Дж. Баняц

Институт ВЛАТАКОМ, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 81.93.29 Информационная безопасность.

Защита информации,

28.21.19 Теория кодирования,

49.33.35 Надежность сетей связи и защита

информации

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Прогресс в области информационных и коммуникационных технологий позволили создать среду симбиоза между людьми и машинами, в которой люди взаимодействуют с машинами для улучшения качества повседневной жизни. В связи с этим возникают проблемы информационной безопасности, в частности, конфиденциальности данных. Во многих странах существуют правовые рамки, регулирующие этот вопрос с точки зрения целей, которые должны осуществляться при манипулировании личными данными, а сама технология является выбором создателей информационных систем. Блокчейн технология является одним из предпочтительных методов обеспечения целостности данных и необходимых транзакций, а цифровые сертификаты в сочетании с ней обеспечивают конфиденциальность информации о пациентах.

Методы: С помощью криптографических методов асимметричной криптографии осуществляется блокчейн технология и надежные методы идентификации в киберпространстве, что позволяет сохранять конфиденциальность информации на высшем уровне.

Результаты: В данной статье описывается метод защиты конфиденциальности медицинских данных пациентов в системе здравоохранения, основанный на цифровых сертификатах как методе идентификации в киберпространстве и блокчейн технологии как методе сохранения целостности транзакций и информационной системы здравоохранения. Предлагаемая концепция позволяет разделить личные и медицинские данные таким образом, что при соблюдении права собственности пациента на медицинские данные становится возможным первичное и вторичное использование медицинских данных, не нарушая права пациента на неприкосновенность личных данных.

Выводы: Концепция идентификации объекта в информационной системе здравоохранения и организация/хранение данных в соответствии с принципами блокчейн технологии, предложенными в этой статье, позволяют повысить конфиденциальность информации до международного уровня в соответствии с Общим регламентом защиты данных Европейского Союза. Помимо того, предлагаемая концепция способствует обнаружению незарегистри-



рованных устройств или объектов в системе, таким образом сохраняя целостность системы и повышая ее общую информационную безопасность.

Ключевые слова: информационная безопасность, медицинская информационная система, медицинские данные, первичное и вторичное использование, асимметричная криптография, цифровая подпись, блокчейн организация, блочная структура.

Концепт приватности података у електронском здравственом систему заснован на блокчејн технологији

Дејан Б. Цизељ, Томислав Б. Ункашевић, Зоран Ђ. Бањац

Институт ВЛАТАКОМ, Београд, Република Србија

ОБЛАСТ: информациони системи, криптологија,
рачунарске науке

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Напредак у информационо-комуникационим технологијама омогућио је стварање симбиотичког окружења људи и машина у којем људи интеракцијом са машинама побољшавају квалитет свакодневног живота. У том контексту, проблеми информационе безбедности и посебно приватности података избијају у први план. У многим земљама постоји законска регулатива којом се тај проблем регулише у смислу обезбеђења циљева који се морају реализовати при манипулацији приватним подацима, а сама технологија је избор креатора информационих система. Блокчејм технологија је једна од метода избора за обезбеђење интегритета података и непорецивости трансакција, док дигитални сертификати у спрези с њом омогућавају остваривање приватности података пацијената.

Методе: Применом криптографских метода асиметричне криптографије реализује се блокчејн технологија и поуздани методи идентификације у сајбер простору, што омогућава очување приватности података на високом нивоу.

Резултати: Овај рад описује концепт заштите приватности података пацијената у здравственом систему. Засно-

ван је на дигиталним сертификатима као методу идентификације у сајбер простору и блокчејн технологији као методу за очување интегритета трансакција и информационог система здравственог осигурања. Предложени концепт омогућава сепарацију приватних и медицинских података тако што је, уз прихваћени принцип власништва пацијента над медицинским подацима, могуће остварити примарну и секундарну употребу медицинских података без угрожавања приватности података пацијента.

Закључак: Концепт идентификације ентитета у здравственом информационом систему и организација/чување података, у складу са принципима блокчејн технологије, који су предложени у овом раду, омогућавају остваривање високог нивоа приватности података у складу са интернационалним документом *European Union General Data Protection Regulation*. Поред тога, предложени концепт омогућава детекцију нерегистрованих уређаја или ентитета у систему и на тај начин очување интегритета система и повећање његове свеукупне информационе безбедности.

Кључне речи: информациона безбедност, здравствени информациони систем, медицински подаци, примарна и секундарна употреба, асиметрична криптографија, дигитални потпис, блокчејн организација, структура блока.

Paper received on / Дата получения работы / Датум пријема чланка: 21.07.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 30.11.2023.

Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 01.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.cb>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.cb>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://vtr.mo.ynp.cb>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).





Optimization of gear ratios and gear-shifting strategy for enhanced efficiency in tracked vehicles

Stefan V. Milićević^a, Ivan A. Blagojević^b

University of Belgrade, Faculty of Mechanical Engineering, Department for Motor Vehicles, Belgrade, Republic of Serbia,

^ae-mail: stefanm9670@gmail.com, **corresponding author**,

ORCID iD: <https://orcid.org/0000-0003-4837-9067>

^be-mail: iblagojevic@mas.bg.ac.rs,

ORCID iD: <https://orcid.org/0000-0002-5776-5990>

DOI: 10.5937/vojtehg71-46133; <https://doi.org/10.5937/vojtehg71-46133>

FIELD: mechanical engineering

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Tracked vehicles play a vital role across various domains, from military operations to construction and agriculture. This study focuses on improving the efficiency of tracked vehicles by optimizing both gear ratios and gear-shifting strategies while preserving other performance aspects.

Methods: The optimization process involves a genetic algorithm for determining optimal gear ratios, considering performance constraints. Furthermore, the paper introduces a gear-shifting optimization algorithm aimed at enhancing fuel economy to the maximum, while allowing for a valid comparison between two sets of gear ratios.

Results: Optimizing gear ratios leads to substantial reductions in fuel consumption, as the engine operates within more efficient regions. Additionally, the optimized gear-shifting strategy further enhances efficiency, resulting in a fuel consumption reduction exceeding 12%, when combined with the optimized gear ratios.

Conclusions: This paper offers a direct and robust approach for optimizing powertrain gear ratios and gear-shifting strategies in tracked vehicles. The results demonstrate significant improvements in fuel efficiency without compromising other critical vehicle performance parameters.

Key words: tracked vehicles, gear ratio optimization, gear-shifting strategy, genetic algorithm, fuel efficiency enhancement.

Introduction

Tracked vehicles encompass a wide range of applications, from construction and agriculture to military purposes. A defining characteristic of all tracked vehicles is their high fuel consumption (Jimenez-Espadafor et al., 2011). Reducing fuel consumption could significantly enhance vehicle design flexibility or extend operational range. Consequently, substantial attention is directed towards enhancing the energy efficiency of tracked vehicles. Recently, hybridization of tracked vehicles has gained significant attraction in the scientific community (Randive et al., 2021; Han et al., 2019; Bhatia, 2015). Many studies extensively analyze and optimize the propulsion systems of these vehicles, yielding considerably improved energy efficiency outcomes (Qin et al., 2018; Zhang et al., 2021).

In the context of the Serbian-made infantry fighting vehicle BVP M80A, initial investigations into hybridization and energy efficiency have emerged (Milićević & Muždeka, 2021; Milićević et al., 2021). Various hybrid propulsion configurations have been introduced, while retaining a manual five-speed gearbox. With the viability of hybridization established, optimization of both the powertrain and transmission has been demonstrated to yield optimal results (Zou et al., 2012). Hence, optimizing the gearbox becomes a logical pursuit. Also, most vehicle efficiency studies have employed a manual gearbox with predetermined gearshifting strategies (Milićević & Blagojević, 2022). So apart from optimizing gear ratios, it is wise to consider gearbox automation and the development of an appropriate gearshifting strategy. It is evident that each set of gear ratios corresponds to a specific gearshifting strategy capable of achieving optimal fuel economy (Ahssan et al., 2020). In other words, determining gear ratios and establishing an optimal gearshifting strategy are inherently intertwined when pursuing optimal fuel consumption.

The objective of this study is to optimize the transmission of a combat tracked vehicle by determining optimal gear ratios and an optimal gearshifting strategy, along with an analysis of enhanced energy efficiency. The reference vehicle chosen for this study is the BVP M80A.

Simulation model

A simulation model was developed to facilitate the optimization of the powertrain. This model encompasses all relevant motion resistances,

which are mathematically formulated and subsequently integrated within the Simulink environment.

Drive cycle

A driving cycle represents the manner in which a vehicle is utilized, encapsulating its speed, acceleration, and path parameters (Achour & Olabi, 2016). At its simplest, it can be understood as the history of motion, specifically the history of a vehicle's speed, acceleration, and road gradient. Consequently, the energy efficiency and responsiveness of the vehicle and all its subsystems significantly depend on the chosen driving cycle. In contrast to wheeled vehicles, which have a set of standardized driving cycles, there is no standardized driving cycle for tracked vehicles. Hence, for the purposes of this study, a custom drive cycle was artificially synthesized, simulating a real-life road path that includes authentic turns and road grades. This drive cycle takes into account road gradient and frequent steering maneuvers, aiming to replicate real-life driving conditions. The speed, lateral acceleration, and grade are presented in Figure 1.

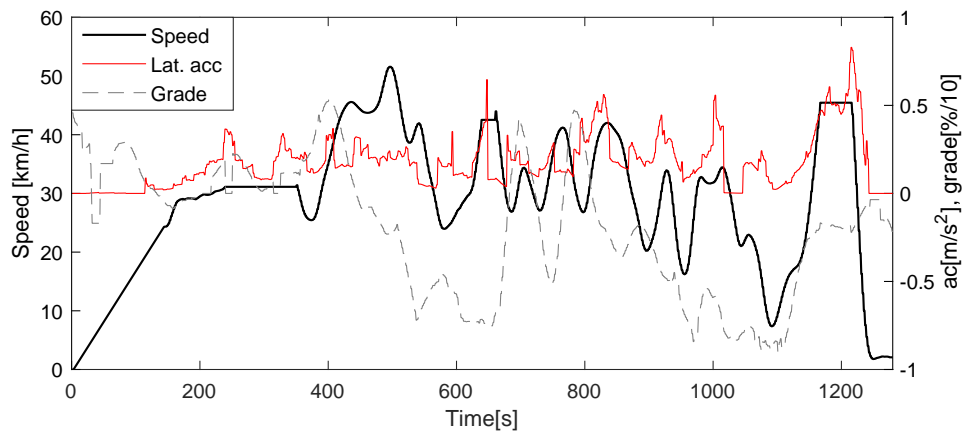


Figure 1 – Adopted drive cycle
 Рис. 1 – Принятый приводной цикл
 Слика 1 – Усвојени циклус вожње

Vehicle dynamics

An established vehicle dynamics model has been employed for external resistances (Milićević & Blagojević, 2023). The theoretical model covers resistances stemming from track-terrain interaction, grade, air resistance, centrifugal force, inertial forces, and turning resistance moments. An empirical formula was utilized for the coefficient of lateral resistance. The force on the outer track is defined as:

$$\begin{aligned}
 F_o = & \left[\frac{G \cos \alpha}{2} + \frac{h}{B} \left(\frac{G \cdot V^2}{g \cdot R} - G \cdot \sin \alpha \sin \psi \right) \right] \cdot f_r \\
 & + \frac{1}{2} \frac{1}{(n+1) \cdot b^{\frac{1}{n}} \cdot \left(\frac{k_c}{b} + k_\phi \right)^{\frac{1}{n}}} \left(\frac{G \cos \alpha}{l} \right)^{\frac{1}{n}} \\
 & + \frac{b}{2} \cdot \left(c \cdot \left(\frac{p}{\frac{k_c}{b} + k_\phi} \right)^{\frac{1}{n}} \cdot K_{pc} + 0,5 \cdot \left[\left(\frac{p}{\frac{k_c}{b} + k_\phi} \right)^{\frac{1}{n}} \right]^2 \cdot \gamma_s \cdot K_{p\gamma} \right) \quad (1) \\
 & + \frac{G \cdot V^2 \cdot s_o}{2g \cdot R'^2} + \frac{G \cdot \sin \alpha \cos \psi}{2} + \frac{\delta m g a}{2} + \frac{C_D \cdot \rho}{4} \cdot A \cdot V^2 \\
 & + \left(\frac{\mu \cdot G \cdot l}{4B} \cdot \left[1 - \left(\frac{\frac{V^2}{g \cdot R} - \sin \alpha \sin \psi}{\mu \cos \alpha} \right)^2 \right] - \frac{I_z \cdot \varepsilon}{B} \right),
 \end{aligned}$$

and the force on the inner track is:

$$\begin{aligned}
 F_i = & \left[\frac{G \cos \alpha}{2} - \frac{h}{B} \left(\frac{G \cdot V^2}{g \cdot R} - G \cdot \sin \alpha \sin \psi \right) \right] \cdot f_r \\
 & + \frac{1}{2} \frac{1}{(n+1) \cdot b^{\frac{1}{n}} \cdot \left(\frac{k_c}{b} + k_\phi \right)^{\frac{1}{n}}} \left(\frac{G \cos \alpha}{l} \right)^{\frac{1}{n}} \\
 & + \frac{b}{2} \cdot \left(c \cdot \left(\frac{p}{\frac{k_c}{b} + k_\phi} \right)^{\frac{1}{n}} \cdot K_{pc} + 0,5 \cdot \left[\left(\frac{p}{\frac{k_c}{b} + k_\phi} \right)^{\frac{1}{n}} \right]^2 \cdot \gamma_s \cdot K_{p\gamma} \right) \quad (2) \\
 & + \frac{G \cdot V^2 \cdot s_o}{2g \cdot R'^2} + \frac{G \cdot \sin \alpha \cos \psi}{2} + \frac{\delta m g a}{2} + \frac{C_D \cdot \rho}{4} \cdot A \cdot V^2 \\
 & - \left(\frac{\mu \cdot G \cdot l}{4B} \cdot \left[1 - \left(\frac{\frac{V^2}{g \cdot R} - \sin \alpha \sin \psi}{\mu \cos \alpha} \right)^2 \right] - \frac{I_z \cdot \varepsilon}{B} \right).
 \end{aligned}$$

In these equations, the first three terms on the right side represent the resistances arising from track-terrain interaction (with the normal reaction

modified due to load transfer). The fourth and fifth terms are the longitudinal forces resulting from the effect of centrifugal force and the slope of the terrain, and the sixth and seventh terms are the acceleration and air resistance. The eighth term is the moment of turning resistance. The presented equations have been implemented in the Simulink environment with the drive cycle data as an input, and the forces on the tracks as an output.

Engine

The quasi-static model with no transient dynamics was adopted. Fuel consumption is defined as:

$$\frac{dm_f}{dt} = f(T_e, n_e), \quad (3)$$

where T_e and n_e are the effective torque and the rotational speed of the engine.

The total consumption is:

$$C = \int_0^t dm_f. \quad (4)$$

The ICE model is based on a fuel map of the reference vehicle ([Hardenberg & Buhl, 1982](#)).

Transmission

Transmission is modeled as a simple five gear mechanical transmission. All kinematical relationships are assumed to be ideal. The model takes into account 'negative' flow of power, i.e. power flowing from the tracks to the engine:

$$T_e = \begin{cases} T_w \cdot \frac{1}{i_{gb} \cdot \eta_{tran}}, & T_w > 0 \\ T_w \cdot \frac{\eta_{tran}}{i_{gb}}, & T_w < 0 \end{cases} \quad (5)$$

where T_w is the torque at the drive wheel, i_{gb} is the current gearbox ratio and η_{tran} is the efficiency coefficient of transmission.

Optimization procedure

This section introduces the optimization procedure applied to determine the optimal gearbox ratios and the most effective gear-shifting strategy for

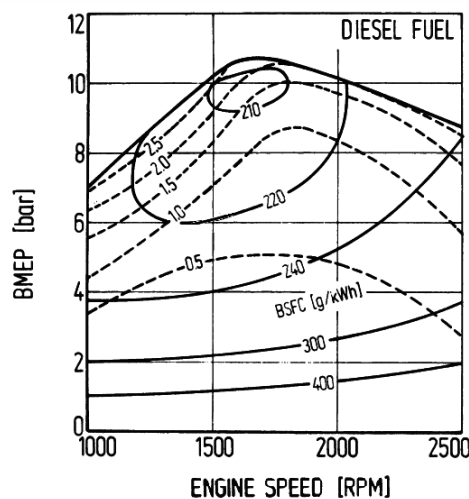


Figure 2 – Fuel map contour of the ICE (g/kWh)
 Рус. 2 – Контур топливной карты ДВС (г/кВтч)
 Слика 2 – Мапа потрошње мотора СУС (г/кВтч)

a given drive cycle. The standard gear-shifting strategy for the reference vehicle is illustrated in Figure 3. However, this strategy remains effective only within specific gear ratios and is not applicable when gear ratios are altered. For that reason, focusing solely on optimizing gear ratios, without also optimizing or at least adjusting the transmission shifting strategy, fails to maximize the vehicle's efficiency and cost-effectiveness, not to mention the absence of a reference for comparison.

Consequently, this paper introduces not only optimization of gear ratios, but also a gear-shifting optimization algorithm, whose main usage is enhancing fuel economy to the maximum, while allowing for a valid comparison between two sets of gear ratios. This comparison is achieved by utilizing an optimal gear-shift strategy for both sets.

In this study, the optimizations of gear ratios and the gear shift strategy are carried out individually. Initially, gear ratios are determined through the utilization of a genetic algorithm and a Simulink vehicle model. Following this, an optimal gear shift strategy is established using an iterative algorithm, based on the predetermined gear ratios. Hence, it can be inferred that the optimization procedure encompasses the enhancement of two distinct problems: optimizing gear ratios and optimizing gear shift strategy.

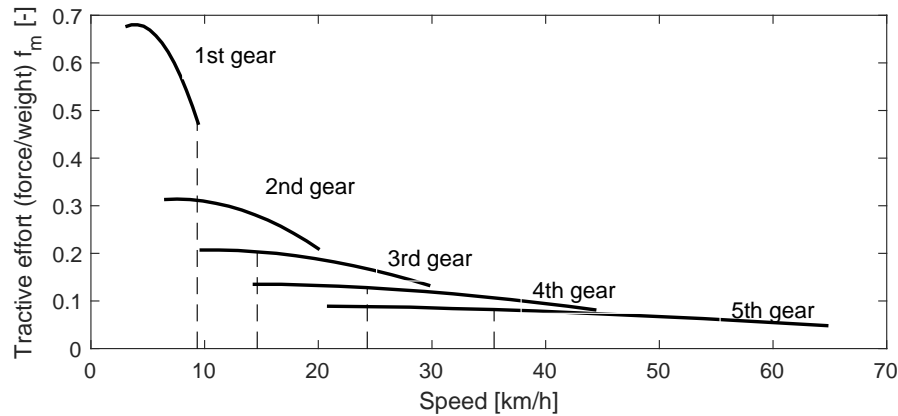


Figure 3 – Diagram of the reference vehicle dynamic coefficient with an example of gear-shifting instances

Рис. 3 – Диаграмма динамического коэффициента эталонного транспортного средства с примером переключения передач

Слика 3 – Динамичка карактеристика референтног возила са примером тренутака промене степена преноса

Furthermore, to ensure that the adopted gear ratios and the gear-shifting strategy can meet the demands of the driving cycle and prevent physically impossible outcomes during optimization, the Simulink model includes stopping criteria in the event of unmet torque or speed requirements.

Optimization of gear ratios

Gear ratio constraints

Gear ratios in the transmission significantly impact vehicle performance. Therefore, during the optimization of gear ratios, it is essential to either have a comprehensive driving cycle covering all possible scenarios and motion conditions, or introduce specific constraints. Ideally, a comprehensive driving cycle would help alleviate algorithm constraints, but since standardized driving cycles for tracked vehicles do not exist, certain limitations must be introduced in this case.

A high-speed tracked vehicle possesses key performance metrics, heavily influenced by transmission gear ratios: gradeability, maximum speed, and acceleration (Randive et al., 2019). Gear ratios of the first and fifth gears notably affect the vehicle's capability to move on slopes and

achieve maximum speed. The adopted test vehicle is capable of operating on a slope of 60% and reaching a top speed of 65 km/h, achieved with the declared gear ratios for the first and fifth gears:

$$i_I = 3.97$$

$$i_V = 0.57.$$

Consequently, the gear ratio for the first gear can be larger but not smaller, whereas for the fifth gear, the situation is reversed. Hence, the constraints on the gear ratios for the first and fifth gears are:

$$\begin{aligned} i_I &> 3.97 \\ i_V &< 0.57. \end{aligned} \tag{6}$$

In principle, gear ratios of the other gears are allowed to vary. However, due to the vehicle's combat nature, performance must never be compromised, ensuring a sufficient power reserve for acceleration at all times. This constraint will be incorporated into the algorithm itself through a penalty function.

In the event of overhauling the entire transmission, even the gear ratio of the final drive could become a subject of optimization. In such a scenario, the product of the final drive gear ratio and the transmission gear ratio would be the optimized parameter. However, given the primary focus on the transmission, for the purposes of this study, the existing gear ratio of the reference vehicle's final drive will be adopted, which is $i_{fd} = 5.786$.

Genetic algorithm procedure

The genetic algorithm (GA) optimization procedure is applied. Among the heuristic-based optimization techniques, the genetic algorithm (GA) stands out, utilizing a population of solutions in its search process. Its application is often in enhancing energy efficiency (Eckert et al., 2016, 2021).

A genetic algorithm (GA) functions as a search heuristic that emulates the natural evolution process. This approach is a common choice for generating valuable solutions to optimization and search problems. By adjusting the optimization parameters, it is possible to modify both the algorithm exploratory capabilities and its convergence speed which makes the GA a very good choice for robust optimization.

The primary objective of optimization is to identify the minimum values of the objective function, corresponding to the designated set of gear ratios relative to the vehicle's drive cycle. To achieve this, a control-oriented Simulink model was developed, and it is executed during each iteration of the optimization process. The optimization's ultimate aim is to reduce fuel consumption across the entire drive cycle. The fuel consumption is expressed in liters per 100 km/h:

$$J_f = \frac{m_{fuel}}{d_{cycle} \cdot \rho_f} \cdot 100, \quad (7)$$

where m_{fuel} is the mass of fuel consumed during the drive cycle, d_{cycle} is the traveled distance and ρ_f is the fuel density. The mass of fuel consumed is obtained as:

$$m_{fuel} = BSFC \cdot \int_{i=1}^N P_{ei}, \quad (8)$$

where $BSFC$ is the brake specific fuel consumption of the engine, and P_e is the engine effective power which directly depends on the required torque and speed:

$$\begin{aligned} T_e &= \frac{T_{req}}{i_{tran}}, \\ \omega_e &= \omega_{req} * i_{tran} \end{aligned} \quad (9)$$

In this way, the objective function can be defined as:

$$\begin{aligned} F &= J_f \\ \text{subject to: } T_e &\leq T_{emax} \\ \omega_{emin} &\leq \omega_e \leq \omega_{emax} \end{aligned} \quad (10)$$

Given that the optimization of the combat tracked vehicle is being performed, the vehicles performance must never be compromised. In this case, the performance primarily refers to the reserve of power (torque) in the second, third, and fourth gear. This constraint is taken into account using a penalty function defined as:

$$P = \frac{1}{T_{res}}, \quad (11)$$

where T_{res} is the torque reserve, which is obtained as the difference between the current torque and the maximum available for the given speed:

$$T_{res} = T_{max}(\omega) - T_{current}(\omega). \quad (12)$$

Therefore, the final objective function for the optimization of gear ratios is obtained as follows:

$$\begin{aligned}
 & F = (w_1 \cdot J_f + w_2 \cdot P) \\
 \text{subject to: } & T_e \leq T_{emax} \\
 & \omega_{emin} \leq \omega_e \leq \omega_{emax}
 \end{aligned} \tag{13}$$

where w_1 and w_2 are weights whose values can be changed depending on optimization priority.

Selection, crossover and mutation

The entire driving cycle is considered as one instance in the optimization. The GA creates a vector of gear ratios $x(k)$ and evaluates its performance over the entire driving cycle:

$$x(k) = [x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5] \tag{14}$$

Each vector $x(k)$ in the population is evaluated. Then, mutation and crossover operations are performed over the entire population, creating modified populations which are then evaluated. Original and modified populations are then combined, reordered best to worst and re-sized.

The crossover function randomly selects two members of the original population via the MATLAB function `randperm`. This step ensures that two distinct parents are chosen for crossover. The uniform crossover is applied to the selected parents' positions. It takes two parent positions and a parameter γ as inputs and returns two child positions. The γ parameter controls the blending of genetic information from the parents.

The Mutate function is called for each child's position. The Mutate function takes the child position, mutation rate, and the mutation step size as inputs and returns the mutated child position. After mutation, the child's position is checked to ensure it remains within the specified boundaries. If the mutated value exceeds the defined boundaries, it is replaced with the boundary value to keep the solution within the feasible search space. The flowchart of the applied genetic algorithm procedure is shown in Figure 4.

As mentioned, the Simulink model is equipped with a stopping mechanism that halts the simulation if any physical constraints are violated. If the simulation duration is shorter than the length of the drive cycle, the value of 'Inf' is assigned for the given population.

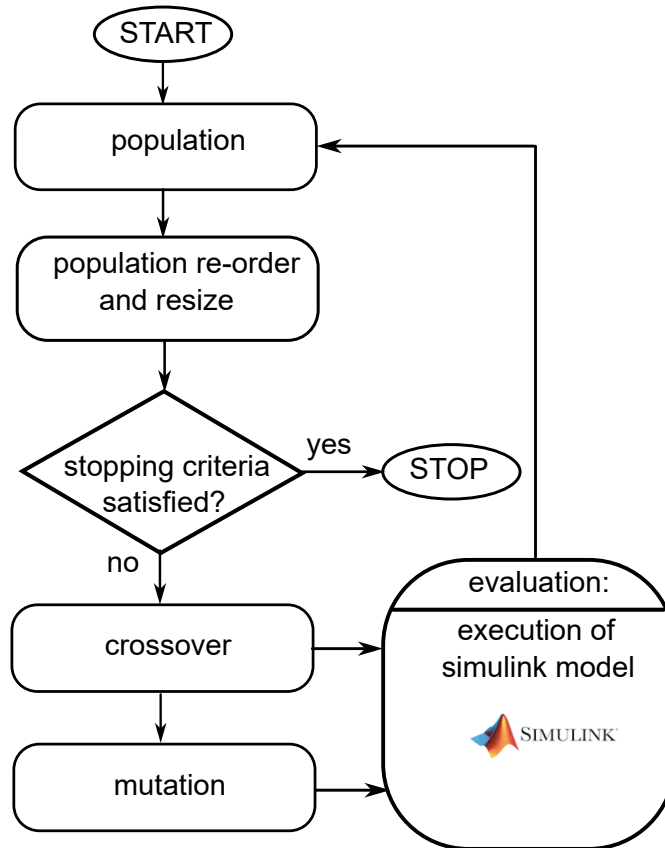


Figure 4 – Genetic algorithm flowchart
 Рис. 4 – Блок-схема генетического алгоритма
 Слика 4 – Графички приказ генетичког алгоритма

Gear selection optimization

In order to minimize fuel consumption while maintaining the adequate performance of the vehicle, it is not enough to determine only the optimal gear ratios; it is also necessary to define the appropriate gear-shifting strategy, i.e., to select the appropriate gear ratio.

This problem constitutes a gear selection optimization challenge. It entails discovering the most efficient gear-shifting strategy for a given drive cycle. Since one must independently select the optimal gear for each drive cycle instance, it qualifies as a discrete optimization problem. This problem is addressed through an iterative process (see Figure 5).

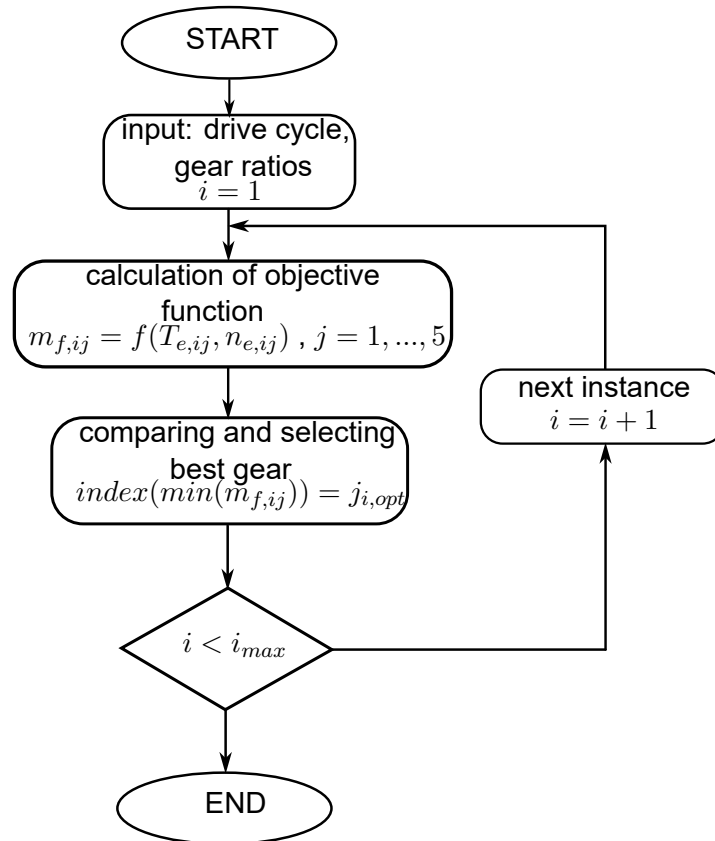


Figure 5 – Iterative gear-shifting optimization procedure
 Рис. 5 – Итеративная процедура оптимизации переключения передач
 Слика 5 – Итеративна процедура оптимизације стратегије промене
 степена преноса

The iterative process involves checking each gear (indexed as j) for every instance i in the drive cycle to find the most fuel-efficient gear-shifting strategy for the vehicle.

Minimizing fuel consumption while maintaining optimal reserve torque may lead to a higher frequency of gear shifts which could drastically increase mechanical wear. For that reason, the durability function L needs to be included. The function gives a predefined penalty value of 1 if the

gear was changed compared to the previous instance, and 0 if it was not:

$$L = \begin{cases} 0, & j_i = j_{i-1} \\ 1, & j_i \neq j_{i-1} \end{cases} \quad (15)$$

The objective function which is evaluated for every gear is defined as:

$$f = w_1 \cdot J_f + w_2 \cdot P + w_3 \cdot L \quad (16)$$

where w_1 , w_2 and w_3 are the weight factors, J_f is the fuel consumption, and P_1 is the reserve power.

Results

Applying the genetic algorithm to the optimization problem of gear ratios results in significantly lower fuel consumption. The change in the objective function value is depicted in Figure 6.

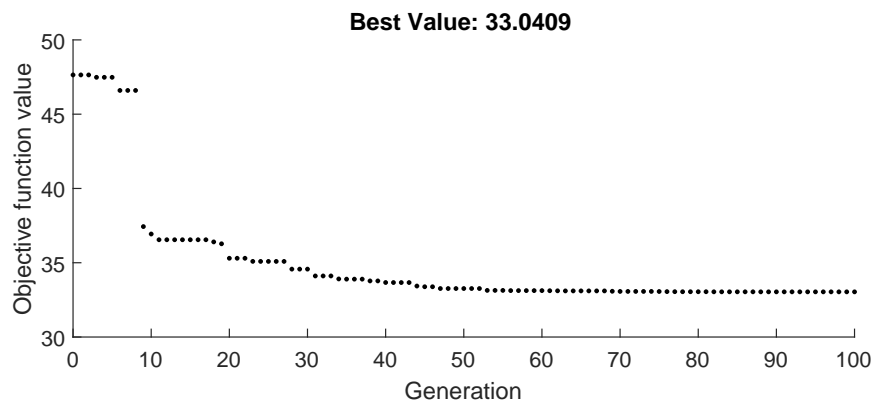


Figure 6 – Fitness function value

Рис. 6 – График изменения значений целевой функции
Слика 6 – Дијаграм промене вредности циљне функције

The new gear ratios lead to the shifting of the engine operating points towards more efficient regions of engine operation (Fig. 7).

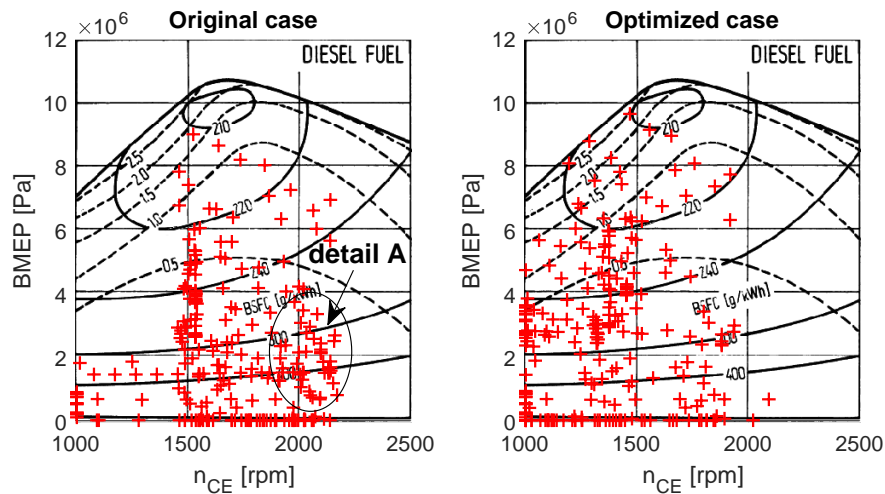


Figure 7 – Distribution of the engine operating points for the original and the optimized case

Рис. 7 – Распределение рабочих точек двигателя в оригинальном и оптимизированном случаях

Слика 7 – Распoдела радних тачака мотора за оригинални и оптимизовани случај

Figure 7 illustrates that, with the new gear ratios, the engine operates in a more efficient region. For instance, it is noticeable that numerous operating points in the highly inefficient region (detail A) are eliminated in the optimized scenario.

The original and optimized gear ratios are compared in Table 1. Due to

Table 1 – Gear ratios - original and optimized values

Таблица 1 – Передаточные числа – исходные и оптимизированные значения

Табела 1 – Преносни односи - оригиналне и оптимизоване вредности

Gear	Original	Optimized
i_1	3.91	3.91
i_2	1.84	1
i_3	1.241	0.7693
i_4	0.833	0.7475
i_5	0.571	0.5412

the close proximity of the gear ratios of the third and fourth gears, consideration can be given to eliminating one gear, effectively resulting in a four-

speed transmission. However, comprehensive analyses of the required performance are necessary for making such a decision.

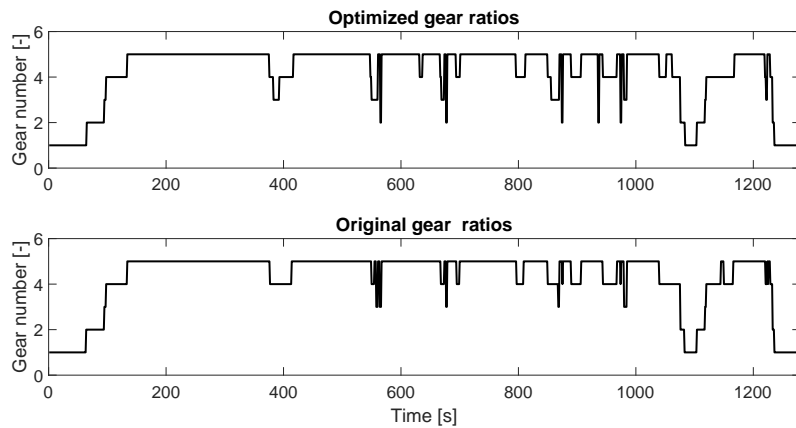


Figure 8 – Comparison of gear-shifting strategies for original and optimized gear ratios

Рис. 8 – Сравнение стратегий переключения передач для исходных и оптимизированных передаточных чисел
 Слика 8 – Поређење стратегија промене степена преноса код оригиналних и оптимизованих преносних односа

After optimizing the gear ratios, the optimization of the gearshift strategy was undertaken. First, the gearshift strategy was optimized for the original gear ratios, followed by the optimization for the optimal gear ratios. The optimization of gear shifting enabled the comparison of two transmissions with different gear ratios, as presented in Table 2. The comparison of the gearshift strategies is illustrated in Figure 8.

Table 2 – Fuel consumption comparison
 Таблица 2 – Сравнение расхода топлива
 Табела 2 – Поређење потрошње горива

Case	Relative fuel consumption [-]	Improvement [%]
Original gear ratios	100	-
Optimized gear ratios	87.32	12.68

Uniform weights were applied to gear-shifting optimization for both the initial and optimized gear ratios. The highest weight was assigned to fuel consumption ($w_1 = 0.4$), while the remaining two weights were set to $w_2 =$

$w_3 = 0.3$. This alignment in weight distribution led to notable similarities in the gear-shifting strategies, attributable to the resemblance in gear ratios.

Conclusion

This paper introduces a study and an analysis focused on improving the efficiency of tracked vehicles by optimizing gear ratios while maintaining other performance aspects. The motivation for this research arises from the existence of previous investigations where modernized powertrains were hybridized, yet the gear ratios remained unchanged, which adversely affected their overall efficiency. In this context, it was natural to explore the potential for efficiency improvement in terms of gear ratios.

A genetic algorithm was employed to optimize the gear ratios. The Serbian IFV named BVP M80A, which had already been studied, was adopted as the reference vehicle. For comparison purposes and to achieve maximum efficiency, optimization of the gear-shifting strategy was also implemented. During the optimization of both the gear ratios and the gear-shift strategy, care was taken not to compromise other crucial vehicle performances. A penalty function was introduced for the preservation of reserve torque, and weight factors for optimizing gear-shift strategies were also considered to ensure torque reserves and gearbox durability.

Using a model created in Simulink, optimization was conducted, yielding results that demonstrated fuel efficiency increase exceeding 12%. It is important to note that weight factors are variable, and the penalty functions magnitude can vary. The method described in this paper offers a direct and robust approach to optimizing powertrain gear ratios for vehicles. In the future, the focus will be on developing forward-looking models to assess vehicle performance, as well as on creating hybrid optimization approaches that encompass weight factors.

References

Achour, H. & Olabi, A.G. 2016. Driving cycle developments and their impacts on energy consumption of transportation. *Journal of Cleaner Production*, 112, pp. 1778–1788. Available at: <https://doi.org/10.1016/j.jclepro.2015.08.007>.

Ahssan, M.R., Ektesabi, M. & Gorji, S. 2020. Gear ratio optimization along with a novel gearshift scheduling strategy for a two-speed transmission system in electric vehicle. *Energies*, 13(19), p. 5073. Available at: <https://doi.org/10.3390/en13195073>.



Bhatia, V. 2015. Hybrid tracked combat vehicle. In: *2015 IEEE International Transportation Electrification Conference (ITEC)*. Chennai, India, pp.1–23, August 27-29. Available at: <https://doi.org/10.1109/ITEC-India.2015.7386862>.

Eckert, J.J., Corrêa, F.C., Santicioli, F.M., Costa, E.d.S., Dionísio, H.J. & Dedini, F.G. 2016. Vehicle gear shifting strategy optimization with respect to performance and fuel consumption. *Mechanics Based Design of Structures and Machines*, 44(1-2), pp. 123–136. Available at: <https://doi.org/10.1080/15397734.2015.1094669>.

Eckert, J.J., da Silva, S.F., de Menezes Lourenço, M.A., Correa, F.C., Silva, L.C. & Dedini, F.G. 2021. Energy management and gear shifting control for a hybridized vehicle to minimize gas emissions, energy consumption and battery aging. *Energy Conversion and Management*, 240, p. 114222. Available at: <https://doi.org/10.1016/j.enconman.2021.114222>.

Han, X., He, H., Wu, J., Peng, J. & Li, Y. 2019. Energy management based on reinforcement learning with double deep Q-learning for a hybrid electric tracked vehicle. *Applied Energy*, 254, p. 113708. Available at: <https://doi.org/10.1016/j.apenergy.2019.113708>.

Hardenberg, H.O. & Buhl, H. 1982. The MERCEDES-BENZ OM 403 VA-A Standard Production, Compression-Ignition, Direct-Injection Multifuel Engine. *SAE transactions*, 91, pp. 93–120 [online]. Available at: <https://www.jstor.org/stable/44631933> [Accessed: 20 August 2023].

Jimenez-Espadafor, F.J., Marín, J.J.R., Villanueva, J.A.B., García, M.T., Trujillo, E.C. & Ojeda, F.J.F. 2011. Infantry mobility hybrid electric vehicle performance analysis and design. *Applied energy*, 88(8), pp. 2641–2652. Available at: <https://doi.org/10.1016/j.apenergy.2011.02.010>.

Milićević, S. & Muždeka, S. 2021. Modelling and performance analysis of the BVP M-80A hybrid drive. *Vojnotehnički glasnik/Military Technical Courier*, 69(1), pp. 64–87. Available at: <https://doi.org/10.5937/vojtehg69-28232>.

Milićević, S.V. & Blagojević, I.A. 2022. Component sizing and energy management for a series hybrid electric tracked vehicle. *Vojnotehnički glasnik/Military Technical Courier*, 70(4), pp. 877–896. Available at: <https://doi.org/10.5937/vojtehg70-39762>.

Milićević, S.V. & Blagojević, I.A. 2023. Theoretical Model of High-Speed Tracked Vehicle General Motion. *FME Transactions*, 51(3), pp. 449–456. Available at: <https://doi.org/10.5937/fme2303449M>.

Milićević, S.V., Blagojević, I.A. & Muždeka, S.R. 2021. Advanced rule-based energy management for better fuel economy of hybrid electric tracked vehicle. *FME Transactions*, 49(3), pp. 711–718. Available at: <https://doi.org/10.5937/fme2103711M>.

Qin, Z., Luo, Y., Zhuang, W., Pan, Z., Li, K. & Peng, H. 2018. Simultaneous optimization of topology, control and size for multi-mode hybrid tracked vehicles. *Applied energy*, 212, pp. 1627–1641. Available at: <https://doi.org/10.1016/j.apenergy.2017.12.081>.

Randive, V., Subramanian, S.C. & Thondiyath, A. 2019. Component Sizing of Single and Dual Drive Series Hybrid Electric Powertrain for Military Tracked Vehicles. In: *2019 IEEE Vehicle Power and Propulsion Conference (VPPC)*. Hanoi, Vietnam, pp.1–6, October 14-17. Available at: <https://doi.org/10.1109/VPPC46532.2019.8952308>.

Randive, V., Subramanian, S.C. & Thondiyath, A. 2021. Design and analysis of a hybrid electric powertrain for military tracked vehicles. *Energy*, 229, p. 120768. Available at: <https://doi.org/10.1016/j.energy.2021.120768>.

Zhang, B., Guo, S., Lv, Q., Zhang, X., Ouyang, M. & Teng, L. 2021. Quantitative analysis of the energy saving mechanism of a hybrid electric tracked vehicle by an analytical method. *Energy Conversion and Management*, 237, p. 114067. Available at: <https://doi.org/10.1016/j.enconman.2021.114067>.

Zou, Y., Sun, F., Hu, X., Guzzella, L. & Peng, H. 2012. Combined optimal sizing and control for a hybrid tracked vehicle. *Energies*, 5(11), pp. 4697–4710. Available at: <https://doi.org/10.3390/en5114697>.

Повышение эффективности гусеничной машины за счет оптимизации передаточных чисел и стратегии переключения передач

Стефан В. Миличевич, **корреспондент**, Иван А. Благоевич

Белградский университет, машиностроительный факультет, кафедра моторных автомобильных транспортных средств, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 78.25.09 Военная автомобильная техника, 78.25.10 Бронетанковая техника

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Гусеничные транспортные средства играют весьма важную роль в различных областях – от военных операций до строительства и сельского хозяйства. Данное исследование сосредоточено на повышении эффективности гусеничных транспортных средств путем оптимизации как передаточных чисел, так и стратегий переключения передач при сохранении других аспектов производительности.

Методы: Процесс оптимизации включает генетический алгоритм для определения оптимальных передаточных чисел с учетом ограничений производительности. Помимо того, в статье представлен алгоритм оптимизации переключения передач, направленный на максимальное



повышение топливной экономии, позволяющий проводить достоверное сравнение двух наборов передаточных чисел.

Результаты: Оптимизация передаточных чисел трансмиссии приводит к значительному снижению расхода топлива, что обусловлено более эффективной работой двигателя внутреннего сгорания. Помимо того, оптимизированная стратегия переключения передач еще больше повышает эффективность, что приводит к снижению расхода топлива более чем на 12%.

Выводы: В данной статье предлагается прямой и надежный подход к оптимизации передаточных чисел силовых агрегатов и стратегий переключения передач гусеничных машин. Результаты показали значительное повышение топливной экономии без ущерба для других важнейших эксплуатационных характеристик автомобиля.

Ключевые слова: гусеничная техника, оптимизация передаточных чисел, стратегия переключения ступени в трансмиссии, генетический алгоритм, повышение эффективности расхода топлива.

Повећање ефикасности гусеничног возила оптимизацијом преносних односа и стратегије промене степена преноса

Стефан В. Милићевић, **аутор за преписку**, Иван А. Благојевић

Универзитет у Београду, Машински факултет, Катедра за моторна возила, Београд, Република Србија

ОБЛАСТ: машинство

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Гусенична возила имају значајну улогу у различитим областима, од борбених операција до грађевинске индустрије и пољопривреде. Рад је фокусиран на повећање ефикасности гусеничних возила оптимизацијом преносних односа и стратегије промене степени преноса, уз задржавање захтеваних перформанси.

Метод: Процес оптимизације укључује генетски алгоритам за одређивање оптималних преносних односа, узимајући у обзир ограничења перформанси. Осим тога, рад уводи алгоритам за оптимизацију промене степена преноса који

има за циљ максимизацију економичности возила, уз обезбеђивање валидног поређења два сета преносних односа.

Резултати: Оптимизација преносних односа доводи до значајних смањења потрошње горива, што је узроковано ефикаснијим радом мотора са унутрашњим сагоревањем. Поред тога, оптимизована стратегија промене степена преноса додатно повећава ефикасност, што је довело до смањења потрошње горива већем од 12%.

Закључак: Представљен је системски приступ оптимизацији односа преноса и стратегија промене степена преноса код гусеничних возила. Резултати показују значајна побољшања у ефикасности возила и смањење потрошње горива без угрожавања осталих критичних параметара перформанси возила.

Кључне речи: гусенична возила, оптимизација преносних односа, стратегија промене степена преноса, генетски алгоритам, повећање ефикасности потрошње горива.

Paper received on / Дата получения работы / Датум пријема чланка: 23.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 29.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 30.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Experimental analysis of the thermal behavior of concrete

Sara Zatir^a, Nacer Rahal^b, Houda Beghdad^c,
Abdelaziz Souici^d, Halima Aouad^e, Khaled Benmahdi^f

^a University Tahri Mohamed of Bechar, Architecture and Urban Department, Bechar, People's Democratic Republic of Algeria, e-mail: zatir.sara@univ-bechar.dz, ORCID iD: <https://orcid.org/0000-0002-6187-3441>

^b Mustapha Stambouli University, Department of Civil Engineering, Mascara, People's Democratic Republic of Algeria; University of Sciences and Technology, Laboratory of Mechanical Structure and Construction Stability, Oran, People's Democratic Republic of Algeria, e-mail: n.rahal@univ-mascara.dz, **corresponding author**, ORCID iD: <https://orcid.org/0009-0002-0400-8360>

^c Mustapha Stambouli University, Department of Civil Engineering, Mascara, People's Democratic Republic of Algeria, e-mail: houda.beghdad@univ-mascara.dz, ORCID iD: <https://orcid.org/0009-0001-3548-5138>

^d Mustapha Stambouli University, Department of Civil Engineering, Mascara, People's Democratic Republic of Algeria; University of Sciences and Technology, Laboratory of Mechanical Structure and Construction Stability, Oran, People's Democratic Republic of Algeria, e-mail: a.souici@univ-mascara.dz, ORCID iD: <https://orcid.org/0009-0004-3845-7409>

^e Mustapha Stambouli University, Department of Civil Engineering, Mascara, People's Democratic Republic of Algeria, e-mail: rahnac2002@yahoo.fr

^f Mustapha Stambouli University, Department of Civil Engineering, Mascara, People's Democratic Republic of Algeria, e-mail: k.benmahdi@univ-mascara.dz, ORCID iD: <https://orcid.org/0000-0002-8244-5817>

DOI: 10.5937/vojtehg71-46462; <https://doi.org/10.5937/vojtehg71-46462>

FIELD: materials, civil engineering

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: When concrete structural members are subjected to fire and then exposed to slow or rapid cooling, there are various changes affecting density, porosity, thermal damage, speed of sound propagation, modulus of elasticity, compressive strength, absorptivity, etc. The heavy use of concrete to build structures on the one hand and the problem of fires on the other require a deep understanding of the effect of fire on the

structural behavior of concrete, especially after cooling. So far, the two cooling methods used to put out a possible fire have been water and free air. Our objective is to experimentally analyze the use of the extinguisher as the third method of cooling concrete exposed to high temperatures.

Methods: To achieve our objective, a series of mechanical and physical tests were carried out on specimens 40 mm in diameter and 40 mm in height, exposed to high temperatures of 200, 400, and 600 °C. These test samples were then subjected to three different cooling regimes, namely: free air, water immersion, and extinguisher use.

Results: The results clearly show that the use of the extinguisher is more appropriate than the other two cooling methods, namely, natural cooling and immersion in water.

Conclusion: The results from this experimental study could be of practical use when trying to extinguish a possible fire in a concrete structure.

Key words: concrete, fire, experimental analysis, extinguish, water, free air.

Introduction

Because of its many advantages over other construction materials, such as simple workmanship, durability, strength, and ease of implementation, concrete has become the primary structural material in the construction of nearly all buildings (Kodur, 2014).

Fire is one of dangerous threats that attack structures. Compared to steel, which has a low thermal conductivity, and to wood, which is rapidly combustible, concrete construction material is characterized by its good fire resistance; however, it can lose part of its resistance (Annerel & Taerwe, 2009; Ingham, 2009). The type of cement, the nature of the aggregate, the dimensions of structural elements, the porosity and the moisture content of concrete as well as its thermal properties are all factors which determine the degree of fire resistance (Akçaözoğlu, 2013). The fire resistance is increased with the increase in the dimensions of a concrete element (Tanaçan et al, 2009).

During their lifetime, concrete structures can be subjected to high temperatures during fire or near furnaces and reactors. It will then lead to the deterioration of the structural quality of concrete.

In China, recent statistics show that in 2018 alone, there were 237,000 fires, including almost 107,000 in residential buildings (Bi et al, 2020). Fires can start in tunnels and buildings alike (Annerel & Taerwe, 2009; Khoury, 2000; Du et al, 2018; Tomar & Khurana, 2019; Zhao et al, 2019). This indicates that the occurrence of fire misfortunes is becoming

more and more common, which affects the safety of structures and leads to significant economic deficits (Hertz, 2005; Aitcin, 2003; Liu et al, 2019).

Under high temperatures, physical properties change and chemical transformations occur in the cementitious matrix, leading to a deterioration of its mechanical characteristics (Hertz, 2005; Aitcin, 2003; Liu et al, 2019; Hammoud et al, 2014; ACI, 1989; Khoury et al, 2007; European Commissions, 1992; CEN, 1994; CEN, 2002; CEN, 2004; Bazant & Kaplan, 1996; Phan & Carino, 2000). They also participate in the growth of shrinkage, transient creep, and changes in durability (Pihlajavaara & Kesler, 1972). Mechanical properties such as strength, modulus of elasticity, and volume stability of concrete are significantly reduced during these exposures (Li et al, 2012). Free water in pores and part of chemically bound water in hydrated cement paste are released and a large amount of energy is consumed due to exposure to high temperatures (Su et al, 2014).

This special situation implies the need to assess the safety of concrete structures with regard to possible fires. This analysis is therefore an essential task to ensure the structural safety of concrete structures (Hammoud et al, 2014). In practice, concrete structural elements must fulfill the fire safety requirements defined in the design codes for building structures (ACI, 2007; ACI, 2008; CEB, 2002).

According to the literature, the analysis of the behavior of concrete under high temperatures has been the subject of numerous works, leading to appreciable results (Zhai et al, 2019). We quote:

Wang et al (Wang, 2014) conducted static compression tests and a Split Hopkinson Pressure Bar Impact (SHPB) test on concrete specimens 75 mm in diameter and 55 mm in height. These specimens are heated to high temperatures of 100 to 900 °C and then cooled naturally.

Tao et al (Tao et al, 2011) conducted a compression test on concrete cylinders 50 mm in diameter and 35 mm in height under rapid heating from 200 to 600 °C using microwaves.

Shi et al (Shi et al, 2014) performed SHPB compression-shock tests on cylindrical specimens 98 mm in diameter and 50 mm in height. These concrete blocks are subjected to high temperatures of 200 to 800 °C and are cooled by natural cooling or cold water.

Under different applied loading levels, Jia et al (Jia et al, 2011ab) carried out compression-impact tests on concrete specimens 50 mm in diameter and 35 mm in height. Using microwaves, these concrete specimens were quickly heated to 200–650 °C.

Under various projectile velocities, Li et al (Li et al, 2012) performed an impact compression experiment on a SHPB device and concrete specimens 98 mm in diameter and 48 mm in height heated to 200–800 °C.

Similarly, Su et al (Su et al, 2014) carried out the same tests but on specimens 49 cm high.

SHPB impact compression tests and numerical simulations on concrete blocks 70 mm in diameter and 35 mm in height heated to 200-800 °C were developed by Huo et al (Huo et al, 2013).

Previous experimental and numerical research revolves around micromechanics and constitutive models of concrete at high temperature (Huo et al, 2013; Gawin et al, 2011; Ezekiel et al, 2013; Jia et al, 2011ab; Bangi & Horiguchi, 2012; Noumowe, 2005; Tenchev & Purnell, 2005; Van der Heijden et al, 2007; Wang & Shang, 2014; Lu, 2011; Zhai et al, 2014; Zhang et al, 2013, Carstensen et al, 2013). They analyze the mechanical properties of concrete at high temperature or after high temperature (Ma et al, 2015). However, the analysis of the behavior of concrete cooled after high temperatures has yet to be fully investigated (Zhai et al, 2019).

In turn, Zhai et al (Zhai et al, 2014) conducted impact compression tests on concrete specimens. These test specimens of 35 MPa compressive strength are heated to high temperatures of 200 to 800 °C and are then cooled naturally or in water.

This article is an experimental contribution analyzing the effect of the cooling mode on the thermal behavior of concrete. Until now, the cooling methods used were natural cooling or immersion in water. Through this work, we used natural cooling, water, and a new mode of cooling, powder extinguishers.

To achieve our objective, we carried out mechanical tests on compressive strength, thermal damage, and dynamic modulus of elasticity, and tested physical properties: porosity, density, and speed of sound propagation. These tests were carried out while hot and after cooling. The samples tested were exposed to high temperatures: 200 °C, 400 °C, and 600 °C. After exposure to these temperatures, the samples were then cooled using air, water, and powder extinguishers.

Materials used and sample preparation

Cement

The cement used is Portland cement composed of the CPJ CEM II/B-L 32.5 N type, with a minimal resistance of 32.5 MPa at 28 days. Tables 1, 2 and 3 respectively give the chemical, mineralogical, and physical composition of the cement used in this study.

Table 1 – Chemical composition of cement
Таблица 1 – Химический состав цемента
Табела 1 – Хемијски састав цемента

CaO	SiO ₂	Al ₂ O ₃	Fe ₂ O ₃	SO ₃	K ₂ O	Na ₂ O	MgO
60.10	18.13	3.25	2.56	2.71	0.26	0.22	1.75

Table 2 – Mineralogical composition of cement according to Bogue
Таблица 2 – Минералогический состав цемента (Bogue)
Табела 2 – Минералогички састав цемента (Bogue)

Element	C ₃ S	C ₂ S	C ₃ A	C ₄ AF
Content (%)	71.976	50.488	4.280	7.790

Table 3 – Physical characteristics of cement
Таблица 3 – Физические свойства цемента
Табела 3 – Физичка својства цемента

Characteristics	Values
Apparent density (g/cm ³)	4000
Absolute density (g/cm ³)	1065
Start of setting (minute)	2990
End of setting (minute)	150 ± 30
Normal consistency (%)	230 ± 50

Water composition

For the manufacture of test specimens, we used drinking water distributed by the public service network. The results of the chemical analysis of this water are summarized in Table 4.

Table 4 – Chemical analysis of water composition
Таблица 4 – Химический анализ состава воды
Табела 4 – Хемијска анализа састава воде

Ca	Mg	Na	K	Cl	SO ₄	CO ₃	NO ₃	Fe	pH	Organic material
32.86	51.36	38.00	0.00	113.60	65.46	368.44	12.22	0.03	7.88	0.18

Aggregates

In this analysis, we used continuous crushed gravel of 3/8 mm in size and quarry sand of 0/4 mm in size.

Preparation of the samples

The dimensions of the specimens used in this study are: the diameter ϕ = the height h = 40 mm. For the preparation of the samples, we adopted the quantities given in Table 5:

Table 5 – Formulation of micro-concrete Kg/m³

Таблица 5 – Состав микробетона, кг/м³

Табела 5 – Формулација микробетона кг/м³

Cement	Sand 0/4	Gravel 3/8	Water	Super-plasticizer	E/C
350	616	1143	202	17.5	0.57

The samples were covered with plastic film to avoid any water exchange with the external environment and were stored in the laboratory at a controlled room temperature of $20 \pm 2^\circ\text{C}$.

The specimen heating and cooling

The specimens were classified into four groups (G_1 , G_2 , G_3 and G_4). We measured the mass and speed of propagation of sonic waves before exposing the samples to temperatures of 200, 400, and 600 °C.

The three groups of specimens (G_1 , G_2 and G_3) were subjected to maximum temperatures of 200°C, 400°C and 600°C, respectively.

The specimens were heated with a constant temperature rise rate equal to 5 °C/min up to the test temperature. Then, to stabilize the thermal field, these specimens were kept at the target temperature for one hour.

The last step was the temperature drop ramp of 1°C/min down to an ambient temperature. On the other hand, the fourth group (G_4) was maintained at an ambient laboratory temperature equal to 20°C. For each group, we used a cooling mode for one minute. For 24 hours after the cooling stage, for each specimen, we calculated the mass and the speed of propagation of sonic waves.

Results and discussion

Density

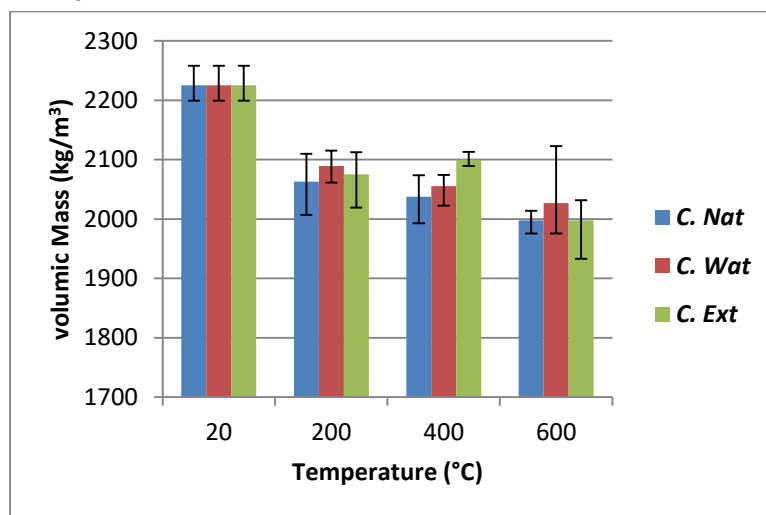


Figure 1 – Effect of temperature and the cooling mode on density
 Рис. 1 – Влияние температуры и режима охлаждения на плотность
 Слика 1 – Утицај температуре и начина хлађења на густину

Table 6 – Effect of temperature and the cooling mode on density (Kg/m3)
 Таблица 6 – Влияние температуры и режима охлаждения на плотность (кг/м3)
 Табела 6 – Утицај температуре и начина хлађења на густину (кг/м3)

	20 °C	600 °C	Kg/m ³	%
C. Nat	2225	1998	227	10.2
C. Wat	2225	2027	198	8.9
C. Ext	2225	1998	227	10.2

C. Nat: natural cooling
C. Wat: water cooling
C.Ext : extinguisher cooling

Figure 1 shows the effect of temperature and the cooling mode (air, water, and extinguisher) on density. When the temperature increases, the density of the samples decreases for the three cooling modes. Table 6 shows that the density drop between 20 and 600 ° C is the same, 10.2%,

in both natural and extinguisher cooling. On the other hand, it is a little lower for rapid cooling by immersion in water, at 8.89%.

Porosity

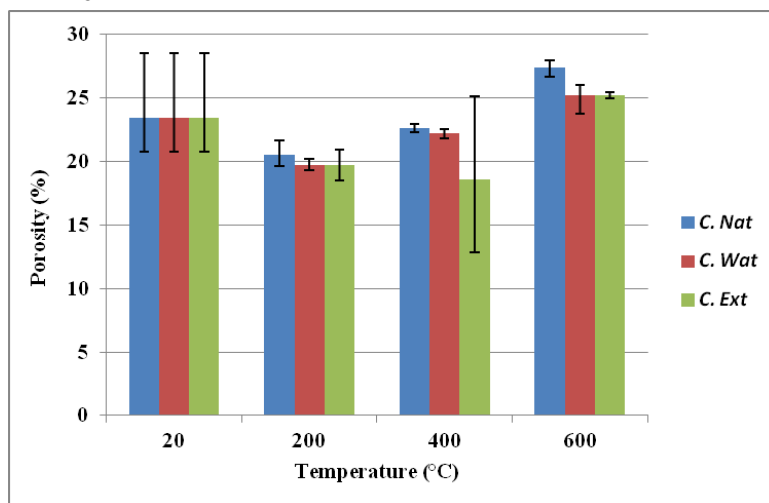


Figure 2 – Effect of temperature and the cooling mode on porosity
 Рис. 2 – Влияние температуры и режима охлаждения на пористость
 Слика 2 – Утицај температуре и начина хлађења на порозност

Table 7 – Effect of temperature and the cooling mode on porosity (%)
 Таблица 7 – Влияние температуры и режима охлаждения на пористость (%)
 Табела 7 – Утицај температуре и начина хлађења на порозност (%)

	20 °C	600 °C	%
C. Nat	23.45	27.38	14.3
C. Wat	23.45	25.24	7.1
C. Ext	23.45	25.21	7.0

Figure 2 shows the effect of temperature and the cooling mode (air, water, and extinguisher) on porosity. It was discovered that the porosity value increases in lockstep with increasing temperature from 20 °C to 600 °C.

Table 7 shows that with natural cooling, porosity increases twice as compared to the other two cooling modes.

The speed of sound propagation

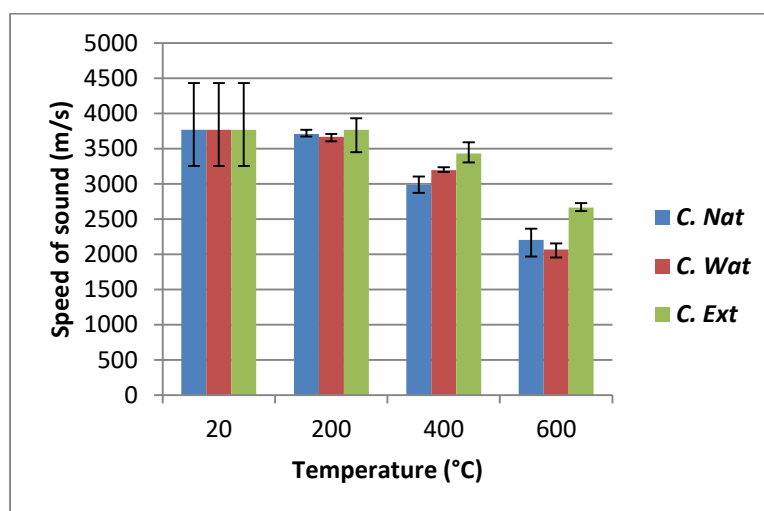


Figure 3 – Effect of temperature and the mode of cooling on the speed of sound propagation

Рис. 3 – Влияние температуры и режима охлаждения на скорость распространения звука

Слика 3 – Утицај температуре и начина хлађења на брзину ширења звука

Table 8 – Effect of temperature and the mode of cooling on the speed of sound propagation (m/s)

Таблица 8 – Влияние температуры и режима охлаждения на скорость распространения звука (м/с)

Табела 8 – Утицај температуре и начина хлађења на брзину ширења звука (м/с)

	20 °C	600 °C	m/s	%
C. Nat	3769	2206	1563	41.47
C. Wat	3769	2068	1701	45.13
C. Ext	3769	2666	1103	29.27

Figure 3 shows the effect of temperature and the mode of cooling (air, water, and extinguisher) on the speed of sound propagation. It clearly shows that the speed of propagation decreases with increasing temperature. Table 8 shows that with sprinkler cooling, the speed of sound propagation is significantly lower than with the other two cooling methods.

Elasticity dynamic modulus

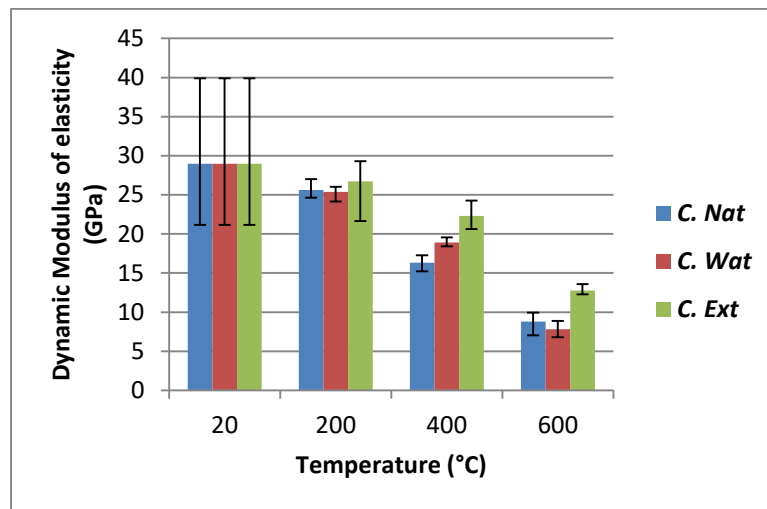


Figure 4 – Effect of temperature and the mode of cooling on the dynamic modulus of elasticity

Рис. 4 – Влияние температуры и режима охлаждения на динамический модуль упругости

Слика 4 – Утицај температуре и начина хлађења на динамички модулу еластичности

Table 9 – Effect of temperature and the mode of cooling on the dynamic modulus of elasticity (GPa)

Таблица 9 – Влияние температуры и режима охлаждения на динамический модуль упругости (ГПа)

Табела 9 – Утицај температуре и начина хлађења на динамички модулу еластичности (ГПа)

	20 °C	600 °C	Gpa	%
C. Nat	28.99	8.78	20.21	69.7
C. Wat	28.99	7.82	21.17	73.03
C. Ext	28.99	12.77	16.22	55.95

In Figure 4 we have shown the effect of temperature and the mode of cooling (air, water, and extinguisher) on the dynamic modulus of elasticity. When temperature increases, the dynamic modulus of elasticity of the samples decreases. Table 9 clearly shows that with quench cooling, the

drop in the dynamic modulus of elasticity is absolutely lower than with the other two cooling modes.

Compressive strength

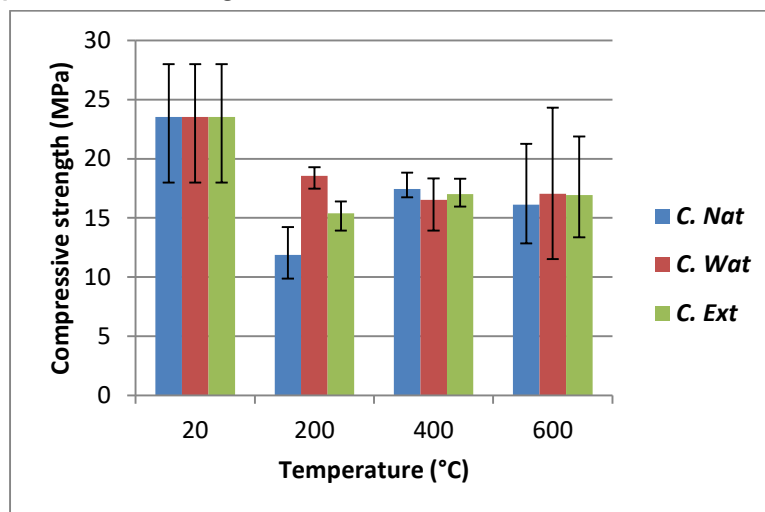


Figure 5 – Effect of temperature and the mode of cooling on compressive strength
 Рис. 5 – Влияние температуры и режима охлаждения на прочность при сжатии
 Слика 5 – Утицај температуре и начина хлађења на компресивну снагу

Table 10 – Effect of temperature and the mode of cooling on compressive strength (MPa)
 Таблица 10 – Влияние температуры и режима охлаждения на прочность при сжатии (МПа)
 Табела 10 – Утицај температуре и начина хлађења на компресивну снагу (МПа)

	20 °C	600 °C	Мра	%
C. Nat	23.53	16.12	7.41	31.5
C. Wat	23.53	17.02	6.51	27.7
C. Ext	23.53	16.93	6.6	28.0

Figure 5 shows the effect of temperature and the cooling mode (air, water, and extinguisher) on compressive strength. We notice that resistance decreases with increasing temperature. This loss of resistance can reach 40%.

Table 10 clearly shows that compressive strength is practically the same for all three cooling modes.

Thermal damage

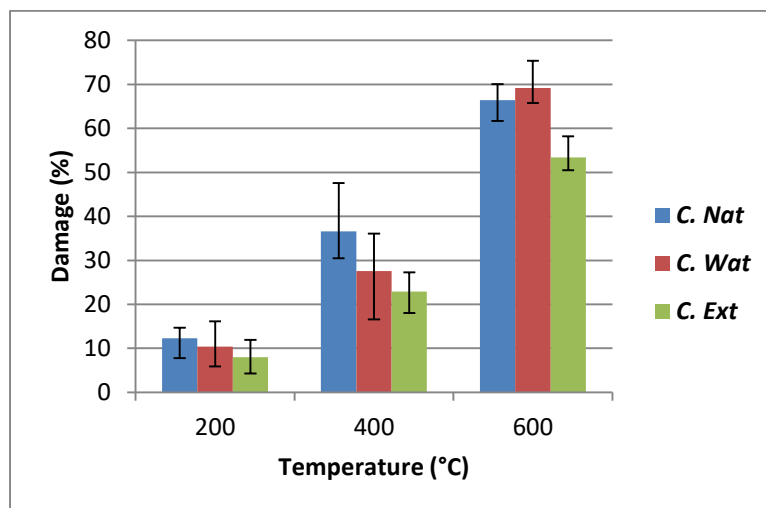


Figure 6 – Variation in thermal damage as a function of temperature and the cooling mode

Рис. 6 – Изменение термического повреждения в зависимости от температуры и режима охлаждения

Слика 6 – Варијација термалног оштећења у зависности од температуре и начина хлађења

Table 11 – Variation in thermal damage as a function of temperature and the cooling mode (%)

Таблица 11 – Изменение термического повреждения в зависимости от температуры и режима охлаждения (%)

Табела 11 – Варијација термалног оштећења у зависности од температуре и начина хлађења (%)

	20 °C	600 °C	%
C. Nat	12.301	66.42	81.5
C. Wat	12.301	69.15	82.2
C. Ext	12.301	53.42	77.0

In Figure 6, we show the effect of temperature and the mode of cooling (air, water, and extinguisher) on the variation of thermal damage. We note, for the three cooling modes, that damage increases with the increase in temperature. It is clear the thermal damage is a little lower with the use of the extinguisher as a means of cooling.

Absorption of water

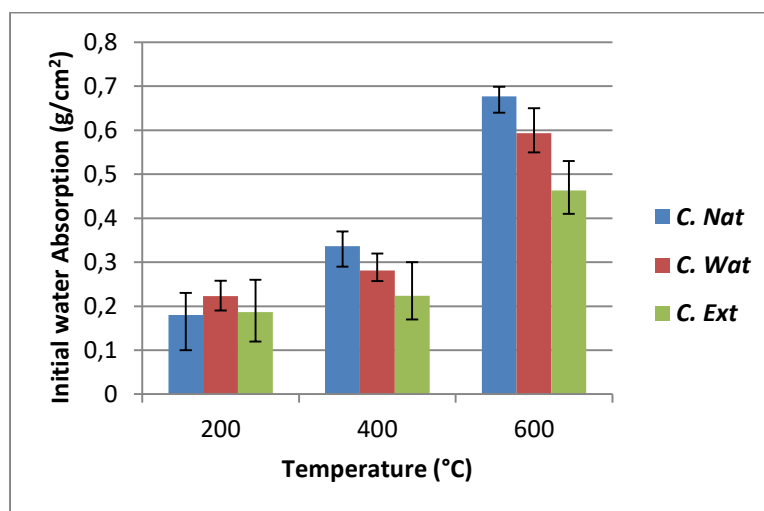


Figure 7 – Effect of temperature and the mode of cooling on initial water absorption

Рис. 7 – Влияние температуры и режима охлаждения на начальное водопоглощение

Слика 7 – Утицај температуре и начина хлађења на иницијалну апсорпцију воде

Table 12 – Effect of temperature and the mode of cooling on initial water absorption (g/cm²)

Таблица 12 – Влияние температуры и режима охлаждения на начальное водопоглощение (г/см²)

Табела 12 – Утицај температуре и начина хлађења на иницијалну апсорпцију воде (г/см²)

	20 °C	600 °C	g/cm ²	%
C. Nat	0.23854	0.6773	0.43876	64.8
C. Wat	0.23854	0.5933	0.35476	59.8
C. Ext	0.23854	0.4633	0.22476	48.5

Figure 7 shows the effect of temperature and the cooling mode (air, water, and extinguisher) on initial water absorption. It is observed that water absorption increases with increasing temperature, particularly at 600 °C. In addition, it is found that water absorption under cooling with the extinguisher is always lower compared to the other two cooling modes. We notice in Table 12 that the use of the extinguisher to put out fire has less absorptivity compared to the two other cooling methods.

Conclusion

The primary goal of this paper is to provide an experimental contribution to the study of the effect of a mode on the behavior of micro-concretes exposed to high temperatures. In this study, the temperatures used are those tested in the majority of previous studies; they are 200, 400, and 600 °C.

Until now, two cooling modes have been used to extinguish fire: one slow, which is natural cooling; and the second fast, which is water cooling. Through this research attempt, we have examined a third mode of cooling; it is the extinguisher. This cooling process practically constitutes an intermediate mode between a slow one and a fast one. For better compression, we carried out mechanical tests concerning compressive strength, thermal damage, modulus of elasticity, and other physical properties: porosity, density, and speed of sound propagation. These tests were carried out hot and after cooling on specimens previously exposed to temperatures of 20°C, 200°C, 400°C, and 600°C.

According to the results obtained (Figures 1 to 7 and Tables 6 to 12), it can be concluded that cooling by the extinguisher presents the most suitable mode for extinguishing a fire of up to 600 °C.

Overall, the analysis of the parameters analyzed (Figures 1 to 7 and Tables 6 to 12) leads us to suggest using the powder extinguisher in the process of extinguishing fire in concrete structures exposed to temperatures up to 600 °C.

In a future study, we will try to analyze the effect of cooling time on the thermal behavior of ordinary concrete as well as to extend this study to other existing concrete types.

References

-ACI (American Concrete Institute). 1989. *216R-89: Guide for Determining the Fire Endurance of Concrete Elements (Reapproved 2001)* [online]. Available at:

https://www.concrete.org/store/productdetail.aspx?ItemID=21689&Format=DOWNLOAD&Language=English&Units=US_Units [Accessed: 05 September 2023].

-ACI (American Concrete Institute). 2007. *ACI 216.1-07/TMS-216-07 Code Requirements for Determining Fire Resistance of Concrete and Masonry Construction Assemblies. An ACI/TMS Standard. Reported by Joint ACI-TMS Committee 216* [online]. Available at: https://www.concrete.org/portals/0/files/pdf/previews/216107_bkstore_view.pdf [Accessed: 05 September 2023].

-ACI (American Concrete Institute). 2008. *Building Code Requirements For Reinforced Concrete and Commentary (ACI 318)*. Farmington Hills, Michigan, USA: American Concrete Institute.

Akçaözoğlu, K. 2013. Microstructural examination of concrete exposed to elevated temperature by using plane polarized transmitted light method. *Construction and Building Materials*, 48, pp.772-779. Available at: <https://doi.org/10.1016/j.conbuildmat.2013.06.059>.

Annerel, E. & Taerwe L. 2009. Revealing the temperature history in concrete after fire exposure by microscopic analysis. *Cement and Concrete Research*, 39(12), pp.1239-1249. Available at: <https://doi.org/10.1016/j.cemconres.2009.08.017>.

Aitcin, P.C.C. 2003. The durability characteristics of high performance concrete: a review. *Cement and Concrete Composites*, 25(4-5), pp.409-420. Available at: [https://doi.org/10.1016/S0958-9465\(02\)00081-1](https://doi.org/10.1016/S0958-9465(02)00081-1).

Bangi, M.R. & Horiguchi, T. 2012. Effect of fibre type and geometry on maximum pore pressures in fibre-reinforced high strength concrete at elevated temperatures. *Cement and Concrete Research*, 42(2), pp.459-466. Available at: <https://doi.org/10.1016/j.cemconres.2011.11.014>.

Bazant, Z.P. & Kaplan, M.F. 1996. *Concrete at High Temperatures (Longman Concrete Design and Construction Series) (1st Edition)*. London, UK: Pearson. ISBN: 978-0582086265.

Bi, J., Liu, P., & Gan, F. 2020. Effects of the cooling treatment on the dynamic behavior of ordinary concrete exposed to high temperatures. *Construction and Building Materials*, 248, art.number:118688. Available at: <https://doi.org/10.1016/j.conbuildmat.2020.118688>.

Carstensen, J.V., Jomaas, G. & Pankaj, P. 2013. Element Size and Other Restrictions in Finite-Element Modeling of Reinforced Concrete at Elevated Temperatures. *Journal of Engineering Mechanics*, 139(10), pp.1325-1333. Available at: [https://doi.org/10.1061/\(ASCE\)EM.1943-7889.0000578](https://doi.org/10.1061/(ASCE)EM.1943-7889.0000578).

-CEN (The European Committee for Standardization). 1994. *CEN ENV 1994-1-2:1994(MAIN) Eurocode 4: Design of composite steel and concrete structures - Part 1-2: General rules - Structural fire design* [online]. Available at: <https://standards.iteh.ai/catalog/standards/cen/6476197f-10f8-435d-8813-683bbdbd497e/env-1994-1-2-1994> [Accessed: 05 September 2023].

-CEN (The European Committee for Standardization). 2002. *CEN EN 1991-1-2:2002(MAIN) Eurocode 1: Actions on structures - Part 1-2: General actions - Actions on structures exposed to fire* [online]. Available at: <https://standards.iteh.ai/catalog/standards/cen/5bdb5478-f413-4f23-a3e2-2eba83dc303f/en-1991-1-2-2002> [Accessed: 05 September 2023].

-CEN (The European Committee for Standardization). 2004. *CEN EN 1992-1-2:2004(MAIN) Eurocode 2: Design of concrete structures - Part 1-2: General rules - Structural fire design* [online]. Available at: <https://standards.iteh.ai/catalog/standards/cen/597bff7e-4f49-446f-ac9b-69829a09d098/en-1992-1-2-2004> [Accessed: 05 September 2023].

Du, S., Zhang, Y., Sun, Q., Gong, W., Geng, J. & Zhang, K. 2018. Experimental study on color change and compression strength of concrete tunnel lining in a fire. *Tunnelling and Underground Space Technology*, 71, pp.106-114. Available at: <https://doi.org/10.1016/j.tust.2017.08.025>.

-European Commissions. 1992. Eurocode 2: Design of concrete structures. *Eurocodes.jrc.ec.europa.eu* [online]. Available at: <https://eurocodes.jrc.ec.europa.eu/EN-Eurocodes/eurocode-2-design-concrete-structures> [Accessed: 05 September 2023].

Ezekiel, S., Xiao, R.Y. & Chin, C.S. 2013. Constitutive Model for Compressive Strength and Elastic Modulus for Concrete under Elevated Temperature. In: *Proceedings of the Structures Congress*, Pittsburgh, Pennsylvania, USA, pp.2916-2925, May 2-4. Available at: <https://doi.org/10.1061/9780784412848.254>.

Gawin, D., Pesavento, F. & Schrefler, B.A. 2011. What physical phenomena can be neglected when modelling concrete at high temperature? A comparative study. Part 2: Comparison between models. *International Journal of Solids and Structures*, 48(13), pp.1945-1961. Available at: <https://doi.org/10.1016/j.ijsolstr.2011.03.003>.

Hammoud, R., Yahia, A. & Boukhili, R. 2014. Triaxial Compressive Strength of Concrete Subjected to High Temperatures. *Journal of Materials in Civil Engineering*, 26(4). Available at: [https://doi.org/10.1061/\(ASCE\)MT.1943-5533.0000871](https://doi.org/10.1061/(ASCE)MT.1943-5533.0000871).

Hertz, K.D. 2005. Concrete strength for fire safety design. *Magazine of Concrete Research*, 57(8), pp.445-453. Available at: <https://doi.org/10.1680/macr.2005.57.8.445>.

Huo, J.S., He, Y.M., Xiao, L.P. & Chen, B.S. 2013. Experimental study on dynamic behaviours of concrete after exposure to high temperatures up to 700 °C. *Materials and Structures*, 46, pp.255-265. Available at: <https://doi.org/10.1617/s11527-012-9899-x>.

Ingham, J.P. 2009. Application of petrographic examination techniques to the assessment of fire-damaged concrete and masonry structures. *Materials Characterization*, 60(7), pp.700-709. Available at: <https://doi.org/10.1016/j.matchar.2008.11.003>.

Jia, B., Li, Z.L., Tao, J.L. & Zhang, C.T. 2011a. The Dynamic Mechanical Constitutive Equation of Concrete under High Temperature. *AMM (Applied Mechanics and Materials)*, Vol.99-100, pp.782-785. Available at: <https://doi.org/10.4028/www.scientific.net/amm.99-100.782>.

Jia, B., Li, Z.L., Yao, H.C. & Tao, J.L. 2011b. SHPB Test on Dynamical Mechanical Behavior of Concrete with High Temperature. *AMM (Applied Mechanics and Materials)*, Vol.71-78, pp.760-763. Available at: <https://doi.org/10.4028/www.scientific.net/amm.71-78.760>.

Khoury, G.A. 2000. Effect of fire on concrete and concrete structures. *Progress in Structural Engineering and Materials*, 2(4), pp.429-447. Available at: <https://doi.org/10.1002/pse.51>.

Khoury, G.A., Anderberg, Y., Both, K., Fellingner, J., Høj, N.P. & Majorana, C. 2007. Fire design of concrete structures - materials, structures and modelling. *fib Bulletin*, 38. Available at: <https://doi.org/10.35789/fib.BULL.0038>.

Kodur, V. 2014. Properties of Concrete at Elevated Temperatures. *International Scholarly Research Notices*, art.ID:468510. Available at: <https://doi.org/10.1155/2014/468510>.

Li, Z., Xu, J. & Bai, E. 2012. Static and dynamic mechanical properties of concrete after high temperature exposure. *Materials Science and Engineering: A*, 544, pp.27-32. Available at: <https://doi.org/10.1016/j.msea.2012.02.058>.

Liu, P., Zhou, X., Qian, Q., Berto, F. & Zhou, L. 2019. Dynamic splitting tensile properties of concrete and cement mortar. *Fatigue and Fracture of Engineering Materials & Structures*, 43(4), pp.757-770. Available at: <https://doi.org/10.1111/ffe.13162>.

Lu, Xia., Lu, Xin., Guan, H. & Ye, L. 2013. Collapse simulation of reinforced concrete highrise building induced by extreme earthquakes. *Earthquake Engineering Structural Dynamics*, 42(5), pp.705-723. Available at: <https://doi.org/10.1002/eqe.2240>.

Ma, Q., Guo, R., Zhao, Z., Lin, Z. & He, K. 2015. Mechanical properties of concrete at high temperature – A review. *Construction and Building Materials*, 93, pp.371-383. Available at: <https://doi.org/10.1016/j.conbuildmat.2015.05.131>.

Noumowe, A. 2005. Mechanical properties and microstructure of high strength concrete containing polypropylene fibers exposed to temperatures up to 200 °C. *Cement and Concrete Research*, 35(11), pp.2192-2198. Available at: <https://doi.org/10.1016/j.cemconres.2005.03.007>.

Phan, L.T. & Carino, N.J. 2000. Fire Performance of High Strength Concrete: Research Needs. In: *Proceedings of Structures Congress*, Philadelphia, Pennsylvania, USA, pp.1-8, May 8-10 Available at: [https://doi.org/10.1061/40492\(2000\)181](https://doi.org/10.1061/40492(2000)181).

Pihlajavaara, S E. & Kesler, C.E. 1972. Analysis of the factors exerting effect on strength and other properties of concrete at elevated temperatures. In: *International seminar on concrete for nuclear reactors*, Berlin, F.R. Germany, October 5 [online]. Available at: <https://www.osti.gov/biblio/4489011> [Accessed: 05 September 2023].

Shi, J-s., Xu, J-y., Ren, W-b. & Su, H-y. 2014. Research on Energy Dissipation and Fractal Characteristics of Concrete after Exposure to Elevated Temperatures under Impact Loading. *Acta Armamentarii*, 35(5), pp.703-710 [online]. Available at: <http://www.co-journal.com/EN/abstract/abstract1191.shtml> [Accessed: 05 September 2023].

Su, H., Xu, J. & Ren, W. 2014. Experimental study on the dynamic compressive mechanical properties of concrete at elevated temperature. *Materials & Design (1980-2015)*, 56, pp.579-588. Available at: <https://doi.org/10.1016/j.matdes.2013.11.024>.

Tanaçan, L., Ersoy, H.Y. & Arpacioğlu, Ü. 2009. Effect of high temperature and cooling conditions on aerated concrete properties. *Construction and Building*

Materials, 23(3), pp.1240-1248. Available at: <https://doi.org/10.1016/j.conbuildmat.2008.08.007>.

Tao, J.-l., Qin, L.-b., Li, K., Liu, D., Jia, B., Chen, X.-w. & Chen, G. 2011. Experimental investigation on dynamic compression mechanical performance of concrete at high temperature. *Explosion and Shock Waves*, 1, pp.101-106 [online]. Available at:

https://caod.oriprobe.com/articles/26396575/Experimental_investigation_on_dynamic_compression_mechanical_performan.htm [Accessed: 05 September 2023].

Tanchev, R. & Purnell, P. 2005. An application of a damage constitutive model to concrete at high temperature and prediction of spalling. *International Journal of Solids and Structures*, 42(26), pp.6550-6565. Available at: <https://doi.org/10.1016/j.ijsolstr.2005.06.016>.

Tomar, M.S. & Khurana, S. 2019. Impact of passive fire protection on heat release rates in road tunnel fire: A review. *Tunnelling and Underground Space Technology*, 85, pp.149-159. Available at: <https://doi.org/10.1016/j.tust.2018.12.018>.

Van der Heijden, G.H.A., Van Bijnen, R.M.W., Pel, L. & Huinink, H.P. 2007. Moisture transport in heated concrete, as studied by NMR, and its consequences for fire spalling. *Cement and Concrete Research*, 37(6), pp.894-901. Available at: <https://doi.org/10.1016/j.cemconres.2007.03.004>.

Wang, Y.-t. 2014. Static and dynamic mechanical properties of concrete after high temperature treatment. *Journal of Vibration and Shock*, 01 January [online]. Available at: https://typeset.io/papers/static-and-dynamic-mechanical-properties-of-concrete-after-3l0vqs3cx6?citations_has_pdf=true [Accessed: 05 September 2023].

Wang, T.-T. & Shang, B. 2014. Three-Wave Mutual-Checking Method for Data Processing of SHPB Experiments of Concrete. *Journal of Mechanics*, 30(5), pp.5-10. Available at: <https://doi.org/10.1017/jmech.2014.55>.

Zhai, Y., Li, Ya., Li, Yu., Wang, S., Liu, Y. & Song, K.-I. 2019. Impact of high-temperature-water cooling damage on the mechanical properties of concrete. *Construction and Building Materials*, 215, pp.233-243. Available at: <https://doi.org/10.1016/j.conbuildmat.2019.04.161>.

Zhai, Yu., Deng, Z., Li, N. & Xu, R. 2014. Study on compressive mechanical capabilities of concrete after high temperature exposure and thermo-damage constitutive model. *Construction and Building Materials*, 68, pp.777-782. Available at: <https://doi.org/10.1016/j.conbuildmat.2014.06.052>.

Zhang, H., Gao, Y.W., Li, F., Lu, F. & Sun, H. 2013. Experimental study on dynamic properties and constitutive model of poly propylene fibre concrete under highstrain rates. *European journal of environmental and civil engineering*, 17(suppl.1), pp.294-303. Available at: <https://doi.org/10.1080/19648189.2013.834601>.

Zhao, Y., Bi, J., Zhou, X. & Huang, Y. 2019. Effect of High Temperature and High Pressure of Water on Micro-Characteristic and Splitting Tensile Strength of Gritstone. *Frontiers in Earth Science*, 7, 13 November. Available at: <https://doi.org/10.3389/feart.2019.00301>.

Экспериментальное исследование тепловых свойств бетона

Сара Затар^а, Наср Рахал^б, **корреспондент**, Худа Багден^в,
Абдулайзиз Суайсии^б, Халима Туауад^в, Халид Ебммахди^в

^а Университет Тахри Мохаммед Бешар, департамент архитектуры и урбанизма, г. Бешар, Алжирская Народная Демократическая Республика

^б Университет Туши Мустафы Стамбули, строительный факультет, г. Маскара, Алжирская Народная Демократическая Республика; Университет естественных наук и технологий, лаборатория машиностроения и прочности конструкций, г. Оран, Алжирская Народная Демократическая Республика

^в Университет Туши Мустафы Стамбули, строительный факультет, Маскара, Алжирская Народная Демократическая Республика

РУБРИКА ГРНТИ: 67.09.33 Бетоны. Железобетон. Строительные растворы, смеси, составы

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: При воздействии огня, а также при быстром или медленном охлаждении частей бетонного сооружения происходят различные изменения плотности, пористости, скорости распространения звука, модуля упругости, прочности на сжатие, водопоглощения и пр. Эти процессы также могут вызвать термическое повреждение. Широкое использование бетона в строительстве, с одной стороны, и проблемы, вызванные воздействием огня, с другой, требуют углубленного понимания влияния огня на поведение бетонной конструкции, особенно после охлаждения. До сих пор для тушения пожара использовались два метода охлаждения: водой и свободным потоком воздуха. Цель данной статьи — экспериментально исследовать использование огнетушителя как третьего способа охлаждения бетона, подвергающегося воздействию высоких температур.

Методы: Для достижения цели исследования была проведена серия механических и физических испытаний образцов диаметром 40 мм и высотой 40 мм, подвергнутых воздействию высоких температур 200, 400 и 600 °С. Затем испытуемые образцы были подвергнуты трем различным режимам охлаждения, а именно: свободным потоком воздуха, водой и огнетушителем.

Результаты: Результаты однозначно показывают, что использование огнетушителя целесообразнее, чем два других метода охлаждения, а именно: воздухом и водой.

Выводы: Результаты этого экспериментального исследования могут быть полезны на практике при тушении пожара в бетонном сооружении.

Ключевые слова: бетон, пожар, экспериментальное исследование, тушение, вода, воздух.

Експериментална анализа изложености бетона термичким променама

Сара Затар^а, Наср Рахал^б, **аутор за преписку**, Худа Багден^в,
Абдулајиз Суајси^б, Халима Туауад^в, Халид Ебммахди^в

^а Универзитет Тахри Мохамед у Бешару, Одељење за архитектуру и урбанизам, Бешар, Народна Демократска Република Алжир

^б Универзитет Мустафа Стамболи, Одсек за грађевинарство, Маскара, Народна Демократска Република Алжир;
Универзитет природних наука и технологије, Лабораторија за машинске структуре и стабилност конструкције, Оран, Народна Демократска Република Алжир

^в Универзитет Мустафа Стамбоули, Одсек за грађевинарство, Маскара, Народна Демократска Република Алжир

ОБЛАСТ: материјали, грађевинарство
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Када су делови бетонске структуре изложени дејству ватре, а затим брзом или спором хлађењу, долази до различитих промена у густини, порозности, термичком оштећењу, брзини ширења звука, модулусу еластичности, компресивној снази, апсорпцији, итд. Раширена употреба бетона у грађевинарству, с једне стране, и проблеми настали услед изложености пожару, с друге стране, захтевају детаљно разумевање утицаја ватре на понашање структуре бетона, нарочито после хлађења. До сада су коришћена два метода хлађења за гашење ватре – водом и слободним струјањем ваздуха. У раду је експериментално анализирано коришћење противпожарног апарата као трећег начина за хлађење бетона изложеног високим температурама.

Методе: Извршена је серија механичких и физичких испитивања узорака, пречника 40 mm и висине 40 mm, изложених високим температурама од 200, 400 и 600 °C. Затим су тест-епрувете подвргнуте хлађењу на три различита начина: слободним струјањем ваздуха, потапањем у воду и коришћењем противпожарног апарата.

Резултати: Резултати јасно показују да је коришћење противпожарног апарата погодније од преостала два метода хлађења, тј. природног хлађења на ваздуху и натапања водом.

Закључак: Резултати ове експерименталне студије могли би да имају практичну примену при гашењу евентуалног пожара у некој бетонској структури.

Кључне речи: бетон, ватра, експериментална анализа, гашење, вода, природно струјање ваздуха.

Paper received on / Дата получения работы / Датум пријема чланка: 10.09.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 01.12.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 02.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).


© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).




Treatment of bauxite residues - acidic leaching (first part)

Srećko R. Stopić^a, Vladimir Damjanović^b, Radislav Filipović^c,
Mary D. Kamara^d, Bernd G. Friedrich^e

^a RWTH Aachen University, IME Process Metallurgy and Metal Recycling, Aachen, Federal Republic of Germany,
e-mail: sstopic@ime-aachen.de, **corresponding author**,
ORCID iD:  <https://orcid.org/0000-0002-1752-5378>

^b Alumina Ltd, Zvornik, Republic of Srpska, Bosnia and Herzegovina,
e-mail: vladimir.damjanovic@birac.ba,
ORCID iD:  <https://orcid.org/0000-0002-5375-440X>

^c Alumina Ltd, Zvornik, Republic of Srpska, Bosnia and Herzegovina,
e-mail: radislav.filipovic@birac.ba,
ORCID iD:  <https://orcid.org/0009-0000-9938-2499>

^d RWTH Aachen University, IME Process Metallurgy and Metal Recycling, Aachen, Federal Republic of Germany,
e-mail: kamaramarydora@gmail.com,
ORCID iD:  <https://orcid.org/0009-0005-1923-3570>

^e RWTH Aachen University, IME Process Metallurgy and Metal Recycling, Aachen, Federal Republic of Germany,
e-mail: bfriedrich@ime-aachen.de,
ORCID iD:  <https://orcid.org/0000-0002-2934-2034>

DOI: 10.5937/vojtehg71-46212; <https://doi.org/10.5937/vojtehg71-46212>

FIELD: chemical technology

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Bauxite residue as a waste product from the aluminium industry produced through the Bayer process is mainly composed of iron oxide, titanium oxide, silicon oxide and undissolved alumina together with a wide range of other oxides and a minor content of rare earth elements, gallium, vanadium and scandium, which vary according to the country of origin of the bauxite. The extraction of valuable elements from bauxite residues and the minimisation of bauxite residues during different treatments are an open research field.

ACKNOWLEDGMENT: This research was funded by the Federal Ministry for Education and Research Grant Number 03SF0626C "Verbundvorhaben GSP Green H2: WASCAL Internationales Masterprogramm für Energie und Grünen Wasserstoff (IMP-EGH)".

Methods: Different hydrometallurgical and pyrometallurgical methods were used for the treatment of bauxite residues. In this study, the results of the hydrometallurgical treatment of bauxite residue from Alumina Zvornik using sulfuric acid and hydrochloric acid will be shown in order to study the change of the mineralogical composition. Leaching efficiency will be calculated using the ICP OES analysis. The XRD-Analysis was used for the characterization of the initial material and solid residues studying the change of the mineralogical phases.

Results: Leaching of bauxite residues with sulphuric and hydrochloric acid leads partially to the change of mineralogical structure and the transfer of elements into a liquid phase. Natural precipitation of iron is observed over time. Silica gel formation is confirmed during leaching of bauxite residues with hydrochloric acid.

Conclusion: A new research strategy for treating bauxite residue is needed in order to ensure a complete change of the initial mineralogical structure and the most efficient transfer of metals into a liquid phase.

Key words: bauxite residues, aluminium, hydrometallurgy, acid, recycling, rare earth elements.

Introduction

The Bayer process is a traditional industrial method for the production of alumina from bauxite ore. The chemical quality of precipitated aluminum hydroxide, and consequently the final alumina product in the Bayer process directly depends on the level of impurities in a refinery's Bayer liquor. Under optimal reaction parameters (temperature and time), it is possible to remove iron, zinc and copper from the Bayer liquor using a precipitation agent such as calcium hydroxide with an efficiency of more than 90%, in such a way that the treated solution is still economically usable in the following stages of processing while obtaining different types of aluminum trihydrate. (Damjanović et al, 2020)

In Europe, alumina refineries operate in Bosnia and Herzegovina (Alumina, Zvornik), France, Hungary, Germany, Greece, Ireland (AAL), Romania (ALUM), Spain and Ukraine, while significant BR deposits from refineries that have stopped their operations (legacy sites) exist in former Yugoslavia (Podgorica, Kidricevo, Mostar, Obrovac), Italy, France (RT), Germany, Hungary and other countries. The current BR production level in the EU is 6.8 million tonnes per year while the cumulative stockpiled level is a staggering >250 million tonnes (dry matter).

The mineralogical structure of bauxite residue, where nearly 80 % consists of three of these phases: cancrinite, sodalite and hematite, is shown in Table 1. (Castaldi et al, 2008)

Table 1 – Typical mineralogical structure of bauxite residue (in wt. -%)
 Таблица 1 – Типичный минералогический состав бокситового шлама (в процентном соотношении)

Табела 1 – Типична минералска структура бокситних остатака (у тежинским процентима)

Cancrinite [$\text{Na}_6\text{Ca}_{1.5}\text{Al}_6\text{Si}_6\text{O}_{24}(\text{CO}_3)_{1.6}$]:	29.0-33.0
Sodalite [$\text{Na}_8(\text{Cl},\text{OH})_2\text{Al}_6\text{Si}_6\text{O}_{24}$]:	16.0-24.0
Hematite [Fe_2O_3]:	27.0-29.0
Boehmite [$\text{AlO}(\text{OH})$]:	5.0-6.0
Gibbsite [$\text{Al}(\text{OH})_3$]:	4.0-5.0
Anatase [TiO_2]:	5.0
Andradite [Ca-Fe-Al-Si oxides]:	4.0
Quartz [SiO_2]:	2.0

Bauxite residues contain scandium and gallium (Approx. 50-150 ppm) and up to an order of magnitude higher for elements such as: vanadium and rare earths elements (0.05-0.5 %). Since 1991, MYTILINEOS, Greece, has been doing pioneering research on BR handling and reuse, focusing initially on massive low value applications such as use as a raw material for geopolymers bricks, cement clinker production, iron production, bricks and tile production, soil remediation (vegetation), extraction of rare earth elements, and road substrate.

Due to the generation of large amounts of bauxite residue (red mud), an alternative method, called the Pedersen Process was considered in order to prevent bauxite residue generation (Lazou et al, 2020). In the conventional Pedersen Process, iron in bauxite is separated in the form of pig iron through a carbothermic smelting-reduction step which has a carbon dioxide emission similar to that during conventional iron production. In order to eliminate the carbon dioxide emission of this step, the focus of their work was to reduce the iron oxides of bauxite ore by hydrogen gas prior to smelting and minimizing the use of solid carbon materials for the reduction. Calcination and reduction of bauxite ore by hydrogen was studied by the thermogravimetry method supported by the microstructural and phase analysis confirming that the reduction of hematite to magnetite and magnetite to iron starts at temperatures below 560 °C with a slow rate and is faster at higher temperatures. At higher temperatures, i.e., 860, 960, and 1060 °C, the formation of hercynite (FeAl_2O_4) retards the complete reduction to metallic iron.

The possibilities to recover rare earths from bauxite residues, which commonly contain only low concentrations of rare-earth elements, but are available in very large volumes and could provide significant amounts of

rare earths to European countries are the main research subject of the European funded projects (EURARE; REMOVAL, SCALE, REDMUD) in the last ten years. The extraction rate of the rare earth recovery from these industrial waste streams is a part of a comprehensive, zero-waste, “product-centric” valorisation scheme, in which applications are found for the residual fractions that are obtained after removal of not only the rare earths but also other critical metals such as scandium, vanadium and gallium and especially the base elements: aluminium, titanium and iron (Binnemans et al, 2015).

Unfortunately, the extraction of aluminium, iron and titanium from bauxite residue under acid leaching is limited due to an insufficient amount of acidic solution from leaching caused by the polymerization of silica (Rivera et al, 2017). Kinetic studies have demonstrated that, at constant temperatures, silica dissolution increases with increasing acid concentrations, but it decreases when the temperature is increased and the acid concentration is reduced. This is due to the enhancement in the solubility of monomeric silicic acid formed during acidic leaching. The control mechanisms of silica dissolution have been described according to the shrinking core model by a chemical reaction stage, i.e., silica polymerization, followed by a diffusion stage, because of the silica gel adsorbed on the surface of the particles that limits the metal extraction. The recovery of iron, titanium, aluminium, and rare earth elements from bauxite residues preventing silica gel formation was performed using the dry digestion process with sulphuric acid and hydrogen peroxide (Alkan et al, 2018). The operational parameters were investigated and the addition of 2.5M hydrogen peroxide into 2.5M sulfuric acid was decided to be the best leaching condition to have favored quartz formation with a suppressed rhomboclase precipitation. Since the leaching reactions are mainly controlled by diffusion, no significant increase in the efficiencies was observed after 30 minutes of leaching. While Si gel was not formed in the oxidative environment, high titanium extraction from bauxite residue was only achieved when hydrogen peroxide was introduced into the acidic solution.

The combined pyrometallurgical and hydrometallurgical treatment of bauxite residue for the recovery of valuable metals included firstly carbothermic reduction (Xakalashé & Friedrich, 2018). The reductive smelting of bauxite residue uses coke as the reductant between 1500 and 1550°C and acidic to basic fluxes to low temperature smelting and the production of conditioned slag. Additional conditioning of bauxite residue with basic oxygen furnace slag and bottom ash as fluxing agents in the smelting process was performed in order to recover the valuable metals

with the exclusive use of the secondary resources as slag formers (Lucas et al, 2018). The final products based on aluminium, titanium, rare earth elements and scandium were obtained after a hydrometallurgical treatment using leaching, filtration, and precipitation (Yagmurlu et al, 2019).

The aim of this work is to offer the first information about the characterisation of bauxite residue from Alumina, Zvornik, and study its behaviour after a hydrometallurgical treatment using hydrochloric and sulphuric acid under the atmospheric pressure in the absence of hydrogen peroxide!

Methods

The mineralogical characterization of the samples was carried out using the X-ray diffraction technique – XRD. After the measurement, we processed the spectral images of the sample with the help of Difrac software, EVA v 4.2.2. The obtained values $d(2\theta)$, which are characteristic for each mineralogical phase, were compared with the literature data in the existing database, and thus we identified the present crystal phases.

The sample preparation was performed in single steps. The samples needed to be prepared so that their granulation was about $50\mu\text{m}$, so that a flat-surface pallet could be made in polyethylene molds. In most samples, it was difficult to fulfill this condition due to the hardness of the samples that could not be prepared in the crucible. Regardless of the difficulties, making a pallet that did not have a flat surface was successful. The operational conditions are present in Table 2:

Table 2 – Operational data for the XRD-measurement
Таблица 2 – Оперативные данные для рентгеноструктурного анализа
Табела 2 – Операциони подаци коришћени за рендгеноструктурну анализу

Device	Model	Producer	Current	Voltage	Time per step	Range 2θ	step
XRD	Endeavor D8	Bruker	40mA	35KV	40mA	10-90	0.5

In order to determine the elements in the ppm range, the samples are measured on the ICP-OES device, using an optical emission technique that uses inductive-coupled plasma as a source. This technique is intended for analysing trace elements and requires translating the sample into an acidic solution. The sample preparation was performed using ISO

6607-1985 method. The method involves the destruction of the sample with three concentrated acids (sulfuric, nitric and hydrochloric) at the beginning, and the treatment of the precipitate with hydrofluoric acid to translate residual elements (except SiO₂) into a solution. After this preparation, a complete dissolution was expected. Total dissolution was confirmed during the treatment of solid residue obtained in the leaching experiments at 90°C.

Material

Due to its properties such as high alkalinity, bauxite residue can be used as an input material in various neutralization processes. Three different types of bauxite residue were compared, as shown in Table 3.

Table 3 – Chemical Composition of BR (Lucas et al, 2021)
Таблица 3 – Химический состав бокситового шлама (Lucas et al, 2021)
Табела 3 – Хемички састав бокситних остатака (Lucas et al, 2021)

Percent (%)	Fe ₂ O ₃	Al ₂ O ₃	CaO	SiO ₂	TiO ₂	Na ₂ O	Cr ₂ O ₃	Sc (ppm)
Germany	35.3	15.7	6.7	14.0	11.4	8.9	0.2	86
Greece	44.0	23.0	10.2	5.5	5.6	1.8	0.3	122
Zvornik	49.3	12.0	8.2	10.5	4.6	2.5	0.13	76

This table shows that the bauxite residue from Zvornik, Bosnia and Herzegovina contains mostly iron oxide. The Greek bauxite residue contains more scandium, aluminium oxide, and chromium oxide but smaller content of sodium oxide than the German and Zvornik ones. The bauxite residue from Germany is highly alkaline due to the presence of sodium hydroxide from the Bayer process. Bauxite residue was provided from Alumina Ltd, Zvornik, Bosnia and Herzegovina, as the starting raw material. The Alumina factory has been in the continuous production mode since October 6, 1978, and continuously processes bauxite and produces alumina, hydrates, zeolites, and other related aluminosilicate products. The Alumina company currently has about 1500 employees, which is about 25 % of all employees in Zvornik. Alumina owns a red mud disposal site located about 5 km from the factory. The transportation of the red mud suspension from the factory to the landfill is carried out by suitable pumps. The area of the red sludge landfill is about 1 km², as shown in Figure 1.

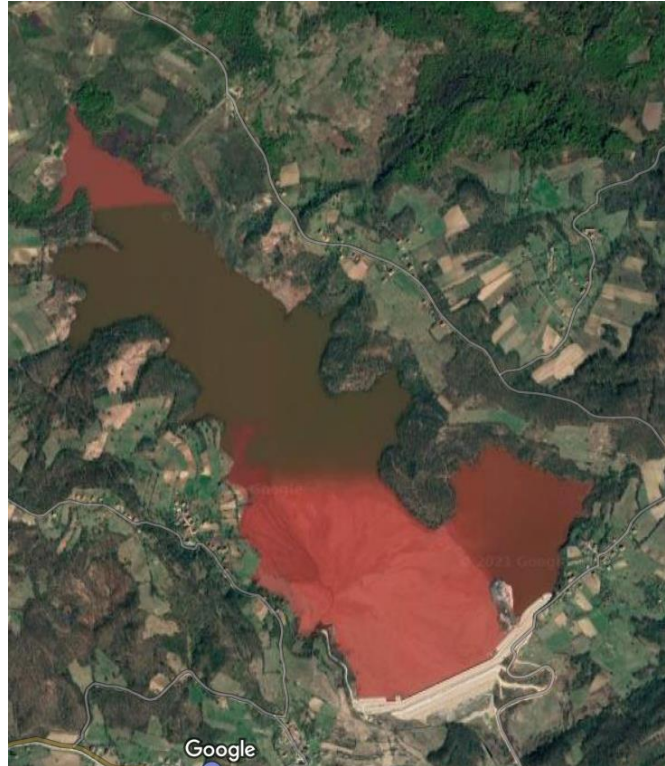


Figure 1 – Area of the accumulated bauxite residue in Zvornik, Bosnia and Herzegovina

Рис. 1 – Площадь скопления бокситового шлама в г.Зворник, Босния и Герцеговина

Слика 1 – Поверхина акумулисаног бокситног остатка у Зворнику, Босна и Херцеговина

During the operation of the Alumina Ltd. company, about 19.4×10^6 m³ of red mud suspension was disposed of. Depending on the quality of bauxite, the amount of completely dry red mud typically ranges from 0.8 to 2 tons of tailings per ton of alumina produced. The Alumina Ltd. company from Zvornik uses bauxite with a silicon dioxide modulus between 8.5 and 12. Accordingly, the amount of red mud that is separated and disposed of at the landfill is about 1.0 - 1.2 tons per ton of Al₂O₃ produced, or approximately 400,000 t / per year. The installed technical-technological equipment at the clearing plant is of a continuous (uninterrupted) nature, where there are five installed autoclave batteries of 11-12 interconnected autoclaves in series (each autoclave has 50 m³).

The bauxite residue from alumina was filtrated, washed and dried at 105 °C for 24 h. The chemical composition of bauxite residue is shown in Table 4.

Table 4 – Chemical composition of BR, Zvornik
Таблица 4 – Химический состав бокситового шлама в г. Зворник
Табела 4 – Хемијски састав бокситних остатака у Зворнику

Compounds	%	Compounds	%
Ignition loss at 1000°C	8,32	Ga ₂ O ₃	0,225
SiO ₂	10,52	CuO	0,007
Fe ₂ O ₃	49,29	K ₂ O	0,159
Na ₂ O	2,45	Tl ₂ O ₃	0,088
TiO ₂	4,59	MnO	0,145
CaO	8,23	MgO	0,627
Al ₂ O ₃	12,03	NiO	0,034
Ag ₂ O	0,001	PbO	0,019
BaO	0,014	P ₂ O ₅	0,930
Cr ₂ O ₃	0,133	ZnO	0,016
Sc ₂ O ₃	0,011	V ₂ O ₅	0,135
Co ₂ O ₃	0,012	SrO	0,075

One additional elemental ICP -OES analysis was performed in order to establish the content of rare earth elements (REE) presented in Table 5:

Table 5 – Content of rare earth elements in BR, Zvornik
Таблица 5 – Содержание редкоземельных элементов бокситового шлама в г. Зворник
Табела 5 – Садржај елемената ретких земаља у бокситним остацима у Зворнику

Content	Pr	Sc	Y	La	Ce	Nd	Sm	Tb	total
ppm	12	76	133	114	250	96	11	8	700

As shown in Figure 2, the XRD-analysis found the following phases: hematite, perovskite, cancrinite, cancrinite, ilmenite, calcite, diaspore, gibbsite, and hydrogarnet. Iron is available in the hematite and ilmenite structures. Titanium is present in perovskite and ilmenite structures, while aluminum is available in the structures of cancrinite, diaspore, boehmite, gibbsite, and hydrogarnet.

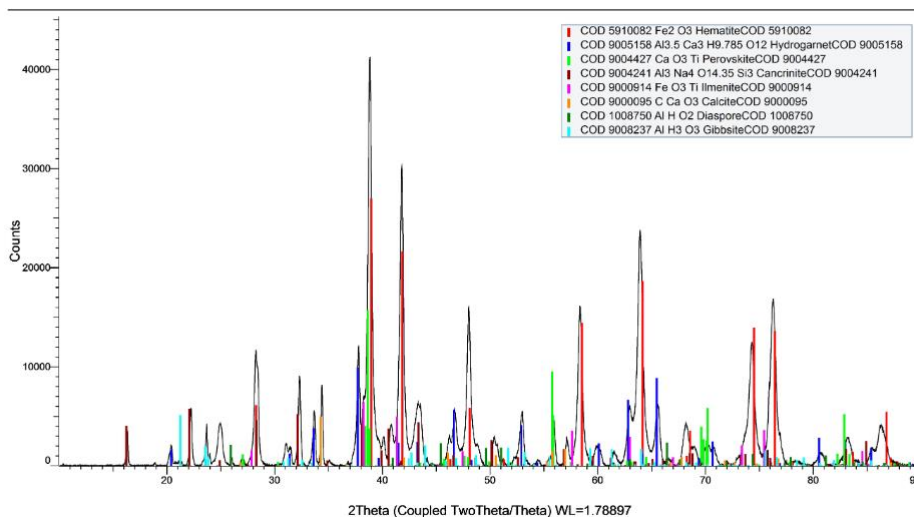


Figure 2 – XRD-analysis of BR from Zvornik
 Рис. 2 – Рентгеноструктурный анализ бокситового шлама в г. Зворник
 Слика 2 – Рендгеноструктурна анализа бокситног остатка из Зворника

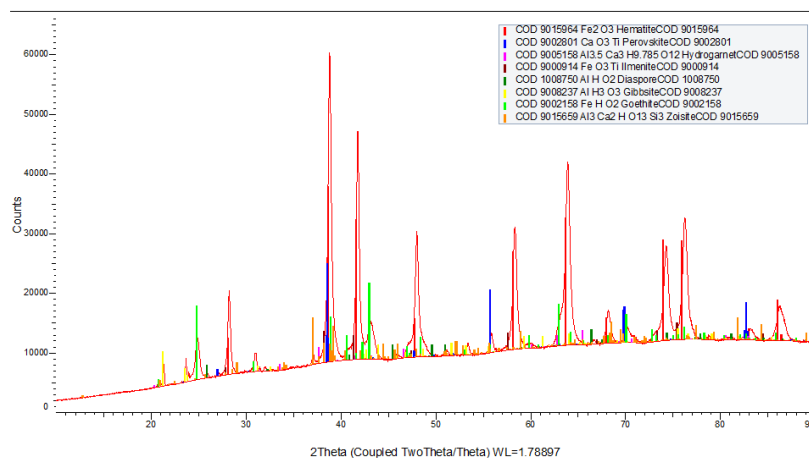


Figure 3 – XRD-analysis of solid residue after leaching with 1mol/L hydrochloric acid at 90 °C for 2 hours
 Рис. 3 – Рентгеноструктурный анализ твердого шлама после выщелачивания 1 моль/л соляной кислоты при 90°C в течение 2 часов
 Слика 3 – Рендгеноструктурна анализа чврстог остатка после лужења 1 Mol/L хлороводоничном киселином на 90°C, у трајању од два сата

Experimental

The first experiments were performed in order to study the change of the mineralogical structure during leaching experiments. The leaching was performed using 1mol/l hydrochloric acid and 1mol/L sulfuric acid at 90 °C with a solid/liquid ratio 1:10 and a mixing rate of 200 rpm for 2 hours. The obtained XRD-analysis results are shown in Figures 3 and 4.

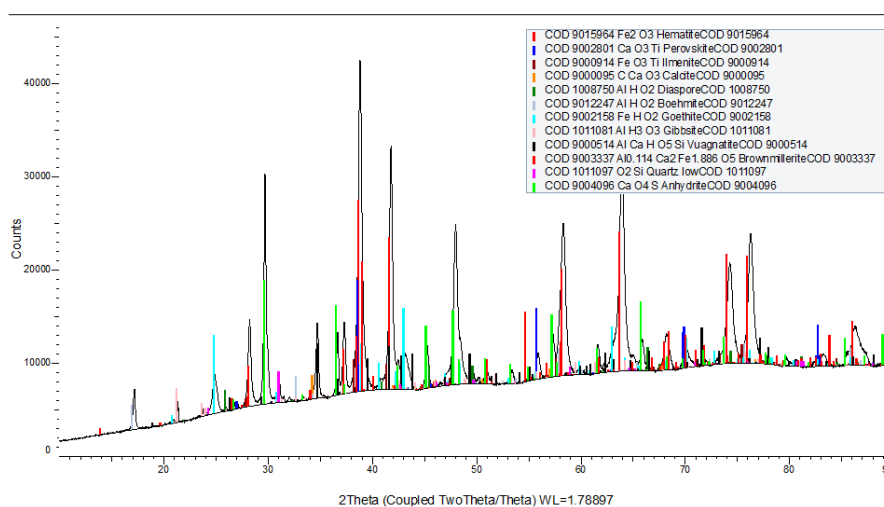


Figure 4 – XRD-analysis of solid residue after leaching with 1mol/L sulphuric acid at 90 °C for 2 hours

Рис. 4 – Рентгеноструктурный анализ твердого шлама после выщелачивания 1 моль/л серной кислоты при 90°C в течение 2 часов

Слика 4 – Рендгеноструктурна анализа черстог остатка после лужења 1 Mol/L сумпорном киселином на 90°C, у трајању од два сата

The comparative analysis of the obtained XRD-analysis results is presented in Table 6.

The analysis of the initial bauxite residue in Figure 2 has shown that Fe is present in the hematite and ilmenite structure, Ti in perovskite and ilmenite and Al in cancrinite, diaspore, boehmite, gibbsite and hydrogarnet. Direct leaching of BR (as shown in Figs. 3 and 4) confirms that the mineral structure is not only changed, but also some new compounds are found such as vuagnitit, brownmillerite, anhydrite (CaSO_4), as shown int Figure 3. The addition of sulphuric acid leads to the formation of insoluble calcium sulphate.

Table 6 – Comparative analysis of the mineralogical phases
 Таблица 6 – Сравнительный анализ минералогических фаз
 Табела 6 – Упоредна анализа минералогичких фаза

Material	Process	Mineral	Phase composition
Red mud (Bauxite residue)	Bayer (autoclave) T=150°C t=2 hours addition of NaOH	Hematite Perovskite Cancrinite Ilmenite Calcite Diaspore Gibbsite Hydrogarnet	Fe ₂ O ₃ CaTiO ₃ Al ₃ Si ₃ Na ₄ O _{14.35} FeTiO ₃ CaCO ₃ AlOOH Al(OH) ₃ Al _{3.5} Ca ₃ H _{9.875} O ₁₂
Solid residue after a leaching of BR with hydrochloric acid	Leaching of BR using 1 mol/L HCl, 90 °C, 120 min	Hematite Perovskite Hydrogarnet Diaspore Gibbsite Goethite Zoisite	Fe ₂ O ₃ CaTiO ₃ Al _{3.5} Ca ₃ H _{9.875} O ₁₂ AlOOH Al(OH) ₃ FeOOH Ca ₂ Al ₃ (SiO ₄)(Si ₂ O ₇)O(OH)
Solid residue after a leaching of BR with sulfuric acid	Leaching of BR using 1 mol/L H ₂ SO ₄ , 90 °C, 120 min	Hematite Perovskite Ilmenite Calcite Diaspore Boehmite Goethite Gibbsite Vuagnatit Brownmillerite Quartz Anhydrite	Fe ₂ O ₃ CaTiO ₃ FeTiO ₃ CaCO ₃ α-AlOOH Y-AlOOH FeOOH Al(OH) ₃ CaAlSiO ₄ (OH) Ca ₂ (Al,Fe) ₂ O ₅ SiO ₂ CaSO ₄

The analysis of the obtained solution with the calculated leaching efficiencies is shown in Table 7:

Table 7 – Chemical composition of the obtained solution and the calculated leaching efficiency

Таблица 7 – Химический состав полученного раствора и рассчитанная эффективность выщелачивания

Табела 7 – Хемијски састав добијеног раствора и израчуната ефикасност лужења

Elements from solutions are presented as compounds	Leaching with 1M HCl (90°C, 2hours, s/L: 1/10)		Leaching with 1M H ₂ SO ₄ (90°C, 2hours, s/L: 1/10)	
	Content (mg/L)	Leaching Efficiency (%)	Content (mg/L)	Leaching Efficiency (%)
Al ₂ O ₃	7190	59.76	7292	60.61
SiO ₂	2351	22.34	1369	13.01
P ₂ O ₅	84.7	9.10	128.1	13.76
V ₂ O ₅	8.8	6.51	41.4	30.66
SrO	12.6	16.8	7.9	10.53
Ga ₂ O ₃	10,9	4.84	22.4	9.95
K ₂ O	46.2	29.05	56.4	35.47
Y ₂ O ₃	16.3	9.65	13.6	8.05
NiO	4.44	13.08	9.1	26.76
Cr ₂ O ₃	15.3	11.50	19.1	14.36
MnO	11.2	7.7	15.2	10.45
Ce ₂ O ₃	13.3	4.54	4.0	1.37
Sc ₂ O ₃	4.98	45.27	5.82	52.90
PbO	5.27	27.73	4.4	23.16
Fe ₂ O ₃	718	1.46	1096	2.23
TiO ₂	233	5.07	441	9.60

For aluminum, the maximum leaching efficiency was about 60 % for both used acids. The small leaching efficiency has confirmed that the leaching time of 2 hours was not enough to ensure complete leaching efficiency. Leaching efficiency from scandium is maximal for critical metals (52.90 %), but not sufficient.

Therefore, the increased concentration of solution, reaction temperature, and duration of process in the presence of hydrogen peroxide will be considered in order to increase leaching efficiency. The formation of silica gel is confirmed in a study of the leaching process with sulfuric acid under the atmospheric pressure, as shown in Figure 5:



Figure 5 – Formation of silica gel after sulfuric acid leaching at 90°C
Рис. 5 – Образование силикагеля после сернокислотного выщелачивания при 90°C
Слика 5 – Формирање силика гела након растварања сумпорном киселином на 90°C

Natural precipitation of iron from the obtained solution has been confirmed after leaching with hydrochloric acid, as shown in Figure 6!

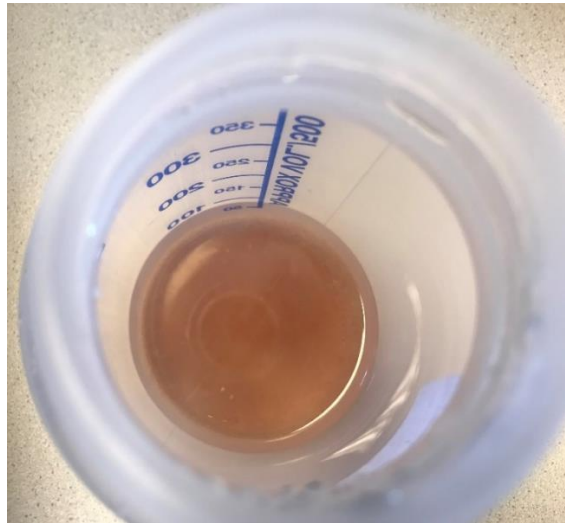


Figure 6 – Natural precipitation of iron after hydrochloric acid leaching at 90°C
Рис. 6 – Естественное осаждение железа после солянокислотного выщелачивания при 90°C
Слика 6 – Природно таложење железа након растварања хлороводоничном киселином на 90°C

The formation of silica gel and the natural precipitation of iron can be prevented through the dry digestion process in the presence of hydrogen

peroxide, as mentioned in the literature review. The performed experiments of acidic leaching confirmed some difficulties related to a direct leaching process. Therefore, highly efficient technology is proposed to improve leaching efficiency of valuable metals. The pyrometallurgical method can ensure destroying the mineralogical structure of bauxite residue forming a more suitable slag structure for better leaching using different acids. A combined pyrometallurgical and hydrometallurgical method for the treatment of bauxite residue will be reported in the future in order to improve a direct leaching process.

Conclusion

The hydrometallurgical treatment of bauxite residue with 1mol/l hydrochloric acid and 1mol/L sulphuric acid at 90°C for 2 hours leads to a maximum leaching efficiency of aluminium about 60 %, 53 % of scandium and a minimum efficiency of other valuable elements, respectively. The analysis of the changes in the mineralogical structure has revealed that small changes are possible during the hydrometallurgical treatment. A new research strategy for the treatment of bauxite residue is needed in order to ensure a full change of the initial mineralogical structure and the most efficient transfer of metals from bauxite residues to a liquid phase. The formation of insoluble calcium sulphate is found during leaching with sulphuric acid. The silica gel formation and the natural precipitation of iron from the solution are some difficulties that can be prevented using dry digestion. The following step is an improvement of a direct leaching process using a pyrometallurgical method such as hydrogen plasma reduction.

References

- Alkan, G., Yagmurlu, B., Cakmakoglu, S., Hertel, T., Kaya, S., Gronen, L., Stopic, S. & Friedrich, B. 2018. Novel Approach for Enhanced Scandium and Titanium Leaching Efficiency from Bauxite Residue with Suppressed Silica Gel Formation. *Scientific Reports*, 8, art.number:5676. Available at: <https://doi.org/10.1038/s41598-018-24077-9>.
- Binnemans, K., Jones, P.T., Blanpain, B., van Garven, T. & Pontikes, Y. 2015. Towards zero-waste valorisation of rare-earth-containing industrial process residues: a critical review. *Journal of Cleaner Production*, 99, pp.17-38. Available at: <https://doi.org/10.1016/j.jclepro.2015.02.089>.
- Castaldi, P., Silvetti, M., Santona, L., Enzo, S. & Melis, P. 2008. XRD, FTIR, and thermal analysis of bauxite ore-processing waste (red mud) exchanged with heavy metals. *Clays and Clay Minerals*, 56, pp.461-469. Available at: <https://doi.org/10.1346/CCMN.2008.0560407>.

Damjanović, V., Kostić, D., Ostojić, Z., Perušić, M., Filipović, R., Oljača, Dj., Obrenović, Z. & Mičić, V. 2020. The Influence of Process Parameters on Removing Iron, Zinc and Copper Impurities from Synthetic Bayer Liquor. In: *TRAVAUX 49, Proceedings of the 38th International ICSOBA Conference*, virtual, pp.325-334, November 16-18 [online]. Available at: <https://icsoba.org/assets/files/publications/2020/AA21S.pdf> [Accessed: 1 June 2023].

Lazou, A., van der Eijk, C., Balomenos, E., Kolbeinsen, L. & Sfarian, J. 2020. On the Direct Reduction Phenomena of Bauxite Ore Using H₂ Gas in a Fixed Bed Reactor. *Journal of Sustainable Metallurgy*, 6, pp.227-238. Available at: <https://doi.org/10.1007/s40831-020-00268-5>.

Lucas, H., Alkan, G., Xakalashé, B. & Friedrich, B. 2018. Conditioning of bauxite residue with bottom ash in view of recovery of valuable metals: A sustainable approach. In: *2nd international Bauxite Residue Valorisation and Best Practices Conference (BR2018)*, Athens, Greece, pp.263-270, May 7-10.

Lucas, H., Stopić, S., Xakalashé, B., Ndlovu, S. & Friedrich, B. 2021. Synergism Red Mud-Acid Mine Drainage as a Sustainable Solution for Neutralizing and Immobilizing Hazardous Elements. *Metals*, 11(4), art.number:620. Available at: <https://doi.org/10.3390/met11040620>.

Rivera, R.M., Ulenaers, B., Ounoughene, G., Binnemans, K. & van Gerven, T. 2017. Behaviour of Silica during Metal Recovery from Bauxite Residue by Acidic Leaching. In: *Travaux 46, Proceedings of 35th International ICSOBA Conference*, Hamburg, Germany, pp.547-556, October 2-5 [online]. Available at: <https://icsoba.org/assets/files/publications/2017/BR13S%20-%20Behavior%20of%20Silica%20during%20Metal%20Recovery%20from%20Bauxite%20Residue%20by%20Acidic%20Leaching.pdf> [Accessed: 1 June 2023].

Xakalashé, B. & Friedrich, B. 2018. Combined carbothermic reduction of bauxite residue and basic oxygen furnace slag for enhanced recovery of Fe and slag conditioning. In: *2nd international Bauxite Residue Valorisation and Best Practices Conference (BR2018)*, Athens, Greece, pp.233-240, May 7-10.

Yagmurlu, B., Alkan, G., Xakalashé, B., Schier, C., Gronen, L., Koiwa, I., Dittrich, C. & Friedrich, B. 2019. Synthesis of Scandium Phosphate after Peroxide Assisted Leaching of Iron Depleted Bauxite Residue (Red Mud) Slags. *Scientific Reports*, 9, art.number:11803. Available at: <https://doi.org/10.1038/s41598-019-48390-z>.

Обработка бокситового шлама – кислотное выщелачивание
(первая часть)

Сречко Р. Стопич, **корреспондент**, Владимир Дамянович^б,
Радислав Филипович^б, Мери Д. Камарад^а, Бернд Г. Фридрих^а

^а Технический университет города Ахен,
Институт металлургических процессов и рециклирования металлов,
г. Ахен, Федеративная Республика Германия

^б ООО „Алумина“, г. Зворник, Республика Сербская,
Босния и Герцеговина

РУБРИКА ГРНТИ: 61.13.21 Химические процессы
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Бокситовый шлам, являющийся побочным продуктом алюминиевой промышленности, получаемый по способу Байера, в основном состоит из оксида железа, оксида титана, оксида кремния и нерастворимого оксида алюминия, а также широкого спектра других оксидов и незначительного содержания редкоземельных элементов, галлия, ванадия и скандия. Извлечение ценных элементов из бокситового шлама и минимизация его образования в ходе обработки являются недостаточно исследованной областью.

Методы: В обработке бокситового шлама использовались различные гидрометаллургические и пирометаллургические методы. В данном исследовании представлены результаты гидрометаллургической обработки бокситового шлама из глинозема Зворник с использованием серной и соляной кислот с целью изучения изменения минералогического состава. Эффективность выщелачивания рассчитана на основании анализа ICP OES. Рентгеноструктурный анализ был использован в изучении свойств исходного материала и твердого шлама и в изучении изменений минералогических фаз.

Результаты: Выщелачивание бокситового шлама серной и соляной кислотой частично приводит к изменению минералогической структуры и преобразованию элементов в жидкую фазу. С течением времени наблюдается естественное осаждение железа в состоянии покоя. Подтверждено образование силикагеля в процессе выщелачивания бокситового шлама соляной кислотой.

Выводы: В области обработки бокситового шлама необходимо разработать новую исследовательскую стратегию с целью обеспечения полного изменения исходной минералогической структуры и наиболее эффективного преобразования металлов в жидкую фазу.

Ключевые слова: бокситовый шлам, алюминий, гидрометаллургия, кислота, рециклирование, редкоземельные элементы.

Третирање бокситних остатака – лужење (први део)

Срећко Р. Стопић, **аутор за преписку**, Владимир Дамјановић^б,
Радислав Филиповић^б, Мери Д. Камарад^а, Бернд Г. Фридрих^а

^а Технички универзитет у Ахену, Институт за процесну металургију и рециклирање метала, Ахен, Савезна Република Немачка

^б Алумина доо, Зворник, Република Српска, Босна и Херцеговина

ОБЛАСТ: хемијске технологије

КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Остатак од лужења боксита је отпадни производ из индустрије алуминијума настао у Бајеровом процесу састављен од оксида железа, титана, силицијума и нераствореног алуминијум-оксида са широким спектром других оксида и минималним садржајем елемената ретких земаља, галијума, ванадијума и скандијума, који се мења сагласно земљи из које потиче. Екстракција вредних елемената из бокситног остатка и минимизација бокситног остатка кроз различите третмане су отворено истраживачко поље.

Методe: Различите хидрометалуршке и пиروметалуршке методе коришћене су за третирање бокситних остатака. У раду су приказани резултати хидрометалуршког третмана коришћењем сумпорне и хлороводоничне киселине како би се проучиле промене минералског састава. Ефикасност лужења биће израчуната коришћењем ИЦП ОЕС анализе. Рендгеноструктурна анализа коришћена је за карактеризацију почетног материјала и чврстог остатка проучавајући промене минералошких фаза.

Резултати: Растварање бокситног остатка сумпорном и хлороводоничном киселином води делимично до промене минералске структуре и трансфера елемената у течну фазу. Природна преципитација железа присутна је током стајања. Формирање силика гела потврђено је током растварања бокситних остатака хлороводоничном киселином.

Закључак: Нова истраживачка стратегија неопходна је за третирање бокситног остатка како би се обезбедила потпуна промена минералошке структуре и много ефикаснији пренос метала у течну фазу.

Кључне речи: бокситни остатак, алуминијум, хидрометалургија, киселина, рециклирање, елементи ретких земаља.

Paper received on / Дата получения работы / Датум пријема чланка: 28.06.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 01.12.2023.

Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 02.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons licencom (<http://creativecommons.org/licenses/by/3.0/rs/>).



Risk management of unexploded ordnance in the Republic of Serbia for environmental protection - Borovac case study

Ivan M. Potić^a, Nenad M. Komazec^b, Ljiljana M. Mihajlović^c, Aleksandar M. Milić^d, Saša T. Bakrač^e

^a Military Geographical Institute "General Stevan Bošković",
Belgrade, Republic of Serbia,
e-mail: ivan.potic@vs.rs,
ORCID iD: <https://orcid.org/0000-0002-0691-7675>

^b University of Defence in Belgrade, Military Academy,
Belgrade, Republic of Serbia,
e-mail: nenadkomazec@yahoo.com,
ORCID iD: <https://orcid.org/0000-0001-9227-118X>

^c University of Belgrade, Faculty of Geography,
Belgrade, Republic of Serbia,
e-mail: ljiljana.mihajlovic@gef.bg.ac.rs, **corresponding author**,
ORCID iD: <https://orcid.org/0000-0003-4022-8248>

^d University of Defence in Belgrade, Military Academy,
Belgrade, Republic of Serbia,
e-mail: milickm5@gmail.com,
ORCID iD: <https://orcid.org/0000-0002-2642-0340>

^e Military Geographical Institute "General Stevan Bošković",
Belgrade, Republic of Serbia,
e-mail: sasa.bakrac@vs.rs,
ORCID iD: <https://orcid.org/0000-0003-0211-3765>

DOI: 10.5937/vojtehg71-44656; <https://doi.org/10.5937/vojtehg71-44656>

FIELD: geographic information systems, environmental management,
risk management

ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Decades of dealing with unexploded ordnance (UXO) in some areas of the Republic of Serbia have confirmed that it presents a substantial hazard to the security of people, property, and the environment. Even though the terrain has been cleaned, various threats from difficult-to-find UXO components remain serious. Inadequate systemic solutions for UXO management can have significant harmful consequences.

ACKNOWLEDGMENT: The research reported in this paper was supported by Project 451-03-47/2023-01/200091 (Ministry of Science, Technological Development and Innovation of the Republic of Serbia) and written as part of Project 1.23/2023 (Ministry of Defence of the Republic of Serbia).

Methods: Based on the spatial distribution analysis and different UXO types and quantities, this article studies the effects of dangerous components of unexploded ordnance on human lives and the environment. Two different geospatial analyses were performed including the guidelines for risk management through risk elimination based on multiple criteria, the GIS, and the Remote Sensing analysis.

Results: Two different geospatial analyses resulted in the areas at high risk of remaining UXO.

Conclusion: The article significantly contributes to creating an environmental risk management strategy for UXO-contaminated regions. It presents an effective technique for addressing risk assessment challenges in such sites. The analysis considers both risk analysis and environmental protection options. Using the multi-criteria analysis and the GIS, it estimates the exposure of built structures, people, soil types, and plant species to UXO dangers in key locations. This paper serves as a guideline for environmental risk assessment.

Keywords: UXO, risk management, environmental protection, security, geospatial analysis.

Introduction

The Republic of Serbia has been facing the problem of unexploded ordnance (UXO)¹ remaining on its territory as a legacy of modern armed conflicts. Removing and destroying UXO should be considered a practical security task, as it entails reducing explosive ordnance and devices to a form in which they can no longer perform their intended lethal function. The detection and removal of UXO have become an increasingly urgent problem.

On the one hand, there is a need to reduce risks to the population and the environment from the explosion. On the other hand, the likelihood of unwanted accidents increase over time due to various physical and chemical processes in UXO, increasing the risk and possibility of extremely negative consequences on the environment and humans. The effects of UXO containing depleted uranium are not territorially or temporally limited; they cause far-reaching impacts on both friendly and hostile military and civilian targets, contaminating the air, land, and water, thus indirectly entering the food chain of living beings. Contamination extends to places that have not been directly impacted by armed conflicts. U-234, U-235, and U-238 are three isotopes of natural uranium that differ

¹ The widely established term unexploded ordnance (UXO) will continue to be used further on.

only in nuclear properties. Since uranium is a radioactive element, it emits atomic radiation when it decomposes in the environment. The chemical properties of depleted uranium (DU) are identical to those of natural uranium; however, it has much fewer isotopes than U-235 (0.2%) (McLaughlin et al, 2003). It is a low-level radioactive waste element as a by-product of uranium processing for nuclear reactors and weapons.

UXO does not contain only depleted uranium which was used during the bombing campaign against the Republic of Serbia in 1999 (Orlić, 2000). First and foremost, the impact of explosive charges (certain types of explosives) must be considered during detonation (explosion). The explosive charge compositions vary depending on the UXO manufacturer although they mainly contain highly destructive explosives (high explosives). TNT is the most common one; smaller charges may use more powerful explosives (such as tetryl) or other types (Cauderay, 1993). Explosive charges come in various weights depending on the type and function of a projectile (Orlić, 2000). Ammunition with higher explosive content harms technical equipment and results in more human resource losses. It does not only harm human health by inflicting physical damage (loss of limbs, loss of sight and hearing, etc.), but it also damages the environment by destroying pedological and geological substrates, causing ecological damage, and alike.

As a by-product of nuclear technology, depleted uranium is classified as low-level radioactive waste (Sahoo et al, 2004) and is mainly disposed of in specialized landfills. Since DU is increasingly used for military and civilian purposes, there is a significant increase in radiotoxicity and chemotoxicity to humans and the environment. Evaluating the depleted uranium impact implications on the environment and individuals is contentious (Orlić, 2000).

Representatives of Western countries' official military and state institutions reduce the potential for damage, stating that uranium is already present in the natural environment and that its increase due to weapons with depleted uranium is insignificant and geographically variable (Popovic et al, 2008). In contrast, non-official organizations, such as US military veterans' associations or environmental movements, often draw harsh conclusions (Popovic et al, 2008). One of the purposes of this research is to show possible acute and subsequent geospatial consequences for the environment using the multi-criteria GIS analysis.

Considering the time that has passed and the fact that the contaminated sites have been cleared for years, it is not likely that the national radioactivity monitoring would reveal substantial quantities of depleted uranium in the environment. Estimating the risk of unexploded

ordnance to the environment, contamination, mobility, and the possibility of depleted uranium being absorbed into diverse inorganic or organic substrates is crucial for future research.

Several research groups in Serbia have examined depleted uranium contamination, primarily through the Ministry of Education, Science, and Technological Development - funded scientific research programs, and, during remediation initiatives in southern Serbia, international cooperation has been achieved (Popovic et al, 2008). Since 2011, radioactivity management (owing to the environmental samples from the places where depleted uranium ammunition was used) has been mandated as part of the national monitoring program for radioactivity. Depending on needs, additional research should consider analytical techniques with higher sensitivity, such as high-resolution mass spectrometry and other more advanced physicochemical methods. Past analyses do not indicate significant deviations from natural variations in the uranium isotope content and ratios. The research might lead to a better understanding of the speciation and mobility of depleted uranium in the environment. Results that show the current or permanent threat of UXO can be obtained using the multi-criteria data analysis and GIS techniques. The effects of the endangerment of subsurface and surface water sources, soil, and other resources were derived based on the geo-ecological features of the studied area. The number of endangered residents can be estimated based on the facilities in the analyzed region at a specified distance from the contaminated sites (Popovic et al, 2008).

The term 'unexploded ordnance' is defined by the majority of experts in the field as "means equipped with military explosives that did not explode or function as intended, which includes military ammunition, anti-tank and anti-personnel mines, water mines, bombs, rockets, mortar shells, artillery shells, hand grenades or rocket-propelled grenades, and missiles or rocket-propelled grenades" (Landmine Action, 2002; The Geneva International Centre for Humanitarian Demining, 2019; Martin et al, 2019; Australian Government, Defence, 2020; Government of Canada, 2021).

Remote sensing is becoming an increasingly necessary and inescapable means of space data collection for military purposes. Along with monitoring and documenting the condition of diverse natural and social phenomena, all satellite primary missions and programs can effectively complete increasingly complex duties associated with military actions (Regodić, 2008). The GIS is critical for data management concerning geographic areas (environmental changes) and is one of the most promising research methodologies and information technologies.

Evelyn Pruitt's (1960) definition of remote sensing was: "Remote sensing is a technique for acquiring data via systems that are not in direct physical touch with the event or item being studied" (Salomonson, 2014). GIS maps enable the integration and updating of vast volumes of data. This procedure is critical for safety purposes while testing for possible UXO.

Materials and methods

According to the research by the Demining Center of Serbia, it is estimated that the territory of the Republic of Serbia contaminated by UXO covers approximately 25 km² (Republika Srbija, Centar za Razminiranje, 2022). The area cleared of cluster bombs following international standards has grown to 11.6 km². Using the data on the sites effectively cleaned in the areas of Bujanovac (Table 1), Preševo (Table 2), and the airport complexes in the vicinity of Sjenica (Table 3), researchers may estimate the level of contamination and the probability of severe environmental impacts.

Table 1 – Overview of the UXO removed from the Bujanovac Municipality (Republika Srbija, Centar za Razminiranje, 2022)

Таблица 1 – Осмотр неразорвавшихся боеприпасов, вывезенных из муниципалитета Буяновац (Республика Сербия, Центр разминирования, 2022 год)

Табела 1 – Преглед неексплодираних убојних средстава уклоњених са територије општине Бујановац (Republika Srbija, Centar za razminiranje, 2022)

S.No.	Locality name	Area (km ²)	Type and quantity of means
1	„Borovac-3“ Bujanovac	0.102	BLU 97 -1 pc
2	„Borovac-4“ Bujanovac	0.109	BLU 97 -1 pc UXO (missile) -1 pc Fragment of KM -1 pc
3	„Turijska brda“ -Bujanovac	0.389	TMA -10 pcs Artillery shell fuzes-3 pcs RB - 1 pc 155 mm artillery shell -1 pc
4	„Bujanovac sever“ Bujanovac	0.276	PMA-2 -3 pcs Hand grenade M52P3 -1 pc
5	„Bujanovac sever“ Bujanovac	0.145	PMA-2 -5 pcs
6	„Bujanovac sever“ Bujanovac	0.071	PMA-1 -3 pcs PMR-2A -1 pc

7	„Bujanovac sever“ Bujanovac	0.114	PMA-2 -5 pcs RB -1 pc Mb bomb -1pc RB -1 pc
8	„Dobrosin“ Bujanovac	0.220	PMA-2 -6 RB -1 pc PMR-2A -3 pcs RB -1 pc
9	„Lučane“ Bujanovac	0.073	UXO -10 RB -1 pc 762 mm rounds -1.341 RB -1 pc
10	„TS Bujanovac – TS Berivojce“ Bujanovac	0.018	PMA -2 RB -1 pc
11	„Končulj-Singerit“ Bujanovac	0.199	PMA -20 RB -1 pc
12	„TS Bujanovac – TS Berivojce“ Bujanovac	0.002	////
13	„Končulj-Singerit 1“ Bujanovac	0.269	TMA-5 -1 pc RB 1 pc Projectiles for RRB M79 - 9 RB 1 pc Ammunition -1.577 RB -1 pc
14	Turijsko brdo	0.076	Anti-personnel mines -4 RB -1 pc
15	Bogdanovac 1	0.113	MK-4 -12 RB -1 pc
16	Bogdanovac 2	0.146	MK-4 -14 RB -1 pc
17	Jastrebac 1	0.114	MK-4 -13 RB -1 pc
18	Jastrebac 2	0.155	MK-4 -8 RB -1 pc
19	Karadnik	0.123	BLU97A/B -10 RB -1 pc UXO -5 RB -1 pc
20	Sebrat	0.176	MK-4 -36 RB -1 pc UXO -1pc RB -1 pc

21	Borovac 1	0.060	BLU97A/B -68 RB -1 pc UXO -15 RB -1 pc
22	Borovac 2	0.088	BLU97A/B - 28 RB -1 pc UXO -56 RB -1 pc
23	Bujanovac	1.179	PMA2 -14 RB -1 pc RB -1 pc RB -1 pc
24	Rafatova česma	0.092	Fragments of AB-6 RB -1 pc Fragments of UXO -5 RB -1 pc

Note: KM - cluster munition; RB, PMA2, BLU97A/B, MK -4, TMA, PMR-2A - different types of cluster bombs, AB - air bomb, MbM - mortar shell, UXO - unexploded ordnance

Over two decades after the bombing of Serbia, the issue of explosive remnants of war still exists. Even in the cleared areas, there is a chance that UXO will be detected. Such a situation presents an exceptional danger to both residents and employees (in construction of roads, housing, tourism, industrial and other infrastructure, etc.). Serbia faces numerous demining issues, and the pace at which they are resolved is contingent on the availability of financial funds for demining, among other things. Since 2002, the Demining Center has performed these functions primarily as an autonomous governmental entity but with significant assistance from foreign organizations and funders. Besides that, reconnaissance of areas suspected of being contaminated with cluster bombs, mines, and other UXO is being carried out to reduce the environmental threat. Additionally, demining projects are being created, and funds are being supplied for their execution. The quality of demining is monitored, international cooperation is conducted, international standards and agreements are implemented, etc. (Republika Srbija, Centar za razminiranje, 2022).

However, the repeated reference to war remnants must not obscure the reality that some areas are also contaminated with ammunition dispersed and buried after explosions in manufacturing units and warehouses or burglaries into ammunition depots. Quantities of unexploded ordnance (whether in warehouses or dispersed) are not the data that may be made widely accessible. The given data is accessible to selected structures to carry out important projects for the clearance of UXO from the

designated sites. As a result of these findings, there is a reasonable assumption that different forms of UXO are, after fires and explosions at military storage and manufacturing units (in the cities of Paraćin, Kraljevo, Vranje, and Čačak), currently being discovered outside military facilities over an area of about 13.5 km².

Table 2 – Overview of the UXO removed from the Preševo Municipality (Republika Srbija, Centar za Razminiranje, 2022)

Таблица 2 – Осмотр неразорвавшихся боеприпасов, вывезенных из муниципалитета Прешево (Республика Сербия, Центр разминирования, 2022 год)
Табела 2 – Преглед неексплодираних убојних средстава уклоњених са територије општине Прешево (Република Србија, Центар за разминирање, 2022)

No.	Locality name	Area (in km ²)	Type and quantity of means
1	Buštranje	0.205	KM -48 pcs
2	Buštranje - Đeren	0.148	KM-9 pcs
3	Šatkin Vir	0.129	fragments of KM
4	Šatkin Vir 1	0.100	KM-2 pcs
5	Šatkin Vir 2	0.032	KM-1 pc AB -1 pc
6	Reljan Brezovčani	0.244	KM-25 pcs UXO -6 pcs
7	Šatkin Vir 3	0.118	fragments of KM
8	Pečeno - school	0.088	///
9	Cerevajka 1	0.165	MbM -1 pc
10	Cerevajka 2	0.106	MbM -2 pcs Fragments of KM-4 pcs

Note: KM - cluster munition, AB - air bomb, MbM - mortar shell, UXO - unexploded ordnance

Table 1, Table 2, and Table 3 list the UXO types reported in the Preševo, Sjenica, and Bujanovac zones. A total of 4.232 km² was cleaned in the Bujanovac area. In the municipality of Preševo, the demining procedure covered 1.334 km² of the territory. In the municipality of Sjenica, the region around the airport complex was cleaned during the last four years.

NATO forces launched approximately 15,000 large projectiles on the territory of the former Yugoslavia (Bozanic et al, 2018). Unguided and guided air bombs and missiles from various combat systems amounted to approximately 25,000 tons, with 1,660 cluster bombs, dispensaries containing about 330,000 cluster bombs and more than 50,000 pieces of depleted uranium ammunition (Pamučar et al, 2011). Depleted uranium is radioactive, a health hazard, and a persistent contaminant of the

environment. Several hundred locations were bombed during the NATO air raids in 16 municipalities in Serbia, not including Kosovo and Metohija (City of Niš - Mediana and Crveni Krst, Kraljevo, Brus, Preševo, Bujanovac, Kuršumlija, Raška, Gadžin Han, Tutin, Sjenica, Čačak, Vladimirci, Knić, Stara Pazova, and Sopot) (Pamučar et al, 2011; Bozanic et al, 2018).

Table 3 – Overview of the UXO removed from the areas of the airport complex in the Sjenica region (Republika Srbija, Centar za Razminiranje, 2022)

Таблица 3 – Осмотр неразорвавшихся боеприпасов, вывезенных с территории аэродромного комплекса в регионе Сьеница (Республика Сербия, Центр разминирования, 2022 год)

Табела 3 – Преглед неексплодираних убојних средстава уклоњених са подручја аеродромског комплекса у региону Сјеница (Republika Srbija, Centar za razminiranje, 2022)

No.	Locality name	Year	Type and quantity of means
1	The airport in the region of Sjenica	2018.	Cluster bomb-29 pcs
2		2019.	Cluster bomb-71 pcs Cluster bomb booster-3 pcs 88 mm artillery shell -1 pc
3		2020.	Cluster bomb-72 pcs Air bomb MK-82 -1 pc 80 mm artillery shell -1 pc

Table 4 – Remaining cluster ammunition in the Bujanovac Municipality (Republika Srbija, Centar za Razminiranje, 2022)

Таблица 4 – Оставшије касетне боеприпаси в муниципалитете Буяновац (Республика Сербия, Центр разминирования, 2022 год)

Табела 4 – Преостала касетна муниција у општини Бујановац (Republika Srbija, Centar za razminiranje, 2022)

No.	District	Municipality	Populated place	Name of the suspected area	Number of suspected areas	Size of the suspected area (km ²)
1	Pčinjski	Bujanovac	Borovac	Borovac 5	1	0.281
IN TOTAL					1	0.281
The remaining mine problems in Bujanovac						
No.	District	Municipality	Populated place	Name of the suspected area	Number of tsuspected areas	Size of the suspected area (km ²)
1	Pčinjski	Bujanovac	Dobrosin	Dobrosin 1	1	0.028
2	Pčinjski	Bujanovac	Končulj	Tuštica	1	0.144
3	Pčinjski	Bujanovac	Ravno Bučje	Đorđevac	1	0.390
IN TOTAL					3	0.562

The study emphasizes the municipality of Bujanovac since it is an area that, according to the most recent official data from the Serbian Demining Center, is primarily contaminated with UXO and demands special attention (Table 4).

Research area

The research area is in the Bujanovac municipality near Borovac, the regional Južna Morava River and the JUG military base. The area encompasses 87.05 km² and is located within UTM 34n 555335.402, 4690210.743 and 564706.827, 4699481.616 coordinates. Three analyses have been performed within this area (Fig. 1). Borovac is a settlement in Serbia in the municipality of Bujanovac in the Pčinja district. According to the 2011 census, its population was 166 people (Republika Srbija, Republički zavod za statistiku Srbije, 2023). In 2002, there were 214 inhabitants. According to the 1991 census (before the bombing), the population was 267. It is essentially an adult population. Only 44 homes have remained in the community, fewer than in the previous census (61 in 2002), and the average number of people per household is 3.77 (Republika Srbija, Republički zavod za statistiku Srbije, 2023). Serbs predominantly populate this village, and a reduction in the number of residents was seen in the past three censuses. During the air raids on Serbia in 1999, Borovac was heavily bombed. In certain instances, using depleted uranium led to the relocation of the inhabitants on a large scale, and some were directly or indirectly killed.

Input data

The current situation with UXO (types and quantities) in the Republic of Serbia can be discovered through the multi-criteria data analysis. The content of the documents was examined based on national and international legal regulations concerning UXO risk management. The comparison method demonstrates the crucial distinction in comprehending the need for protection and adequate risk management of residual UXO containing depleted uranium. The GIS analysis is fundamental in the areas with such a significant time and space framework in which this study is conducted. The spatial dispersion of harmful consequences on environmental and human health is not depicted.

Different sets of geospatial data were used to perform a spatial analysis of the potential diffusion of the extension of the UXO impact on the environment:

- Digital Elevation Model (DEM): A DEM with 4.4 m vertical accuracy (Tadono et al, 2016) and 22.45 m spatial resolution was chosen as elevation

data. The initial data for completing a hydrographic analysis to extract watersheds and watercourses was the JAXA ALOS Global Digital Surface Model AW3D30 (Eorc.Jaxa, 2019). TauDEM 5.3 (Tarboton et al, 2015) was used for a terrain analysis to delineate watersheds and extract watercourses.

- Land Cover is created using multispectral satellite imagery: Sentinel 2 satellite imagery was downloaded from Copernicus Sci-Hub (Copernicus, 2020) to create a land cover map using the Dzetsaka classification plugin (Karasiak, 2016) in QGis (QGIS, 2022). The research used Sentinel 2 S2B MSIL2A 20210913T093029 N0301 R136 T34TEN 20210913T114013 cloud-free imagery collected on September 13th, 2021. Satellite data was analyzed and classified using 10m red, green, blue, and near-infrared bands. The Random Forest machine learning algorithm classified five classes from satellite imagery: developed, barren, forest, pastures, and planted/cultivated areas. The Random Forest supervised classification necessitates the creation of a comprehensive and precise training zone selection for each class (Mas & Flores, 2008; Duro et al, 2012; Potić & Potić, 2017; Potić et al, 2017). Regression is used as a pixel-based supervised learning task to model and predict variables where numerical true ground values are provided for the research area. Regression trees (decision trees) are used to classify satellite data, iteratively separating the dataset into distinct branches and maximizing the information gained to understand nonlinear correlations. The Random Forest classifier classifies data with high accuracy using classification trees. The accuracy assessment is performed by generating the error matrix in the Semi-Automatic Classification Plugin (Congedo, 2021) in QGis (QGIS, 2022), which is provided as a table that compares reference data (i.e., ground truth data) with map information for several sample areas to ensure the quality of the classification (Congalton & Green, 2019). Twenty randomly selected points are obtained for each class to finalize the accuracy assessment. Overall accuracy is the ratio of correctly classified samples to total sample units (Congalton & Green, 2019). The Kappa analysis is a discrete multivariate technique for detecting whether two error matrices differ statistically (Plackett, 1976; Congalton & Green, 2019). High-resolution imagery from Google Earth Pro (Google Earth, 2020) and downloadable Sentinel 2 colour and false-colour composites were used to ensure the quality of the accuracy evaluation points.

- Google Earth Pro (Google Earth, 2020) was used to collect additional data, with all watercourses enclosed by a 1-kilometer buffer zone around four UXO locations corrected and updated. Furthermore, the same software is used for digitizing topographic labels and all buildings within a 1-

kilometer buffer zone. The buffer zone for building collection was created as a 1-kilometer 3D distance from the main four UXO drainage streams.

Results

The first analysis for the entire research area consists of delineating watersheds, creating streams and drainage paths from four UXO locations (Fig. 1), and performing a land cover (LC) classification (Fig. 2). When of adequate quality, groundwater is a resource initially considered in all water supply evaluations to settlements. However, subsurface waters have a very tight relationship with surface waters, and they most commonly share their fate in quantity and quality. Significantly, when soil is contaminated with UXO and drainage systems contain contaminating particles (for example, depleted uranium), they affect groundwater quality and, belonging to multiple catchments, go to other watersheds. Therefore, risk assessment and environmental management (land and water) are crucial. Groundwater and surface water contamination are long-term concerns, mainly if we are talking about increasing water radioactivity.

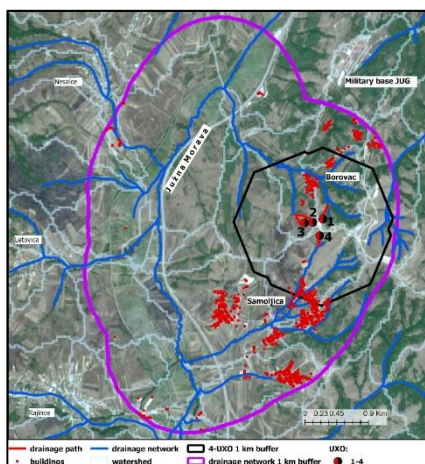


Figure 1 – Research area (source: Sentinel 2 (ESA, 2020) and Google Earth Pro (Google Earth, 2020))
 Рис. 1 – Область обследования (источник: Sentinel 2 (ESA, 2020) и Google Earth Pro (Google Earth, 2020))
 Слика 1 – Подручје истраживања (извор: Sentinel 2 (ESA, 2020) и Google Earth, 2020)

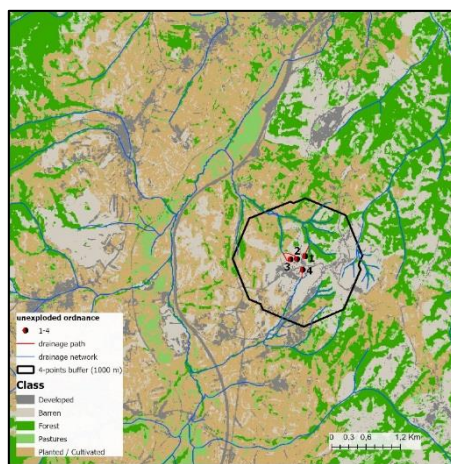


Figure 2 – Land cover of the research area
 Рис. 2 – Земляной покров области обследования
 Слика 2 – Земљишни покривач подручја истраживања

The land cover analysis (Fig. 2) results (Table 5) revealed that planted/cultivated areas dominate the research area, accounting for more than 33% of the total area, followed by forest and barren classes, each accounting for more than 20%. Both the developed class and the pasture class account for less than 10% of the total area (Table 5).

Table 5 – Land cover report for the entire research area
Таблица 5 – Отчет о земляном покрове по всей территории обследования
Табела 5 – Извештај о земљишном покривачу за целокупно подручје истраживања

Class	Pixel Sum	Percentage %	Area (km ²)
1 developed	67094	7.71	6.71
2 barren	183244	21.05	18.32
3 forest	247794	28.47	24.78
4 pastures	79705	9.15	7.97
5 planted/cultivated	292627	33.62	29.26
Total	870464	100	87.05

The classification data's reliability is assessed by calculating the confusion matrix, followed by an overall accuracy and a discrete multivariate technique - Kappa analysis (Congalton & Green, 2019) (Table 6). The forest class is the only one which is 100% accurately classified. All other classes have some misclassifications, which leads to an overall accuracy of 84.28% and a Kappa hat classification of 0.79, which is a substantial result (Table 6).

Table 6 – Confusion matrix (pixel count)
Таблица 6 – Матрица путаницы (количество пикселей)
Табела 6 – Матрица конфузије (број пиксела)

Value\Classified	1	2	3	4	5	Total ground truth points to the class
1 developed	18	1	0	0	2	21
2 barren	2	16	0	0	3	21
3 forest	0	0	20	0	0	20
4 pastures	0	0	0	17	0	17
5 planted/cultivated	0	3	0	3	15	21
Total	20	20	20	20	20	100

Overall accuracy [%] = 84.28 Kappa hat classification = 0.79

All drainage paths belong to the Južna Morava River watershed, a regional drainage network. Therefore, the second performed analysis was to determine the number of buildings within a 1-kilometer 3D distance buffer

zone (19.13 km²) from four UXO locations with drainage paths directly connected to the drainage network (Fig. 1). The total number of 801 buildings is collected in the second analysis in the broader zone of UXO impact.

The third, more focused analysis spans 3.62 km² by encircling a 1-kilometer 3D distance buffer zone around four UXO locations (Figs. 1- 8). The total number of buildings within this 3D distance buffer zone is 168 (Fig. 3).

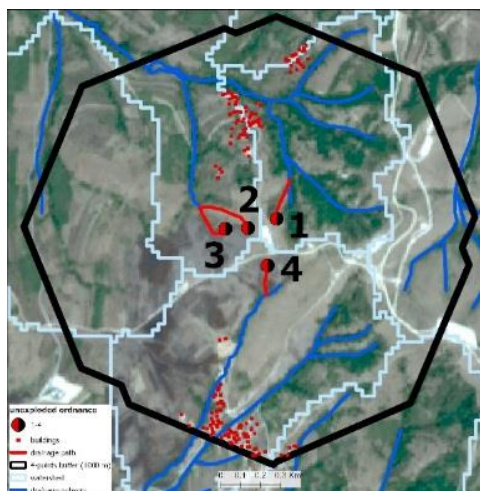


Figure 3 – Four UXO areas with a 1 km buffer zone, source: Sentinel 2 (Copernicus, 2020)

Рис. 3 – Четыре местности под неразорвавшимися боеприпасами с буферной зоной протяженностью 1 км, источник: Sentinel 2 (Copernicus, 2020)

Слика 3 – Четири подручја под неексплодираним убојним средствима са бафер зоном од 1 км (Copernicus, 2020)

The first selected UXO location is within a 1 km 3D distance buffer zone encompassing 79 buildings. The minimum building distance from UXO is 355.44 m, while the maximum distance from UXO is 980.56 m. The mean distance from UXO is 637.26 m (Fig. 4).

The second selected UXO location is within a 1 km 3D distance buffer zone and counts 86 buildings, where the closest one is 309.98 m from UXO. The farthest building is 982.96 m away. The mean building's distance from UXO is 683.89 m (Fig. 5).

The third selected UXO location is within a 1 km 3D distance buffer zone that counts 79 buildings, where the closest one is 258.61 m away from UXO. The farthest building is 978.79 m away. The mean building's distance from UXO is 665.97 m (Fig. 6).

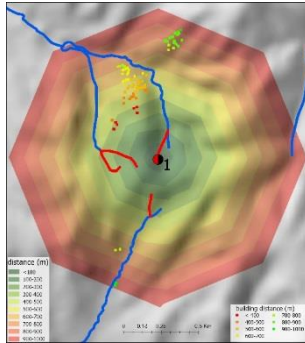


Figure 4 – UXO area 1 with a 1 km buffer zone and buildings within the zone
 Рус. 4 – Местность 1 под неразорвавшимися боеприпасами с буферной зоной протяженностью 1 км и сооружениями внутри зоны
 Слика 4 – Подручје 1 под неексплодираним убојним средствима са бафер зоном од 1 км и објектима унутар зоне

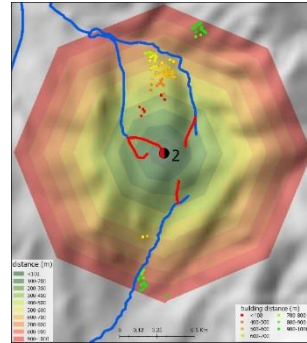


Figure 5 – UXO area 2 with a 1 km buffer zone and buildings within the zone
 Рус. 5 – Местность 2 под неразорвавшимися боеприпасами с буферной зоной протяженностью 1 км и сооружениями внутри зоны
 Слика 5 – Подручје 2 под неексплодираним убојним средствима са бафер зоном од 1 км и објектима унутар зоне

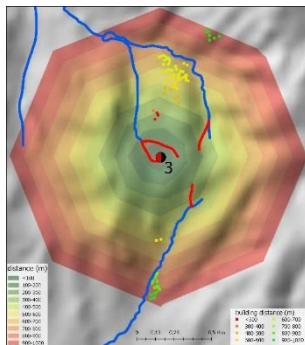


Figure 6 – UXO point 3 with a 1 km buffer zone and buildings within the zone
 Рус. 6 – Местность 3 под неразорвавшимися боеприпасами с буферной зоной протяженностью 1 км и сооружениями внутри зоны
 Слика 6 – Подручје 3 под неексплодираним убојним средствима са бафер зоном од 1 км и објектима унутар зоне

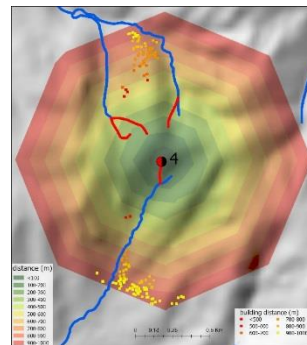


Figure 7 – UXO point 4 with a 1 km buffer zone and buildings within the zone
 Рус. 7 – Местность 4 под неразорвавшимися боеприпасами с буферной зоной протяженностью 1 км и сооружениями внутри зоны
 Слика 7 – Подручје 4 под неексплодираним убојним средствима са бафер зоном од 1 км и објектима унутар зоне

There are 131 buildings in a 1 km 3D distance buffer zone, the closest of which is 469.38 m from UXO in the fourth UXO location. The farthest building is located 996.43 m away. The mean distance between buildings and UXO is 843.24 m (Fig. 7).

The land cover (Fig. 8) report (Table 7) for the area within four UXO 1 km buffer zones reveals that the dominant class in the area is the barren land with 43.5 % area coverage, followed by the planted/cultivated area (~23%) and forests (17.5%).

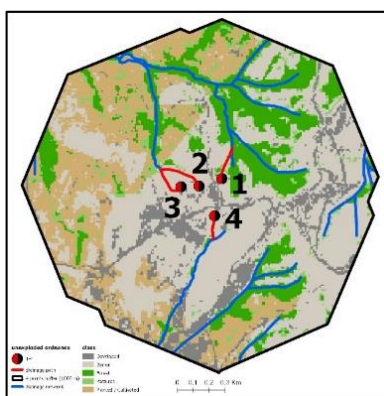


Figure 8 – Land cover of four UXO areas within a 1 km buffer zone
 Рис. 8 – Земляной покров четырех местностей под неразорвавшимися боеприпасами в пределах 1-километровой буферной зоны
 Слика 8 – Земљишни покривач четири подручја под неексплодираним убојним средствима у оквиру бафер зоне од 1 km

Table 7 – Land cover report for four UXO areas within a 1 km buffer zone
 Таблица 7 – Отчет о земляном покрове четырех местностей под неразорвавшимися боеприпасами в пределах 1-километровой буферной зоны
 Табела 7 – Извештај о земљишном покривачу за четири подручја са неексплодираним убојним средствима у оквиру бафер зоне од 1 km

Class	Pixel Sum	Percentage %	Area (km ²)
1 developed	3871	10.69	0.39
2 barren	15765	43.54	1.58
3 forest	6341	17.51	0.63
4 pastures	1900	5.25	0.19
5 planted/cultivated	8328	23.01	0.83
Total	36205	100	3.62

Discussion

The usage of the word UXO is commonly connected with the threats presented by anti-personnel and anti-tank mines set during war events and the deployment of engineering units (Pamučar et al, 2011), as well as the repercussions they cause left behind after armed conflicts. There are generally mine-explosive barrier records with accurate locations for these explosive devices. However, cluster bombs also constitute a significant and genuine hazard. The method they are deployed (dispersion of bomblets from various delivery canisters or missiles) results in a vast scattering zone whose borders are not simple to find and designate. Simultaneously with landing on uneven terrain or owing to the surrounding vegetation, there is an extra dispersion of explosives, further increasing the contaminated area. A variety in their looks (colour) and detonators (which are activated in a specific way), unable their trouble-free clearance /demining. Furthermore, damage to UXO causes the delay of the intended "self-destruction - self-sterilization" thus producing an extension of the period of its destruction capabilities. The preceding section describes the sites where soil decontamination was applied but also indicates the regions where the hazard persists to a considerable degree. Gamma-ray spectrometry techniques have been developed to determine the uranium content of surface samples of the soil contaminated with depleted uranium (Sahoo et al, 2004). This approach may estimate contaminated surface soil samples' natural and depleted uranium content and the depleted uranium activity ratio of $^{235}\text{U}/^{238}\text{U}$ (Vukanac et al, 2010). It would be necessary to do such analyses to improve everyday life of the local population.

Geoecological aspect

The use of depleted uranium is contentious and has been the subject of international discussion (UN Institute for Disarmament Research, 2008). When it comes to contamination and degradation of the environment, it can be said that uranium and depleted uranium are isotopically very similar, chemically radioactive heavy metals that are dangerous to humans in four ways (Fairlie, 2009):

- as a toxic heavy metal,
- as a chemical carcinogen,
- as an endocrine disorder agent, and
- as a carcinogenic radiation agent.

Another difficulty is with bombs, grenades, and projectiles buried in the ground for many years and whose detonators and primary explosive

charges have become "dormant." They can be activated due to an external effect (earthquakes, landslides, excavation of building foundations, increased temperature due to fire, etc.). In addition to fatal consequences for the population (as the most significant loss), there are long-term psychological consequences for the people, water pollution, disabling of water and electricity supply installations, damage to road infrastructure, damage to health systems, and significant economic consequences.

After conducting a multi-criteria study of the described area, it was determined that in addition to the cultivated land cover (33 % - Fig. 2, Table 5), this area contains 21.05 % of the total infertile land. The barren soil is essentially the most contaminated. In the 18.32 km² area, there is an enhanced danger to human life and health. Such locations are appropriately referred to as zones of low security. The same is typical for forest-covered places (28.46 %). In this part of Serbia, the population depends on exploiting wood mass, so the existing danger of UXO endangers their primary economic activity. The removal of UXO is complicated in the forest area due to the area relief, lack of visibility, and other obstacles. Pastures cover only 7.97 km², but it is not an immeasurable area where cattle and people can be endangered as well as other wild animals that live or feed there. Additionally, pastures are crucial regions for honey production, medicinal plants harvesting, and more. Increased radioactivity in these locations has a direct effect on human health degradation.

Following the confirmation that ammunition containing U-236 with depleted uranium (DU) was used during the NATO air campaign in Serbia in 1999, concern was expressed about the possibility that other nuclides from the nuclear fuel cycle, especially transuranium nuclides, could be present with this type of ammunition. Numerous tests have been performed, and many papers have been published. For example, in an article entitled "Actinide Analysis of a Depleted Uranium Penetrator from a 1999 Target Site in Southern Serbia," published in the Journal of Environmental Radioactivity (2003), McLaughlin et al published the results of the analyses of uranium and plutonium from the target location in southern Serbia (McLaughlin et al, 2003). The results of that and many other works confirmed the presence of trace plutonium in the penetrator, the highest concentration of plutonium ever reported in the Balkans.

After military operations, most UXO (or their fragments) containing depleted uranium remained underground in specific geomorphological and geochemical environments exposed to local climatic conditions. The distribution, mobility, and/or fixing of depleted uranium in the contaminated soil varied according to the geological and pedological surroundings, vegetation type, and climatic factors. Corrosion products of depleted

uranium and other contaminating particles associated with UXO fluctuate over time depending on the extent of their geochemical fractionation. It is an assumption that has been validated in several studies. At around 150 mm from the source, the concentration of depleted uranium decreases to 1% of its original value (Radenković et al, 2008).

Moreover, the danger of UXO activation varies by season and during dry and rainy periods. The ability to transfer contaminated material over various environmental mediums signals an infinite hazard to the living world. Human epidemiological research has shown that exposure to low and moderate radon concentrations may cause up to 14% of malignant tumours. Due to the radiation in the soil, animals living in subterranean cavities are exposed to more significant amounts. Over the years, numerous dose-effect models have been created to evaluate the dangers to individuals and the environment (Ćujić et al, 2021).

Studies of the mobility and geo-fractionation of depleted uranium in the soil have shown that depleted uranium may be very mobile under substantial contamination conditions and intensive ion exchange with the environment. Furthermore, as previously mentioned in the study, the decomposition rate is also soil-dependent, mainly for Fe and Mn oxides and carbonate substrates in the soil (Popovic et al, 2008).

In the past few decades, the southern part of Central Serbia has undergone significant ecological changes, including depopulation as a social factor (Potić et al, 2022), where the natural process of ecological revitalization due to population ageing and emigration is taking place, and forest areas are expanding. Due to the growth and spread of vegetation on uncultivated surfaces, it will become more challenging to clean and remediate that area over time (Mihajlović et al, 2014).

Risk management of unexploded ordnance

One risk assessment method is insufficient for UXO locations. The UXO risk assessment procedure requires creating civil-military collaboration to develop alternative approaches. The initial step might be prioritizing UXO cleanup areas. This data type is beneficial for allocating financial and non-financial resources, such as equipment and personnel. A full description or geoecological investigation of UXO-contaminated regions would be the second stage in risk assessment (risk assessment for specific locations). With this approach, quantifiable data on the possible harm to individuals living around the UXO location (as shown in Figs. 1 - 8) and local ecosystems may be supplied.

Location data is often unavailable and wildly inaccurate. Using remote sensing allows the creation of at least a rough database with the most

endangered locations. However, detailed information is necessary for data collection to establish UXO risk management correctly. Two sources of risk at UXO sites must also be considered: the risk of explosion and environmental contamination from ammunition components flushed into water and soil. These two types of threats are significantly different. The first leads to immediate consequences for a man or his material environment; in contrast, the consequences of permanent exposure to ammunition are chronic impairment of the quality of life.

The presence of 33% arable land (Table 5) indicated significant agricultural activity and increased people's mobility and daily activities in the vicinity of UXO. According to the 2011 census, this region had 166 people living in 44 homes. Such a demographic distribution would suggest an equal number of potential UXO victims.

At only four notable locations where the Serbian Center for Demining confirmed the presence of UXO, there are 801 built structures: houses, shops, schools, food storage facilities, warehouses, garages with mechanization for agricultural surface processing, and fuel depots, among others. Without security measures over an extended period, it is logical to presume that this area poses an enhanced security risk. Given the unknown and unexpected composition of UXO, the threats to the environment, groundwater and surface water, soil, and air, and the long-term impacts on living organisms' DNA, it is deemed essential to affirm environmental risk management.

Risk assessment methods can define the level of danger to people, property, and the environment in an area and establish priorities and courses of action. It is necessary to determine the factors and levels of risk to develop a UXO risk management system. Such a system would provide a strategic advantage over the area's level of vulnerability. Specifically, applying various (physical, educational, economic, etc.) measures would lower the risk of endangering people, property, and the environment. This claim is supported by the fact that the problem of UXO has the characteristics of a "long shadow" of a crisis, i.e., a problem arises quickly, while its consequences remain for a long time in the future. Therefore, developing an adequate methodology for risk assessment and a risk management strategy in this area is paramount.

Conclusion

Besides unexploded ordnance left behind after the 1999 bombing campaign on the territory of former Yugoslavia, there is also UXO left from World Wars I and II and still buried in the ground. The data on the mentioned

amounts is not accessible except in the circumstances encountered during particular land excavation works. Afterwards, the problem of UXO intensifies, but it does not move away from stating the problem and demanding that it be solved. The frequent reference to UXO in the ground inadvertently covers the issues of our waterways which are also contaminated with unexploded ammunition. Contamination levels considerably impact planning and decision making when choosing safe locations for crossing an area while undertaking different activities (Bozanic et al, 2018).

Combining physical and chemical procedures and analyses may help decision making on the cleanup plan for depleted uranium-contaminated military sites. It is vital to consider establishing radioactive monitoring in such a location and others where UXO is an issue. Such surveillance must be genuine, radiological surveillance must be reasonably valid, and unprofessional groups or people cannot conduct it. In Serbia, such monitoring is undertaken by the Department of Radiation and Environmental Protection of the Institute of Nuclear Sciences in Vinča, Belgrade (Krneta Nikolić et al, 2014).

The article contributes significantly to creating a strategy for environmental risk management in regions contaminated by UXO. The paper provides an example of an effective technique for resolving risk assessment issues experienced by the Army in UXO locations. Not only does it present a suitable risk analysis, but it also considers numerous environmental protection possibilities. It is feasible to calculate the number of structures and people, soil kinds, plant types, and others exposed to UXO dangers based on the key spots using the multi-criteria analysis and the GIS. This paper is one of the guidelines for environmental risk assessment.

Since the UXO issue in the observed region has not been resolved for the last two decades and based on the findings of this paper's analyses, it can be stated that the UXO problem in this area will persist and continue to threaten the safety of people and property. Consequently, establishing a UXO risk management plan and a methodology for risk assessment following strategic guidelines is paramount. The findings of this paper's analyses unequivocally reveal the level of risk to people, property, and the environment with a detrimental long-term effect on this region. Appropriate risk assessment and UXO risk management would contribute to slowing down the UXO detrimental consequences in all aspects.

Future studies should identify the criteria for zoning UXO-contaminated regions based on threats to people, property, and the environment. The findings of the analyses presented in this article may be used as a foundation for establishing the criteria and methodology and then estimating

the danger of UXO. According to the same approach, it is conceivable to do comparable analyses for other areas and the whole territory of the Republic of Serbia, therefore resolving the issue of UXO risk management and laying the groundwork for more effective protection of people's property and the environment.

References

- Australian Government, Defence. 2020. *Unexploded Ordnance (UXO) in Australia* [online]. Available at: <https://uxo.defence.gov.au/> [Accessed: 20 May 2023].
- Bozanic, D., Tešić, D. & Milićević, J. 2018. A hybrid fuzzy AHP-MABAC model: Application in the Serbian Army – The selection of the location for deep wading as a technique of crossing the river by tanks. *Decision Making: Applications in Management and Engineering*, 1(1), pp.143-164 [online]. Available at: <https://dmame-journal.org/index.php/dmame/article/view/2> [Accessed: 20 May 2023].
- Cauderay, G.C. 1993. Anti-Personnel Mines. *International Review of the Red Cross*, 33(295), pp.273-287. Available at: <https://doi.org/10.1017/S0020860400080530>.
- Congalton, R.G. & Green, K. 2019. *Assessing the Accuracy of Remotely Sensed Data: Principles and Practices, Third Edition*. Boca Raton: CRC Press. Available at: <https://doi.org/10.1201/9780429052729>.
- Congedo, L. 2021. Semi-Automatic Classification Plugin: A Python tool for the download and processing of remote sensing images in QGIS. *The Journal of Open Source Software*, 6(64), art.number:3172. Available at: <https://doi.org/10.21105/joss.03172>.
- Copernicus. 2020. *Copernicus Open Access Hub* [online]. Available at: <https://scihub.copernicus.eu/> [Accessed: 20 May 2023].
- Čujić, M., Janković Mandić, Lj., Petrović, J., Dragović, R., Đorđević, M., Đokić, M. & Dragović, S. 2021. Radon-222: environmental behavior and impact to (human and non-human) biota. *International Journal of Biometeorology*, 65, pp.69-83. Available at: <https://doi.org/10.1007/s00484-020-01860-w>.
- Duro, D.C., Franklin, S.E. & Dubé, M.G. 2012. A comparison of pixel-based and object-based image analysis with selected machine learning algorithms for the classification of agricultural landscapes using SPOT-5 HRG imagery. *Remote Sensing of Environment*, 118, pp.259-272. Available at: <https://doi.org/10.1016/j.rse.2011.11.020>.
- Eorc.Jaxa. 2019. *Precise Global Digital 3D Map "ALOS World 3D"* [online]. Available at: https://www.eorc.jaxa.jp/ALOS/en/dataset/aw3d_e.htm [Accessed: 20 May 2023].
- Fairlie, I. 2009. Depleted uranium: properties, military use and health risks. *Medicine, Conflict and Survival*, 25(1), pp.41-64. Available at: <https://doi.org/10.1080/13623690802568962>.

- Google Earth. 2020. *Geospatial Solutions: Google Earth Pro 7.3.3.7786* [online]. Available at: <https://www.google.com/earth/versions/> [Accessed: 20 May 2023].
- Government of Canada. 2021. *What is Unexploded Explosive Ordnance (UXO)?* [online]. Available at: <https://www.canada.ca/en/department-national-defence/services/uxo/what-is-uxo.html> [Accessed: 20 May 2023].
- Karasiak, N. 2016. lennepkade/dzetsaka: Fix bug in processing provider with vector files. *Zenodo.org*. Available at: <https://doi.org/10.5281/zenodo.2552284>.
- Krneta Nikolić, J.D., Todorović, D.J., Janković, M.M., Pantelić, G.K. & Rajačić, M.M. 2014. Quality assurance and quality control in environmental radioactivity monitoring. *Quality Assurance and Safety of Crops and Foods*, 6(4), pp.403-409. Available at: <https://doi.org/10.3920/QAS2012.0.236>.
- Landmine Action. 2002. *Summary: Explosive remnants of war, Unexploded ordnance and postconflict communities* [online]. Available at: http://www.cpeo.org/pubs/UXOreport_3_26.pdf (Accessed: 25 November 2022).
- Martin, M.F., Dolven, B., Feickert, A. & Lum, T. 2019. War Legacy Issues in Southeast Asia: Unexploded Ordnance (UXO). *Congressional Research Service* [online]. Available at: <https://sgp.fas.org/crs/weapons/R45749.pdf> [Accessed: 20 May 2023].
- Mas, J.F. & Flores, J.J. 2008. The application of artificial neural networks to the analysis of remotely sensed data. *International Journal of Remote Sensing*, 29(3), pp.617-663. Available at: <https://doi.org/10.1080/01431160701352154>.
- McLaughlin, J.P., Vintró, L.L., Smith, K.J., Mitchell, P.I. & Žunić, Z.S. 2003. Actinide analysis of a depleted uranium penetrator from a 1999 target site in southern Serbia. *Journal of Environmental Radioactivity*, 64(2-3), pp.155-165. Available at: [https://doi.org/10.1016/S0265-931X\(02\)00046-2](https://doi.org/10.1016/S0265-931X(02)00046-2).
- Mihajlović, Lj., Komazec, N., Milinčić, M., Mihajlović, B. & Đorđević, T. 2014. Prevention of Environmental Migration Using GIS as a Research Method. In: Trajanović, M. & Stanković, M. (Eds.) *6th International ICT Conference, Proceedings*, Niš, Serbia, pp.60-63, October 14-16 [online]. Available at: https://www.academia.edu/10518758/Proceedings_of_6th_International_ICT_Conference [Accessed: 20 May 2023]. ISBN: 978-86-80593-52-4.
- Orlić, M. 2000. Depleted uranium as a product of nuclear technology. In: *XLIV ETRAN Conference*, Sokobanja, Serbia, pp.35-42, June 26-29 [online]. Available at: [https://www.etrans.rs/common/archive/ETLAN_1955-2006/ET\(R\)AN_1955-2006/eTRAN/44.ETLAN.2000.4/Orlic.M.ETLAN.2000.4.pdf](https://www.etrans.rs/common/archive/ETLAN_1955-2006/ET(R)AN_1955-2006/eTRAN/44.ETLAN.2000.4/Orlic.M.ETLAN.2000.4.pdf) (in Serbian) [Accessed: 20 May 2023].
- Pamućar, D., Božanić, D., Đorović, B. & Milić, A. 2011. Modelling of the fuzzy logical system for offering support in making decisions within the engineering units of the Serbian Army. *International Journal of Physical Sciences*, 6(3), pp.592-609 [online]. Available at: <https://academicjournals.org/journal/IJPS/article-abstract/139CC9428354> [Accessed: 20 May 2023].
- Plackett, RL 1976. *Reviewed Work: Discrete Multivariate Analysis: Theory and Practice*. by Yvonne M.M. Bishop, Stephen E. Fienberg, Paul W. Holland.

Journal of the Royal Statistical Society. Series A (General), 139(3), pp.402-403. Available at: <https://doi.org/10.2307/2344845>.

Popovic, D., Todorovic, D., Frontasyeva, M., Ajtic, J., Tasic, M. & Rajsic, S. 2008. Radionuclides and heavy metals in Borovac, Southern Serbia. *Environmental Science and Pollution Research*, 15(6), pp.509-520. Available at: <https://doi.org/10.1007/s11356-008-0003-6>.

Potić, I.M., Čurčić, N.B., Potić, M.M., Radovanović, M.M. & Tretiakova, T.N. 2017. Remote sensing role in environmental stress analysis: East Serbia wildfires case study (2007-2017). *Journal of the Geographical Institute "Jovan Cvijic" SASA*, 67(3), pp.249-264. Available at: <https://doi.org/10.2298/ijgi1703249p>.

Potić, I., Mihajlović, Lj.M., Šimunić, V., Čurčić, N.B. & Milinčić, M. 2022. Deforestation as a Cause of Increased Surface Runoff in the Catchment: Remote Sensing and SWAT Approach—A Case Study of Southern Serbia. *Frontiers in Environmental Science*, 10(June), art.number: 896404. Available at: <https://doi.org/10.3389/fenvs.2022.896404>.

Potić, I. & Potić, M. 2017. Remote sensing machine learning algorithms in environmental stress detection: Case study of Pan-European south section of Corridor 10 in Serbia. *The University Thought - Publication in Natural Sciences*, 7(2), pp.41-46. Available at: <https://doi.org/10.5937/univtho7-14957>.

-QGIS. 2022. *QGIS A Free and Open Source Geographic Information System* [online]. Available at: <https://www.qgis.org/en/site/forusers/download.html> [Accessed: 20 May 2023].

Radenković, M.B., Cupać, S.A., Joksić, J.D. & Todorović, D.J. 2008. Depleted uranium mobility and fractionation in contaminated soil (Southern Serbia). *Environmental Science and Pollution Research*, 15(1), pp.61-67. Available at: <https://doi.org/10.1065/espr2007.03.399>.

Regodić, M. 2008. Remote sensing as a method of space data acquisition. *Vojnotehnički glasnik/Military Technical Courier*, 56(1), pp.91-112 (in Serbian). Available at: <https://doi.org/10.5937/vojtehg0801091R>.

-Republika Srbija, Centar za Razminiranje. 2022. *Minska situacija: MINSKA SITUACIJA NOVEMBAR 2022*. [online]. Available at: <https://www.czrs.gov.rs/lat/minska-situacija.php> [Accessed: 10 November 2022].

-Republika Srbija, Republički zavod za statistiku. 2023. *Popis stanovništva, domaćinstava i stanova, Popis 2011, Popisni podaci - eksel tabele* [online]. Available at: <https://www.stat.gov.rs/sr-Latn/oblasti/popis/popis-2011/popisni-podaci-eksel-tabele> (in Serbian) [Accessed: 20 May 2023].

Sahoo, S.K., Fujimoto, K., Čeliković, I., Ujić, P. & Žunić, Z.S. 2004. Distribution of uranium, thorium, and isotopic composition of uranium in soil samples of south Serbia: Evidence of depleted uranium. *Nuclear Technology and Radiation Protection*, 19(1), pp.26-30. Available at: <https://doi.org/10.2298/NTRP0401026S>.

Salomonson, V.V. 2014. Remote Sensing, Historical Perspective. In: Njoku, EG (Eds) *Encyclopedia of Remote Sensing. Encyclopedia of Earth Sciences Series*, pp.684-691. New York, NY: Springer. Available at: https://doi.org/10.1007/978-0-387-36699-9_158.

Tadono, T., Nagai, H., Ishida, H., Oda, F., Naito, S., Minakawa, K. & Iwamoto, H. 2016. Generation of the 30 M-MESH global digital surface model by alos prism. In: *XXIII ISPRS Congress: The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLI-B4*, Prague, Czech Republic, July 12-19. Available at: <https://doi.org/10.5194/isprsarchives-XLI-B4-157-2016>.

Tarboton, D.G., Dash, P. & Sazib, N. 2015. *TauDEM 5.3: Guide to using the TauDEM command line functions 2015*. Logan: Utah State University [online]. Available at: <https://hydrology.usu.edu/taudem/taudem5/TauDEM53CommandLineGuide.pdf> [Accessed: 20 May 2023].

-The Geneva International Centre for Humanitarian Demining (GICHD). 2019. *Explosive ordnance: Types of explosive ordnance* [online]. Available at: <https://www.gichd.org/en/explosive-ordnance/> [Accessed: 20 May 2023].

-UN Institute for Disarmament Research. 2008. *Disarmament forum. 2008/1 = Forum du désarmement. 2008/1*. Geneva: UN Institute for Disarmament Research [online]. Available at: <http://digitallibrary.un.org/record/633351>. ISBN/ISSN: 1020-7287.

Vukanac, I., Novković, D., Kandić, A., Djurašević, M. & Milošević, Z. 2010. A simple method for determination of natural and depleted uranium in surface soil samples. *Applied Radiation and Isotopes*, 68(7-8), pp.1433-1434. Available at: <https://doi.org/10.1016/j.apradiso.2009.11.056>.

Управление рисками, связанными с неразорвавшимися боеприпасами, в Республике Сербия в целях защиты окружающей среды – исследование случая Боровац

Иван М. Потич^а, Ненад М. Комазец^б, Лиляна М. Михайлович^в, Александр М. Милич^б, Саша Т. Бакрач^а

^а Военно-географический институт имени генерала Стевана Бошковица, г. Белград, Республика Сербия

^б Университет обороны в г. Белград, Военная академия, г. Белград, Республика Сербия

^в Белградский университет, географический факультет, г. Белград, Республика Сербия, **корресподент**

РУБРИКА ГРНТИ: 81.93.03 Методология оценки вероятности аварий, катастроф, стихийных бедствий и их последствий. Оценка риска, 34.35.51 Антропогенные воздействия на экосистемы, 20.23.25 Информационные системы с базами знаний.

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: После нескольких десятилетий борьбы с неразорвавшимися боеприпасами (НРБ) в некоторых районах Республики Сербия обнаружено, что они все еще представляют значительную опасность для населения, имущества и окружающей среды. Несмотря на то, что местность была разминирована, все еще стоит серьезная угроза от труднодоступных частей неразорвавшихся боеприпасов. Несоответствующие системные решения в управлении неразорвавшимися боеприпасами могут повлечь за собой серьезные негативные последствия.

Методы: В данной статье изучается воздействие частей НРБ на население и окружающую среду на основании анализа пространственного распределения различных видов и количества НРБ. Были проведены два различных геопропространственных анализа, а также разработаны рекомендации по управлению рисками с помощью многокритериального устранения рисков, анализа ГИС и дистанционного зондирования.

Результаты: Было проведено два различных геопропространственных анализа, в результате которых осуществлена классификация территории с высоким риском от неразорвавшихся боеприпасов.

Выводы: Данная статья вносит значительный вклад в создание стратегии управления экологическими рисками на местности, загрязненной неразорвавшимися боеприпасами. Такой тип стратегии является эффективным методом для решения проблемы оценки риска на местности с неразорвавшимися боеприпасами. В статье также обсуждается анализ рисков и меры по охране окружающей среды. С помощью многокритериального анализа и ГИС оценивается степень риска для населения, имущества, типов почвы и растительности от воздействия НРБ. Данная статья представляет собой руководство по оценке экологических рисков.

Ключевые слова: Неразорвавшиеся боеприпасы, управление рисками в кризисных ситуациях, охрана окружающей среды, безопасность, геопропространственный анализ.

Управљање ризиком од неексплодираних убојних средстава у Републици Србији у функцији заштите животне средине – студија случаја Боровац

Иван М. Потих^а, Ненад М. Комазец^б, Љиљана М. Михајловић^в,
Александар М. Милић^б, Саша Т. Бакрач^а

^а Војногеографски институт „Генерал Стеван Бошковић”,
Београд, Република Србија

^б Универзитет одбране у Београду, Војна академија,
Београд, Република Србија

^в Универзитет у Београду, Географски факултет,
Београд, Република Србија, **аутор за преписку**

ОБЛАСТ: географски информациони системи,
менаџмент животне средине, управљање ризицима
КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: После вишедеценијског решавања проблема са неексплодираним убојним средствима у неким областима Републике Србије, она још увек представљају знатан ризик по безбедност људи, имовине и животне средине. Иако је терен знатно очишћен, постоје озбиљне претње од компоненти које се тешко проналазе. Неадекватна системска решења за управљање овим средствима могу изазивати веома велике последице.

Методе: На основу анализе просторне дистрибуције различитих типова и количина неексплодираних убојних средстава, у чланку се проучавају ефекти ових компоненти на људске животе и животну средину. Извршене су две различите геопросторне анализе, а укључене су и смернице за управљање ризиком путем елиминације ризика на основу више критеријума, ГИС анализа и даљинске детекције.

Резултати: Две различите геопросторне анализе резултирале су класификацијом области које су под високим ризиком од преосталих неексплодираних убојних средстава.

Закључак: Чланак значајно доприноси стварању стратегије управљања еколошким ризицима у регионима контаминираним неексплодираним убојним средствима. Она представља ефикасну технику за решавање изазова процене ризика на тим просторима. У раду се разматрају и анализа ризика и опције заштите животне средине. Користећи вишекритеријумску анализу и ГИС, процењује се изложеност структуре, људи, врста земљишта и биљних врста опасностима које неексплодирана убојна средства изазивају на кључним локацијама. Овај рад служи као смерница за процену еколошког ризика.

Кључне речи: неексплодирана убојна средства, менаџмент кризних ситуација, заштита животне средине, сигурност, геопросторна анализа.

Paper received on / Дата получения работы / Датум пријема чланка: 24.05.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 30.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 01.12.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



ПРЕГЛЕДНИ РАДОВИ

ОБЗОРНЫЕ СТАТЬИ

REVIEW PAPERS

Collective phenomena

Nicola Fabiano

University of Belgrade, “Vinča” Institute of Nuclear Sciences - National Institute of the Republic of Serbia, Belgrade, Republic of Serbia,
e-mail: nicola.fabiano@gmail.com,
ORCID iD: <https://orcid.org/0000-0003-1645-2071>

DOI: 10.5937/vojtehg71-42540;<https://doi.org/10.5937/vojtehg71-42540>

FIELD: solid state physics, statistical physics

ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: Quantum field theory techniques are able to describe precisely, inter alia, collective phenomena of statistical and solid state physics.

Method: The path integral method with a Wick rotation shows its complete analogy with the partition function of statistical mechanics.

Results: The Landau–Ginzburg phenomenology successfully describes collective phenomena such as spontaneous magnetization and superconductivity.

Conclusions: Symmetry breaking phenomena could give macroscopic results.

Key words: vacuum energy, symmetry breaking, Landau–Ginzburg model.

Collective phenomena

The techniques we have met so far (Fabiano, 2021a,b, 2022) are not connected exclusively to the field theory. For instance the Anderson–Higgs–Brout–Englert–Guralnik–Hagen–Kibble phenomenon (Anderson, 1963; Higgs, 1964a,b; Englert & Brout, 1964; Guralnik et al., 1964) was mutated essentially from solid state physics. A deeper understanding of physical meaning of the renormalisation group was given by Kadanoff’s proposal of block spin renormalisation (Kadanoff, 1966), and Wilson’s approach to critical phenomena (Wilson, 1971a,b). Physics does not operate through airlocks.

Path integral versus the partition function

We have already introduced the partition function in (Fabiano, 2022) eq. (28) for a scalar field. Recall that in D dimensions

$$Z = \int \mathcal{D}\phi e^{(i/\hbar) \int d^D x [\frac{1}{2}(\partial\phi)^2 - V(\phi)]} . \quad (1)$$

By means of a Wick rotation, we write $d^D x = -i d_E^D x$, where $d_E^D x = dt_E d^{(D-1)}x$, and $(\partial\phi)^2 = (\partial\phi/\partial t)^2 - (\vec{\nabla}\phi)^2$ becomes $(\partial\phi)^2 = (\partial\phi/\partial t_E)^2 + (\vec{\nabla}\phi)^2$, which is the energy operator $E(\phi)$, positive definite, so we obtain the Euclidean version of the path integral

$$Z_E = \int \mathcal{D}\phi e^{(i/\hbar) \int d_E^D x [\frac{1}{2}(\partial\phi)^2 + V(\phi)]} = \int \mathcal{D}\phi e^{-(1/\hbar)E(\phi)} . \quad (2)$$

The Euclidean version (2) we have obtained closely resembles the known expression of statistical mechanics. Indeed, making the substitution $\hbar \leftrightarrow kT \equiv 1/\beta$, the probability of a statistical state is proportional to the Boltzmann factor $e^{-\beta E}$, where E is the classical energy of the state. For a system of N particles, classical energy is given by

$$E(p, q) = \sum_{i=1}^N \frac{p_i^2}{2m_i} + V(q_1, q_2, \dots, q_N) , \quad (3)$$

and the corresponding partition function is proportional to

$$Z = \prod_{i=1}^N \int dp_i dq_i e^{-\beta E(p, q)} . \quad (4)$$

The kinetic term of energy is known so the integral over p can be explicitly done, and we are left with the (reduced) partition function

$$Z = \prod_{i=1}^N \left(\frac{2m_i\pi}{\beta} \right)^{N/2} \int dq_i e^{-\beta V(q_1, q_2, \dots, q_N)} . \quad (5)$$

Going to the continuum limit as we did in (Fabiano, 2022) eq. (24), by promoting $i \rightarrow x$ and $q_i \rightarrow \phi(x)$ we reobtain the expression found in eq. (2).

We show below a translation table among languages of the field theory in Minkowski space and statistical mechanics, both D dimensional:

Table 1 – Translation table of the field theory and statistical mechanics
 Таблица 1 – Таблица перевода теории поля и статистической механики
 Табела 1 – Табела преводжења теорије поља и статистичке механике

Field theory	↔	Statistical mechanics
x_0	↔	ix_0
$d^D x$	↔	$-id^D x$
$(\partial\phi/\partial t)^2 - (\vec{\nabla}\phi)^2$	↔	$(\partial\phi/\partial t)^2 + (\vec{\nabla}\phi)^2$
\hbar	↔	$\beta \equiv 1/(kT)$

Landau–Ginzburg phenomenology

We consider magnetization. Let us briefly review the Goldstone mechanism (Goldstone, 1961) of symmetry breaking, where there is the complex field $\phi \equiv (\phi_1 + i\phi_2)/\sqrt{2}$ in the Lagrangian

$$\mathcal{L} = \partial\phi^\dagger\partial\phi + \mu^2(\phi^\dagger\phi) - \lambda(\phi^\dagger\phi)^2, \quad (6)$$

as the mass term has the wrong sign, we are already in a broken symmetry phase. In Fig. 1, the potential is described by eq. (6). It is clear that it is invariant under rotations, that is invariant under the global $U(1)$ transformation $\phi \rightarrow e^{i\alpha}\phi$ because the groups $SO(2)$ and $U(1)$ are isomorphic. We could rewrite eq. (6) in the polar coordinates by $\phi(x) = \rho(x)e^{i\theta(x)}$, so that $\partial_\mu\phi = (\partial_\mu\rho + i\rho\partial_\mu\theta)e^{i\theta(x)}$, finally obtaining

$$\mathcal{L} = \rho^2(\partial\theta)^2 + (\partial\rho)^2 + \mu^2\rho^2 - \lambda\rho^4. \quad (7)$$

In the broken phase, we have

$$v = +\sqrt{\frac{\mu^2}{2\lambda}} \quad (8)$$

and putting $\rho = v + \chi$ we end up with the Lagrangian

$$\begin{aligned} \mathcal{L} = v^2(\partial\theta)^2 + & \left[(\partial\chi)^2 - 2\mu^2\chi^2 - 4\sqrt{\frac{\mu^2\lambda}{2}}\chi^3 - \lambda\chi^4 \right] \\ & + \left(\sqrt{\frac{2\mu^2}{\lambda}}\chi + \chi^2 \right) (\partial\theta)^2, \end{aligned} \quad (9)$$

where one recognizes $\theta(x)$ as the massless Goldstone field.

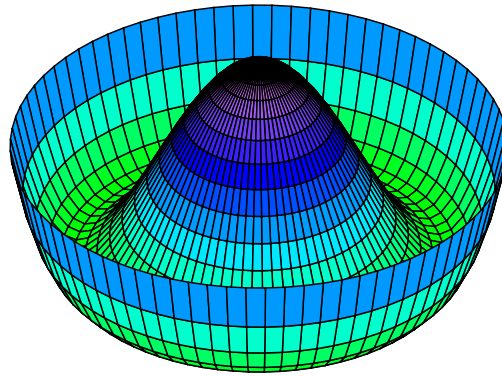


Figure 1 – Complex field potential in the broken symmetry phase
 Рис. 1 – Комплексный потенциал поля в фазе нарушенной симметрии
 Слика 1 – Потенцијал комплексног поља у фази нарушене симетрије

Consider a ferromagnetic material in the thermal equilibrium at the temperature T . Define the magnetization $\vec{M}(x)$ as the average of atomic magnetic momenta over a region much larger than the relevant microscopic scale.

When the temperature T is high enough, the magnetization vectors should be expected to point out at random, as there is not a preferred direction because of spatial isotropy. The magnetization vector average should add up to zero. However, lowering the temperature under a critical value T_c shows experimentally that the behaviour of magnetism changes in the following manner

$$|\vec{M}| \propto (T_c - T)^\beta, \quad (10)$$

where it is experimentally found that β (here a critical exponent, not to be confused with the inverse of the temperature) covers the range of 0.3–0.38 for different materials.

In order to explain this behavior, Landau and Ginzburg (Ginzburg & Landau, 2009) made the hypothesis that the thermodynamic properties of the system should be derivable from a free energy G which is an analytic function of the magnetism $M = |\vec{M}|$ and the temperature T . Then the magnetic field H would be given by

$$H = \frac{\partial}{\partial M} G(M, T). \quad (11)$$

Near T_c where M is small we can write a Taylor series in the powers of M for the free energy G

$$G(M, T) = G_c(T) + a(T)M^2 + b(T)M^4 + \mathcal{O}(M^6), \quad (12)$$

we include only even powers of M because of rotational symmetry and spin-up-down symmetry. The magnetic field is therefore given by

$$H = 2a(T)M + 4b(T)M^3 + \mathcal{O}(M^5). \quad (13)$$

At this point, the similarity of the free energy in eq. (12) and the potential of Lagrangian (6) is evident. We are left with two possible phenomena. If $a > 0$, then G will have a single minimum at M_0 (we could assume its value is zero by symmetry) as shown in Fig. 2a, but if $a < 0$ then G shows two symmetric minima around the origin, at the points $\pm M_0$, corresponding to $H = 0$, as in Fig. 2b. The system will choose a state of the minimum free energy which according to Fig. 2b corresponds to a state of non-vanishing magnetization. It is clear that the possibility $a > 0$ corresponds to $T > T_c$, where spontaneous magnetization is zero, while $a < 0$ means $T < T_c$.

Continuing with these analyticity assumptions, we can obtain some of the critical exponents. It is clear that $a(T_c) = 0$ while $b(T_c)$ will have a nonzero value. The next stage is assuming a linear behaviour for a in the vicinity of T_c ,

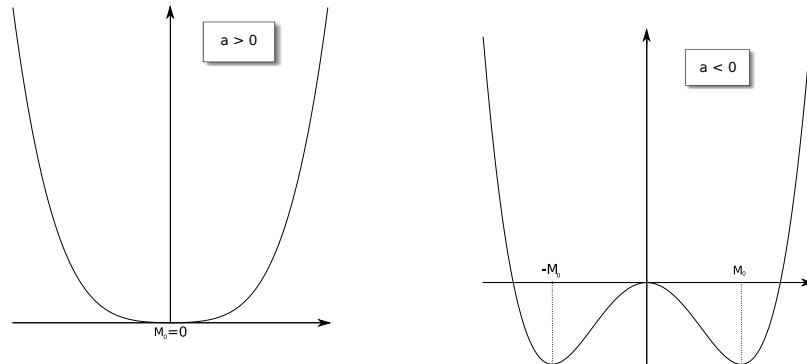
$$a(T) \propto (T_c - T). \quad (14)$$

Then, for $a < 0$ from eqs. (12) and (8), we have

$$M = \sqrt{-\frac{a(T)}{2b(T)}} \propto (T_c - T)^{1/2}, \quad (15)$$

for which we identify

$$\beta = \frac{1}{2} \quad (16)$$



- (a) *Unbroken symmetry, $a > 0$ and $M_0 = 0$*
 (a) *Непрерывная симметрия, $a > 0$ и $M_0 = 0$*
 (a) *Ненарушена симетрија, $a > 0$ и $M_0 = 0$*
- (b) *Broken symmetry, $a < 0$ and $M_0 > 0$*
 (б) *Нарушенная симметрия, $a < 0$ и $M_0 > 0$*
 (б) *Нарушена симетрија, $a < 0$ и $M_0 > 0$*

Figure 2 – Free energy G versus magnetization M

Рис. 2 – Свободная энергия G по сравнению с намагниченностью M

Слика 2 – Слободна енергија G наспрам магнетизације M

as the first critical exponent. If $T > T_c$, then near zero magnetization from (13) we have

$$M = \frac{H}{2a(T)}, \quad (17)$$

and defining the magnetic susceptibility as

$$\chi \equiv \left. \frac{\partial M}{\partial H} \right|_{H=0} \quad (18)$$

with the critical exponent γ such that $\chi \propto (T - T_c)^{-\gamma}$, we calculate

$$\chi = \frac{1}{2a(T)} \propto (T - T_c)^{-1} \quad (19)$$

obtaining another critical exponent, $\gamma = 1$.

This approach of the *mean field* does not give very accurate values for critical exponents, but provides a very simple picture of critical behaviour.

Landau and Ginzburg considered the possibility that \vec{M} depends on a position (here the space is three dimensional, we consider only non rela-

tivistic effects), then G could be written as

$$G = \int d^3x [\partial_i \vec{M} \partial_i \vec{M} + a \vec{M}^2 + b(\vec{M}^2)^2 + \dots]. \quad (20)$$

Again, this expression is in complete analogy with eq. (6), where a plays the role of a square mass and b is a coupling constant. So the length scale is determined by $1/\sqrt{a}$. For $T > T_c$ add a magnetic field $\vec{H}(x)$ that interacts with the magnetization with the term $-\vec{H} \cdot \vec{M}$ (observe the similarity with the source function in (Fabiano, 2022) eq. (35)). Assuming M is small and minimizing G , we obtain at the first order $(-\partial^2 + a)\vec{M} \propto \vec{H}$ with the solution

$$\begin{aligned} \vec{M}(x) &= \int d^3y \int \frac{d^3k}{(2\pi)^3} \frac{e^{i\vec{k} \cdot (\vec{x} - \vec{y})}}{k^2 + a} \vec{H}(y) = \\ &= \int d^3y \iiint d\phi d\theta \frac{dk}{(2\pi)^3} k^2 \sin\theta \frac{e^{ik|\vec{x} - \vec{y}| \cos\theta}}{k^2 + a} \vec{H}(y) = \\ &= \int d^3y \frac{1}{4\pi|\vec{x} - \vec{y}|} e^{-\sqrt{a}|\vec{x} - \vec{y}|} \vec{H}(y). \end{aligned} \quad (21)$$

The two point function or the correlation function is defined as

$$\langle \vec{M}(x) \vec{M}(0) \rangle, \quad (22)$$

that is, starting from some magnetization $\vec{M}(0)$ at the origin we ask what the magnetization will be at a certain point x . One expects it to be a steeply decreasing function of distance, such as $e^{-|\vec{x}|/\xi}$, where ξ is the correlation length. For $T > T_c$ the critical exponent ν is defined as $\xi \propto (T - T_c)^{-\nu}$. In the Landau–Ginzburg model (Ginzburg & Landau, 2009; Abrikosov, 1957; Gorkov, 1959) the correlation length is given by $\xi = 1/\sqrt{a}$ giving the value $\nu = 1/2$.

Superconductivity

A *superconductor* is a material which below a temperature $T < T_c$ exhibits no resistance to electrical current. The long-standing suspicion that this behaviour was correlated to Bose–Einstein condensation, even if electrons are fermions, was confirmed after the discovery of the Cooper pair (Cooper, 1956), where two electrons bound together at low temperature with some energy lower than the Fermi energy. This condensation is responsible for the effect of superconductivity. Landau and Ginzburg

had the idea of describing the mechanism by studying the field $\phi(x)$ associated with these condensing bosons without knowing the mechanism of electrons pairing. This description is analogous to the previous one of magnetism. There is a complex field $\phi(x)$ carrying two charge units, the Cooper pair. The Lagrangian is the one already seen in eq. (6) with the variation of $\mathcal{D}_i\phi = (\partial_i - i2eA_i)\phi$ because ϕ is charged¹.

The free energy inclusive of the energy of external magnetic field is given by

$$G = \frac{1}{4}F_{ij}^2 + |\mathcal{D}_i\phi|^2 + a|\phi|^2 + b|\phi|^4 + \dots, \quad (23)$$

clearly invariant by construction under the $U(1)$ transformation $\phi \rightarrow e^{2ie\Lambda}\phi$ and $A_i \rightarrow A_i + \partial_i\Lambda$.

An important consequence of superconductivity is the Meissner effect: below a critical temperature $T < T_c$ an external magnetic field \vec{B} is expelled from the conductor. This means that a magnetic field inside the material is energetically disfavoured.

If a constant magnetic field is considered, then it costs an energy of the order of $E \propto \vec{B}^2 L^3$, where L^3 is the volume of the conductor. In terms of a potential field \vec{A} , where $\vec{B} = \vec{\nabla} \times \vec{A}$ there is $\vec{B}^2 \propto \vec{A}^2$. A constant field \vec{B} implies that \vec{A} grows linearly with the distance L , so one obtains $E \propto \vec{A}^2 L^3 \propto L^5$. In order to maintain a constant magnetic field inside the superconductor, a huge amount of energy is needed, so such configuration is heavily disfavoured, and as a consequence, \vec{B} is expelled from the superconductor.

As before in (14), we assume a linear behaviour in temperature for the coefficient $a \propto (T - T_c)$ while b remains positive. For $T > T_c$ G has a unique trivial minimum for $|\phi| = 0$, while for $T < T_c$ G has minima for $|\phi| = \sqrt{-a/(2b)} \equiv v$ as found in eq. (8), in complete analogy to Figs. 2a and 2b, respectively, after the exchange of M with $|\phi|$. The free energy (23) becomes below the critical temperature (Nambu, 1960; Hooft, 1971)

$$G = \frac{1}{4}F_{ij}^2 + (2ev)^2 A_i^2 + \dots. \quad (24)$$

In order to estimate more precisely the penetration length of a magnetic field inside a superconductor, known as the London penetration length, we

¹Actually Landau had this intuition much before the discovery of Cooper pairs, but he considered only a single electron instead of a pair.

need the results of the Landau–Ginzburg model. From (24) one expects the two terms to compete for the same energy, i.e.

$$F_{ij}^2 \propto (ev)^2 A^2. \quad (25)$$

Let l_L be the London penetration length, so the energy of the electromagnetic field is $F_{ij}^2 \propto A^2/l_L^2$, and from the comparison with (25) we obtain

$$l_L \propto \frac{1}{ev} = \frac{1}{e} \sqrt{\frac{2b}{-a}}. \quad (26)$$

As already discussed in (20), the characteristic length of the scalar field ϕ is of the order of $l_\phi \propto 1/\sqrt{-a}$, because the coefficient a plays the role of a squared mass.

Comparing the two characteristic lengths, we finally obtain

$$\frac{l_L}{l_\phi} \propto \frac{\sqrt{b}}{e}. \quad (27)$$

References

Abrikosov, A.A. 1957. On the magnetic properties of superconductors of the second group. *Soviet Physics - JETP*, 5, pp.1174-1182 [online]. Available at: <https://elibrary.ru/item.asp?id=21757785> [Accessed: 14 January 2023].

Anderson, P.W. 1963. Plasmons, Gauge Invariance and Mass. *Physical Review*, 130(1), pp.439-442. Available at: <https://doi.org/10.1103/PhysRev.130.439>.

Cooper, L.N. 1956. Bound Electron Pairs in a Degenerate Fermi Gas. *Physical Review*, 104(4), pp.1189-1190. Available at: <https://doi.org/10.1103/PhysRev.104.1189>.

Englert, F. & Brout, R. 1964. Broken Symmetry and the Mass of Gauge Vector Mesons. *Physical Review Letters*, 13(9), pp.321-323. Available at: <https://doi.org/10.1103/PhysRevLett.13.321>.

Fabiano, N. 2021a. Quantum electrodynamics divergencies. *Vojnotehnički glasnik/Military Technical Courier*, 69(3), pp.656-675. Available at: <https://doi.org/10.5937/vojtehg69-30366>.

Fabiano, N. 2021b. Corrections to propagators of quantum electrodynamics. *Vojnotehnički glasnik/Military Technical Courier*, 69(4), pp.930-940. Available at: <https://doi.org/10.5937/vojtehg69-30604>.

Fabiano, N. 2022. Path integral in quantum field theories. *Vojnotehnički glasnik/Military Technical Courier*, 70(4), pp.993-1016. Available at: <https://doi.org/10.5937/vojtehg70-35882>.

Ginzburg, V.L. & Landau, L.D. 2009. On the Theory of Superconductivity. In: *On Superconductivity and Superfluidity*, pp.113-137. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/978-3-540-68008-6_4.

Goldstone, J. 1961. Field theories with « Superconductor » solutions. *Il Nuovo Cimento (1955-1965)*, 19(1), pp.154-164. Available at: <https://doi.org/10.1007/BF02812722>.

Gor'kov, L.P. 1959. Microscopic derivation of the Ginzburg-Landau equations in the theory of superconductivity. *Soviet Physics - JETP*, Vol.36(9), No.6, pp.1364-1367 [online]. Available at: http://www.jetp.ras.ru/cgi-bin/dn/e_009_06_1364.pdf [Accessed: 14 January 2023].

Guralnik, G.S., Hagen, C.R. & Kibble, T.W.B. 1964. Global Conservation Laws and Massless Particles. *Physical Review Letters*, 13(20), pp.585-587. Available at: <https://doi.org/10.1103/PhysRevLett.13.585>.

Higgs, P.W. 1964a. Broken symmetries, massless particles and gauge fields. *Physics Letters*, 12(2), pp.132-133. Available at: [https://doi.org/10.1016/0031-9163\(64\)91136-9](https://doi.org/10.1016/0031-9163(64)91136-9).

Higgs, P.W. 1964b. Broken Symmetries and the Masses of Gauge Bosons. *Physical Review Letters*, 13(16), pp.508-509. Available at: <https://doi.org/10.1103/PhysRevLett.13.508>.

Hooft, G.'t. 1971. Renormalizable Lagrangians for massive Yang-Mills fields. *Nuclear physics B*, 35(1), pp.167-188. Available at: [https://doi.org/10.1016/0550-3213\(71\)90139-8](https://doi.org/10.1016/0550-3213(71)90139-8).

Kadanoff, L.P. 1966. Scaling laws for Ising models near T_c . *Physics Physique Fizika*, 2(6), pp.263-272. Available at: <https://doi.org/10.1103/PhysicsPhysiqueFizika.2.263>.

Nambu, Y. 1960. Quasi-Particles and Gauge Invariance in the Theory of Superconductivity. *Physical Review*, 117(3), pp.648-663. Available at: <https://doi.org/10.1103/PhysRev.117.648>.

Wilson, K.G. 1971a. Renormalization Group and Critical Phenomena. I. Renormalization Group and the Kadanoff Scaling Picture. *Physical Review B*, 4(9), pp.3174-3183. Available at: <https://doi.org/10.1103/PhysRevB.4.3174>.

Wilson, K.G. 1971b. Renormalization Group and Critical Phenomena. II. Phase-Space Cell Analysis of Critical Behavior. *Physical Review B*, 4(9), pp.3184-3205. Available at: <https://doi.org/10.1103/PhysRevB.4.3184>.

Коллективные явления

Никола Фабиано

Белградский университет, Институт ядерных исследований
«Винча» – Институт государственного значения для Республики
Сербия, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 29.19.00 Физика твердых тел
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Методы квантовой теории поля способны точно описать также коллективные явления статистической физики и физики твердого тела.

Методы: Метод интеграла по путям с вращением Вика показывает свою полную аналогию со статистической суммой статистической механики.

Результаты: Феноменология Ландау-Гинзбурга успешно описывает такие коллективные явления, как спонтанная намагниченность и сверхпроводимость.

Выводы: Явления нарушения симметрии могут дать макроскопические результаты.

Ключевые слова: энергия вакуума, нарушение симметрии, модель Ландау-Гинзбурга.

Коллективни феномени

Никола Фабиано

Универзитет у Београду, Институт за нуклеарне науке "Винча"-
Институт од националног значаја за Републику Србију,
Београд, Република Србија

ОБЛАСТ: физика чврстог стања, статистичка физика
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: Технике квантне теорије поља такође могу прецизно да опишу колективне појаве статистичке и физике чврстог стања.

Методе: Метода интеграла путање са Виковом ротацијом показује своју потпуну аналогију са партиционом функцијом статистичке механике.

Резултати: Ландау-Гинзбургова феноменологија успешно описује колективне феномене као што су спонтана магнетизација и суперпроводљивост.

Закључак: Феномен нарушавања симетрије могао би дати макроскопске резултате.

Кључне речи: енергија вакуума, нарушавање симетрије, Ландау-Гинзбургов модел.

Paper received on / Дата получения работы / Датум пријема чланка: 15.01.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 28.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 29.11.2023.

© 2023 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в "Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier" (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Данная статья в открытом доступе и распространяется в соответствии с лицензией "Creative Commons" (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (<http://vtg.mod.gov.rs>, <http://втр.мо.унр.срб>). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Challenges of the Fourth Industrial Revolution (4IR), transformation of modern armed forces and the ethical dilemma of robotic automation

Nenad M. Miloradović^a, Goran M. Vukadinović^b

Ministry of Defence of the Republic of Serbia, Sector for Material Resources, Belgrade, Republic of Serbia

^a e-mail: nenad.miloradovic@mod.gov.rs,
ORCID iD: <https://orcid.org/0009-0006-4123-2627>

^b e-mail: goran.vukadinovic@mod.gov.rs, **corresponding author**,
ORCID iD: <https://orcid.org/0009-0008-9919-3709>

DOI: 10.5937/vojtehg71-44825; <https://doi.org/10.5937/vojtehg71-44825>

FIELD: technology, engineering, machine learning and applications
ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: The first industrial revolution used the power of steam and water for the mechanization of manufacturing. The second one used electricity for mass production. The third one used electronics and information technologies for the automation of production, while the fourth industrial revolution aims to enable erasing of the boundaries between the physical, digital and biological spheres in order to reach smart automation and increase the interconnection of system elements. Thus, previous industrial revolutions changed the way we work, the next one is changing the way we think. Our generation is privileged of being a contemporary of tectonic technological changes, a witness to changes that fundamentally convert production processes and relations in production, but also a witness to the changes that those products bring to the functioning of the mankind, from individuals to state organizations, including the military as well. The main goal of this paper is to indicate to the wider military academic community the need for coordination and interdependent development of combat systems, doctrine and structure of defence organizations.

Methods: This paper will use general scientific methods that are used, or can be used, to acquire scientific knowledge in all scientific fields and disciplines. We highlight the hypothetical-deductive method, the analytical-deductive method and the comparative method.

Results: (Increased) Equipping with weapons and military equipment generated from the current technological revolution requires radical changes in the defence area, both in the combat component, i.e. changes of basic combat units that should optimally use these weapons (their doctrines, tactics, organization, training, etc.) as well as the

administrative-bureaucratic component of the national defence system that deals with the procedures of weapons development, production and procurement, which should follow the fastest pace of innovation ever in the commercial industry area.

Conclusion: The authors would like to point out the interdependence between the emerging challenges of the 4IR and the directions of transformation of modern armed forces.

Keywords: industrial revolution, organization, transformation, war, unmanned/robotized platforms.

Introduction

Unmanned/robotized platforms significantly increase the operational capabilities of modern armed forces, presenting one of the main force multipliers of the military operation power, especially their collaborative action in combined arms operations, integrated into units equipped with manned combat platforms and supported with Command Informational Systems (CIS) of the new generation based on artificial intelligence. Such a combination enables to make maximum use of huge sensor potentials, reaction speed and lethality of robotic systems with cognitive capabilities of soldiers in manned platforms. The level of force protection is significantly improved and at the same time the level of situational awareness, the quality and speed of decision making by commands, with accelerated combat dynamics will radically change and reshape the combat philosophy in the near future. Despite the advantages of their application in armed forces, no military in the world is able to quickly introduce radical structural changes that the appearance of unmanned platforms and robotic automation inevitably brings with it, especially not at the speed at which these platforms are developing.

Therefore, it is necessary to have a holistic approach and develop robotic platforms and in parallel the related doctrines of their usage, and finally, most importantly, the organization of the forces that use them, with a lot of experimentation until reaching the optimal solution.

Tectonic global changes are accelerating since the establishment and then the demise of the bipolar world, i.e. since its transformation into the unipolar world with the multipolar world emerging before our eyes, at a speed that is difficult to understand, since we are accustomed to conditions that last for several centuries, a whole century or at least 50 years.

The speed of social changes is conditioned, first of all, by technological achievements that are developing like never before in the entire human history. In relation to the overall development of the mankind,

the journey of one and a half century, which man has travelled from pre-industry to the 4IR, to which we are contemporaries, is quite short.

Nowadays, the pace of changes makes a clear difference between "small and big players", i.e., between those who are only able to use the results of technological achievements, and those who develop these achievements.

In other words, in the modern world, the former will remain deaf and blind consumers of the knowledge of technology owners, and the latter will be able to leverage their role in the development of innovations through the paradigm of the overall struggle for supremacy in international relations. The use of the 4IR achievements for military purposes has potential and tendency to change the philosophy of combat operations, the existing doctrines of each and every branch and service of the armed forces, the strategy and the usage of armed formations in war.

Although the time to come will judge the correctness of the following lines, we predict that even small countries (in terms of territory, population, economic strength, etc.) that can manage to keep pace with the development, production of robotic combat systems and their integration into combat units (in the previously described way), will in the very near future ensure the necessary level of capability and competence of their armed forces to enable security independence or neutrality primarily through deterrence.

Fundamentals and terms

Industrial revolutions and their basic characteristics are (Schwab, 2016):

- First industrial revolution: Water and the power of steam bring unprecedented mechanization of production,
- Second industrial revolution: Electricity and electrical machines enable mass production,
- Third industrial revolution: Electronics and information technologies will enable the automation of production and increase in produced quantities, and
- Fourth industrial revolution: Erasing the boundaries between the physical, digital and biological spheres with the aim of smart automation and increasing the interconnection of system elements.

The basic technological innovations in the Fourth Industrial Revolution are (Schwab, 2016):

- Artificial intelligence¹,
- Robotics,
- Autonomous systems,
- Fast production technologies/3D printing,
- Nanotechnologies,
- Biotechnologies,
- Energy storage, and
- Quantum computing.

In the future, the mentioned and unmentioned technological innovations will bring an increase in the overall combat capabilities of armed forces, including an increase in the ability to manoeuvre, fire and move, protect one's own forces and increase situational awareness on the battlefield from the strategic command level down to the individual soldier.

The need to introduce automatization in the process of decision making, command and the use of forces is rapidly emerging, and the reaction time from receiving reconnaissance data to the target engagement will be measured in minutes/seconds (Bishop, 2006).

At the very centre of the development of the mentioned abilities that are related to artificial intelligence (AI), there is an activity called machine learning (ML). Such learning involves the development and use of a computer system that, without prior explicit instructions, using algorithms and statistical models, analyses and derives conclusions/predictions from "patterns" in the data and it can be (Russel & Norvig, 2016):

- supervised learning,
- unsupervised learning, and
- reinforcement learning.

For military purposes, a model will be used that enables the highest possible combat capabilities, regardless of ethical obstacles (which will be discussed later) that have not prevented the world's armed forces from renouncing their firepower or lethal power.

¹ Author's remark: A computer system that, by using a large set of data, is aimed to perform tasks that normally require human intelligence - visual and audio perception and recognition, reasoning and decision making (digital intuition).

Robotic combat platforms (RCP)

Robotic combat platforms or robotic combat systems (RCP or RCS) in use, and especially those under development, can be divided into two main categories, depending on their concepts.

The first group includes those designed to imitate the behaviour of insects - to be used en masse (in swarms) thus overcoming the opponent's defence - not their individual qualities, but their numbers and coordinated movements and actions. Such platforms are an expendable resource; a good part of them can be considered ammunition (killer/kamikaze drones) and must be as cheap as possible. They will incorporate fast production technologies, ultralight materials, miniature sensors, and protected telecommunications with very high bandwidth and of course artificial intelligence (AI), i.e., powerful algorithms with machine learning (ML) for image processing (Sutton & Barto, 1998), target recognition and coordination of the movement of the entire swarm during the execution of the task (e.g. attack on the given types of targets).

The second group includes robotic combat systems designed to imitate a human warrior or a manned combat platform and should be integrated and used within formations/units that use conventional manned ground, air or naval weapon systems. Such platforms are much more valuable, more expensive, with individual combat characteristics similar to corresponding manned platforms and will require an increased level of combat toughness. All current technologies applied to newly developed manned platforms are relevant to this class of robotic combat systems.

Airborne robotic combat systems, either offensive (UCAV²), which as a rule are sent into the enemy's airspace in front of piloted formations and controlled from the ground, or those of the *Loyal wingmen*³ type, which will be integrated into piloted aircraft formations and directly controlled by them, have a stealth design, are made of a new generation of composite materials, have similar flight-dynamic characteristics and are equipped with similar sensors (radar and optoelectronic), systems for electronic reconnaissance, anti-electronic combat and self-protection, links and weapons as multipurpose aircraft of the latest generation.

Therefore, all applied technologies for the development and production of the aforementioned subsystems will be applied to airborne

² Author's remark: UCAV (Unmanned combat aerial vehicle) - an unmanned combat aircraft with the task of surveillance, reconnaissance and combat action on observed or assigned targets.

³ Author's remark: The first flight of the robotic combat system *Loyal wingmen* was carried out by the RAAF, Boeing Australia, on 27 February 2021.

robotic combat platforms. The exception, of course, are systems for the direct functioning of the pilot (survival, visualization, control, etc.) whose overall system and subsystems design, due to the absence of the pilot, require a somewhat reduced level of redundancies due to the generally reduced required level of reliability of the entire system, which contributes to the reduction of its price and mass and can affect the increase of dynamic characteristics. Certainly, both artificial intelligence and machine learning are essential for the functioning of these RCPs because they should provide them with the necessary level of autonomy - from avoiding obstacles, collisions in airspace to avoiding or responding appropriately to perceived threats and detecting and recognizing targets and using their own weapons.

Ground robotic combat platforms have a concept similar to that of manned vehicles, most often tracked, less often wheeled; they are equipped with remote-controlled weapon stations, generally standard ones, i.e. developed for manned combat vehicles. Therefore, as with air and ground robotic combat platforms, all the technologies planned for application on current platforms with crew, sensors, weapons, ammunition, protection, camouflage, propulsion and transmission, etc. will be used. Also, the design of both manned platforms and RCPs will represent an appropriate compromise of technical solutions in order to achieve a balanced ratio of protection, tactical agility and lethality in accordance with the tactical-technical requirements (TTR) for a given vehicle category.

The current US strategy for the development of (robotic) ground land forces (and which will probably be followed by other advanced armies, both allied and adversary), envisages the development of three categories of robotic platforms (U.S. Army Training and Doctrine Command, 2017). The first consists of light robotic combat systems that are deployed in front of other forces both in attack and defence and will be the first to cross the line of contact with the enemy; the second group are medium robotic platforms deployed between light and heavy ones with an increased level of protection and lethality; and finally heavy platforms deployed together with formations of manned vehicles (MUM – manned – unmanned teams) and with the characteristics (protection, lethality and mobility) at their level.

When it comes to protection, it will represent a combination of camouflage measures, emission management in the EM spectrum (reduction of reflection in all parts of the EM spectrum and the probability of detection or identification) and passive (less often active) ballistic protection, depending on the vehicle-system category. The level of ballistic protection will certainly be lower than that required for modern manned vehicles and will range from minimum protection of vital subsystems for

observation and communication in light RCPs (in order to preserve at least the reconnaissance functions in the event of combat damage to the platform), through protection at the level of STANAG 4569⁴ level 2–3 in medium RCPs, up to the level of protection for the heavy RCP equivalent to the one for the main battle tank. The Serbian robotic combat platform *Mali Miloš* was conceived from the beginning as fully protected with armoured steel plates. The next version of this family will have a modern composite armour made of ceramics and HMWP polyethylene plates.

The next generation of such vehicles will benefit from the progress in developing new materials such as lighter and more resistant materials, for example non-Newtonian fluids for ballistic protection, materials enabling advanced camouflage through biomimicry (Biomimetic), as well as intelligent materials which will enable the collection of energy from the environment - Energy Harvesting or the monitoring of the state of an unmanned system in real time - Structural Health Monitoring. They will even enable self-healing in some domain - Self-Healing Materials (Miloradović, 2022).

The most important technologies applied to RCPs

The physical environment in which unmanned autonomous systems operate varies on land, at sea, under water, in the air, and in space. Electromagnetic waves, light, vibrations, and heat spread differently through different media. Also, the principles of movement in the air and in the water cannot be the same due to the different density of matter and the corresponding laws of fluid dynamics that are completely different from those that apply to movement on the land. Therefore, some technologies, materials from which the structure is built, power units, systems that ensure manoeuvrability, observation and communication systems applied to RCPs specialized for operations in these different domains will certainly be different. Also, optimal energy sources for use in different domains will be different. For example, fuel cells are more suitable for underwater systems, batteries and hybrid drives are more suitable for light air and land platforms, and fossil fuel power units are still optimal for heavy land and air platforms which use oxygen from the air.

Of course, there are also technologies that, with more or less variations, are applicable in all four domains. For example, the architecture of electronic components is the same for all applications in all domains. In addition, the 4IR tends to encompass and pervade all aspects and

⁴ Author's remark: NATO AEP-55 STANAG 4569 - NATO standardization for "Protection Level for Occupants of Logistic and Light Armoured Vehicles".

domains of human life and actions equally, and it is in its essence to unite different domains and worlds.

It is certain that all technologies related to humans, from the individual combatant/system operator to the highest joint command of armed forces, will by their nature converge towards more or less similar solutions in all domains. More precisely, in the coming revolution in the warfare of combined human-robot armed forces, the human factor becomes the key limiting element and its ability to manage all these systems (and management and control will practically be the only functions left for exclusive human actions) will require a significant technological reinforcement adapted to the man as a unique biological mechanism, regardless of the domain in which the object of his management is.

This, therefore, refers to command and information systems (CIS) and management control consoles and devices (Man Machine Interface - MMI) which have been operated in all physical domains with all available forces, including all available manned and unmanned platforms and all application hardware and software solutions (Miloradović, 2022).

It is in this area that AI/ML will be of great importance and will make a huge difference in the combat capability between armed forces that make such advances in force integration and command and those that continue to perform this function in the traditional way; this difference will probably be more significant than the difference any single combat system or a planned "superweapon" can bring (Miloradović, 2022).

It is evident that within the framework of the new geopolitical paradigm of the renewed competition of global powers in the multipolar world, as well as under the influence of the revolutionary development of new military technologies, especially those that are the subject of this discussion, a fundamental change is taking place in the capabilities of the armed forces of the main global players from the highest strategic down to the lowest tactical level. Operations will be carried out simultaneously in as many as five domains (land, water, air, space and cyberspace) and will involve the application of a wide range of combat and non-combat activities where the commander of the operation will, optimally and much faster than before, use the resources assigned to him from all five domains and choose "services" that are necessary for him at a given moment or are the most appropriate.

The first task that such an organization should achieve is decision dominance in relation to the adversary, i.e., to faster analyse and understand the operational picture of the battlefield formed on the basis of information collected from all the mentioned domains formed and

refreshed in real time, and make decisions faster and act faster than a potential adversary (U.S. Army Acquisition Command, 2022).

One of the current Battle Management Systems (BMS), being developed with such a goal, is the American CJADC2 (Connecting Joint All-Domain Command and Control), which on a global level provides assistance in command (U.S. Army Acquisition Command, 2022). That system, helped by massive AI/MU algorithms, significantly shortens the time that the command staff would spend on deciding in certain situations and allows the order/instruction and the necessary data for the operation to be transmitted in seconds to the best positioned units or effectors.

Apart from this example of AI-supported BMS at the highest strategic level of command, and as an illustration of currently applicable technologies, we also cite an example of AI-supported BMS at the lowest tactical level, i.e., at the level of an infantry (robotized) platoon, and the individual soldier/operator within it. It is called AISUM (Artificial Intelligence for Small Manoeuvre Unit) and is a part of the US Army project 10X Platoon⁵ (Platoon - robotic - tenfold increased combat capabilities). A specific requirement that this BMS should achieve is a tenfold shortening of the OODA loop⁶.

The system enables the data fusion of sensors integrated on both robots and soldiers, creation of a simplified picture of the situation with indicated goals and instructions of the higher command, its analysis and recommendation of specific activities, with the aim of improving and greatly accelerating the decision-making and execution process. At the robot level, the BMS enables autonomy of movement and even opening fire on targets previously approved by the operator, which significantly reduces the burden on the soldier and speeds up the control of the robot - individually and collectively at the platoon level.

The visualization system integrated on the soldier's helmet projects symbology onto a realistic 2D image of the environment. The system is connected by radio to both the soldier's personal weaponry and the RCP which the soldier controls thus enabling the use of different packages of weapons that the RCP can be equipped with.

⁵ Author's remark: still in the experimental phase.

⁶ Author's remark: OODA - Observe, Orient, Decide, Act.

Ethical issues of the use of the RCP and artificial intelligence in general

Every new technology, especially the so-called "disruptive technologies" (Armstrong, 2017), in addition to solving a certain class of problems, also brings with it the unknown as well as many organizational and ethical problems and dilemmas. But since the discovery of the atomic bomb, nothing has agitated the imagination of both the civilian and military public as much as artificial intelligence, and especially weaponized artificial intelligence, i.e., artificial intelligence-controlled RCPs. The atomic bomb created the possibility that the human race could destroy itself with its technology, and artificial intelligence brings a theoretical possibility that technology could destroy the human race without the latter's participation or will. It has captured the global attention for the last 30 years and brings significant revenue to the sci-fi film industry ever since.

In the last two decades, this issue has been seriously discussed at the level of the armed forces and defence ministries of a number of countries. The first legal regulations were passed and adopted, the essence of which boils down to the following: "autonomous and semi-autonomous weapon systems must be designed to enable commanders and operators to exercise an appropriate level of human judgment over the use of lethal force" (Department of Defence US army, 2012), which means that a robot must not be allowed to (independently) decide to kill a human.

According to the currently generally accepted gradation of the autonomy of unmanned systems (from Level 1- fully remotely controlled by a human to Level 10 - fully autonomous in the execution of a task previously obtained by a human) RCPs can be divided into those with "man in the loop", "man over the loop", and "a man out of the loop". The world famous unmanned aerial vehicle *Predator* was probably in Level 2 on the said scale. RCP systems under development today mainly belong to those with a "man over the loop" with a high level of autonomy in movement and limited autonomy in fire action, i.e., that the operator issues an instruction based on the recommendation of the artificial intelligence, and the sighting and shooting process is performed by the robot with the possibility of the operator stopping it. Imagined combat actions in the future with mass strikes of robotic "swarms" from the air, purely robotic or mixed human-robotic ground combat formations, require a dramatic shortening of the OODA loop.

In just a few seconds, it is necessary to detect the threat, evaluate the threat, choose an adequate response and take action, while the number

of possible simultaneous threats is measured in the hundreds. It simply exceeds the mental and physical capabilities of the man. Human capabilities barely allow a quick response to an individual threat. It is clear that humans (in other words, the limitations of human biology and ability, i.e., slowness in processing information and reacting) reduce the overall efficiency of future human-robot armies and individual RBPs (used in groups); therefore, they will inevitably become more and more autonomous, and the above described moral dilemmas and risks of misuse are increasing.

The previously described MMI (man-machine interface) and CIS are tasked with ensuring maximum efficiency of the system, i.e., to facilitate and speed up human reaction and still provide sufficient control over the effect of weapons in accordance with current legal norms. One can imagine the consequences of a situation in which the artificial intelligence of the above-mentioned global CIS, which controls a huge number of combat systems (including autonomous ones), issues a "wrong recommendation" to the commanders, and they, not seeing the error or errors, transmit such commands and coordinates for action.

A similar level of moral-ethical dilemmas (with enormous possible progress) also brings the issue of the potential application of HA - "human augmentation" - the improvement of human abilities with the application of technology. Science (medicine) has been working for millennia on technologies for maintaining and repairing the human body, i.e., restoring its abilities degraded by aging, diseases or physical injuries. However, the technologies that will enable not renewed but "superhuman abilities" are maturing rapidly and of course will find military application first. We can conditionally divide them into "wearable" ones, i.e. placed on the human body, and "built-in" ones, i.e. which are implanted (surgically) in the human body. The beginning of the (massive) use of the former is a matter of solving the remaining (not crucial) technological problems and does not carry with it any moral dilemmas. To mention some of the most interesting ones: shortening the OODA loop is key to increasing the efficiency of any weapon system or military formation, and AR (AR - Augmented Reality⁷) is currently a key technology for that purpose (Miloradović, 2022). AR allows the transmission of symbology, imagery (processed by AI), information and instructions from sensors, weapon systems, and CIS to a helmet-mounted device.

⁷ Author's remark: AR - Augmented Reality - augmented reality with digital information about the environment in real time, i.e. an image of the real environment with perceptual information generated through it from the sensor into the user's field of vision.

It has been in use in aviation for decades, and through numerous projects of "soldiers of the future", this ability will soon be acquired by most infantrymen of modern armies, as well as combat vehicles crews (Through Armour Vision⁸) (Miloradović, 2022). For the needs of the Serbian Armed Forces, at least two helmet systems are currently being developed, for which there are ambitions to be further refined with AI technologies. RCP management at a low tactical level will be dominantly based on this technology.

By using a (powered) exoskeleton, a soldier will be able to carry a standard load of clothes, equipment, ammunition and tools - 60+ kg according to today's standards (Headquarters Department of the US Army, 1990) and uphill, with the effort of walking on the beach in a bathing suit. And in the near future (when new energy sources of higher energy density become operational), soldiers will be able to carry heavier and stronger armour as well as more powerful and heavier weapons.

Another ones, built-in (implanted) technologies, "threaten" to move rapidly from the domain of science fiction to the domain of real application.

The miniaturization of sensors, computers and communication systems will allow IR, acoustic sensors, position sensors, and others, to be "embedded" in or behind the human eye and ear, enabling significantly increased sensitivity. This will also enable embedding processors with AI/ML algorithms which will process information from these and natural sensors and communicate with the human brain, giving it "superior cognitive abilities", or installing RF transceivers that would enable "telepathic" communication, as well as supplying all of these with either artificial or natural energy sources available in the human body. The moral dilemmas related to the emergence of such super-soldiers with "technological implants provided with superhuman abilities" are comparable in importance to those related to the emergence of "self-aware armed artificial intelligence" and will probably slow down the application of the mentioned technologies, but cannot completely prevent it (Miloradović, 2022).

Organizational problems and dilemmas

Martek's Law (Brinker, 2013), states that "technology changes exponentially, while the organizational structure changes logarithmically", meaning much more slowly. Organizations work on the basis of

⁸ Author's remark: Visibility through armor - a set of monitors including head-mounted ones that project an image of the environment from cameras/sensors deployed on vehicles, giving full visibility of the environment.

regulations and procedures, and the related bureaucracy, as a rule, "defends itself against changes" by using those regulations, and tends constantly to enlarge itself and to "regulate or prohibit something additionally". This especially could be applied to revolutionary technologies because they inevitably bring dramatic changes to the organization, and the administration, which naturally tries to delay this happening stressing potential hazards and the need to "further improve technology" before it is applied.

However, when the international circumstances reach the point they are now at, with the increased danger of the outbreak of a direct global armed conflict, which otherwise is already raging in all but the kinetic - armed phase, the management of the leading military organizations become aware, and rightly so, that the technological progress of potential adversaries threatens significantly to change the balance of power. Then the hunger for "disruptive technologies" overrides the comfort and established practice of the bureaucracy, and the threshold of tolerance for new and not yet fully perfected technologies grows, as does the budget for their acquisition.

By its nature, the technology of the 4IR brings the democratization of industry and production in general, because it enables a small group of people working from their homes, without huge investments in production facilities with numerous highly specialized workforce, to achieve notable technological development and commercial success. We see that the defence organizations of the most powerful countries (MoD of France Directorate for Innovation, numerous agencies under the DoD and the commands of the US Armed Forces) and even multinational organizations (NATO - DIANA) are urgently reorienting themselves and their operational procedures to use such entities (SME - Small to Medium Enterprises) as the main actors of technological development.

Also, there are more and more doctrinal documents and instructions announcing greater innovation within military organizations, the need for "a cultural change that follows changes in the economy, civil technologies, organizations and society in general..." (U.S. Army Training and Doctrine Command, 2017) constant improvement (not only related to weapons), constant reorganization and transformation, in other words: "transformation is a way of life thus it never ends, one can only finish the ongoing phase of it". It also demands constant experimentation with both organization and technology, preferably at the same time (Miloradović, 2022). We see that, through the Soldiertouch series (repeated experiments organized in a simulated combat environment as realistically as possible), experimental units are testing systems of "commercial

quality" and at an increasingly lower level of technology readiness/maturity (TRL - Technology Readiness Level).

As history teaches us, the results and lessons learned from globally significant wars (the one currently being fought in Europe certainly comes into this category) dramatically speed up the change. Naturally, and following the instinct for self-preservation, smaller countries should be even more aggressive, bolder in experimenting and applying both technological and organizational novelties in order to balance or (at least partially) reduce the natural advantage of larger and by nature more bureaucratized and regarding innovations slower potential opponents. Undoubtedly, there are such examples (Miloradović, 2022). Time is probably the only natural resource that is equally distributed to everyone. Those who manage that resource more successfully, i.e., do not spend it (too much) on procedures, bureaucracy, internal tensions regarding responsibilities and priorities, accept risks and implement innovations (proven to be useful and feasible by experiments), adopt visions faster, make decisions that will be, with (other) available resources, implemented quickly - have a chance to gain an advantage over opponents who use that resource less successfully, even though their other potentials are greater.

Therefore, we believe that we will see an increasingly rapid application of "revolutionary weapons" in the immediate future, including RCPs that are the subject of this paper, and that the ethical issues related to their application by the main global factors will "become less relevant".

Certainly, the technologies described here will be used for some time (probably by the end of the next decade) to increase the effectiveness of actions based on already existing concepts of operations, without dramatic changes in the structure of military organizations and hierarchies. It is likely that advances in technology (perhaps by the middle of this century) will cause a dramatic change in concepts of operations and lead to heralded dramatic changes in the military organization itself (Hubin, 2012). It is possible that at the end of the century we will face the described catastrophic scenarios of the conflict between the human race and its self-aware artificially intelligent technology. We believe that the former will be naturally intelligent enough to restrain the latter and ensure their joint journey into the future, and thus their further prosperity.

The Serbian Armed Forces capabilities development by implementing the achievements of the 4IR focusing especially on robotic automation

By following actively the global trends in equipping with armaments and military equipment (AME), as well as by analysing the lessons from low and high intensity conflicts worldwide (Middle East, Central Asia and West Africa, above all) and especially these from the ongoing war on our continent (in Europe), the Serbian military also recognized an urgent need for the development of robotic capabilities. The collected war experience, especially from the current war in Ukraine, unequivocally confirms that the described tectonic changes already exist in all areas of development, production and use of RCPs for military purposes.

It should be mentioned that the Serbian Armed Forces have already been equipped with various ground and airborne unmanned platforms for many years, intended mainly for combat operations, reconnaissance and logistical support. They were developed and procured at the individual request of certain branches and services of the armed forces. They are the result of domestic development and production or produced in cooperation with foreign partners or acquired as finished products from foreign suppliers. Nevertheless, following the collected experiences, and with the aim of implementing the achievements of the Fourth Industrial Revolution in the armed forces, the need has emerged to have a comprehensive approach and further massively equip all branches and services of our armed forces with robotic/unmanned platforms. Special attention should be paid to the transition from remotely controlled platforms to robotic platforms. In this way, the emphasis will be on the development and procurement of new unmanned platforms with more autonomous functions based on artificial intelligence but also on the successive improvement of the already introduced systems without the mentioned functions in order to expand their autonomous capabilities.

In the following period (and in accordance with the already determined types and quantities), it is necessary to equip the Serbian Armed Forces with ground and aerial unmanned platforms, starting from the lowest tactical level in infantry, mechanized and special forces, up to the level of artillery and aviation brigades. At the same time, assessing the current threats to the security (in view of the Serbian military neutrality), it is necessary to complete the structure of their optimal deployment in military units and enable their integration into a unified CIS operating on advanced software solutions. The mentioned activities should be carried out in order to:

- Improve situational awareness at all tactical/operational levels,
- Improve the command&control with the development of appropriate CIS,
- Increase force protection, and
- Increase the effective range and lethality of combat units armed with unmanned platforms.

In this regard, it is necessary to equip the Serbian Armed Forces with several dozens of types of ground and air combat, reconnaissance and logistics unmanned systems. Bearing in mind the increasing combat importance of *Loitering munitions* - i.e., killer drones, which have shown great effectiveness in current conflicts, it is essential to procure large quantities of various types and categories of these assets.

It is necessary to perform equipping following the principle of successive, individual and incremental introduction of one system at a time, along with the development of the doctrine of use and the user's organization. Also in parallel, the entire military-industrial complex of the Republic of Serbia (with their foreign partners) has to make additional effort to develop/produce appropriate unmanned platforms and to experiment with the aim of finding optimal solutions: technical, doctrinal and organizational.

Conclusion

The current trend of technological development within the most modern armed forces: USA, Western countries, but also technological giants of the Far East (China, Japan, Korea), indicates that, in the coming period (not later than 2030), a new generation of weapons will be implemented based on the achievements of the Fourth Industrial Revolution followed by the corresponding transformation of their armed forces. In addition, by 2050, there will probably be a drastic change - a "revolution in military affairs" as well as derogation from hundreds of years old principles of classic military structures and their combat operation principles.

One of the basic elements of that revolution is (gradual) robotic automation, both in terms of the increasingly massive application of unmanned and robotic platforms, as well as the automation of command and decision-making functions.

Spectacular results in this area have been achieved so far by many advanced militaries worldwide, accompanied by various experiments, conducted from the technological aspect as well as the tactical one. Due

to many challenges and constrains, the process has a slow pace, with none of the armed forces having implemented it completely throughout all branches/services and unit levels, especially not within the entire ground forces.

The US Army have achieved most in this direction, planning to form the first robotic companies within cavalry battalions in the Army brigades by 2028/2030.

The Serbian Armed Forces are currently the regional leader in this area, having achieved more than many bigger and more developed European countries, especially in terms of the development/procurement and operational use of armed drones and remotely controlled ground combat platforms. It should be emphasized that such types of platforms are significantly more complex to operate than purely reconnaissance ones, but they contribute much more to the overall operational capability due to their ability to perform a wide range of missions.

Today, the Serbian military industrial complex has significant technological capabilities in this area.

The Ministry of Defense of Serbia intends to further expand the technological base predominantly by including more scientific research organizations, technical institutes and private companies that have the ability to master appropriate technologies needed for development and production of unmanned and robotic platforms.

In the next ten-year period, a huge gap in capabilities will arise between the armed forces that will implement the results of this "robotic revolution", and those that fail to do it; consequently, the Republic of Serbia, as a militarily neutral country, must not lag behind.

References

Armstrong, P. 2017. *Disruptive Technologies: Understand, Evaluate, Respond, 1st Edition*. New York, NY: Kogan Page. ISBN-13: 978-0749477288.

Bishop, C.M. 2006. *Pattern Recognition and Machine Learning*. New York, NY: Springer. ISBN: 978-0-387-31073-2.

Brinker, S. 2013. Martec's Law: Technology changes exponentially, organizations change logarithmically. *Chiefmartec.com* [online]. Available at: <https://chiefmartec.com/2013/06/martecs-law-technology-changes-exponentially-organizations-change-logarithmically/> [Accessed: 1 June 2023].

-Department of Defence US army. 2012. DOD directive 3000.09: Autonomy in weapon systems. *Washington Headquarters Services: Executive Services Directorate*, 21 november [online]. Available at: <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf> [Accessed: 1 June 2023].

-Headquarters Department of the US Army. 1990. Field Manual No. 21-18: Foot Marches. *Elon.edu* [online]. Available at: <https://www.elon.edu/assets/docs/rotc/FM%2021-18%20Foot%20Marches.pdf> [Accessed: 1 June 2023].

Hubin, G. 2012. *La Guerre - une vision française*. Paris: Economica. ISBN-13: 978-2717861525.

Miloradović, N. 2022. Nove tehnologije u izradi robotizovanih borbenih sistema: deca 4. industrijske revolucije. *Obrana*, 361, pp.12-21 [online]. Available at: https://mod.gov.rs/multimedia/file/staticki_sadrzaj/mediji/2022/%D0%88%D1%83%D0%BD%202022/Obrana361-str12-21.pdf (in Serbian) [Accessed: 1 June 2023].

Russel, S. & Norvig, P. 2016. *Artificial Intelligence: A Modern Approach, 3rd Edition*. Harlow, UK: Pearson. ISBN-13: 978-0136042594.

Schwab, K. 2016. The 4th Industrial Revolution: What It Means, How to Respond. *GE.com*, 17 January [online]. Available at: <https://www.ge.com/news/reports/the-4th-industrial-revolution-what-it-means-how-to-respond> [Accessed: 1 June 2023].

Sutton, R.S. & Barto, A.G. 1998. *Reinforcement Learning: An Introduction (Adaptive Computation and Machine Learning) (Adaptive Computation and Machine Learning series), second edition*. Cambridge, MA: A Bradford Book, MIT press. ISBN-13: 978-0262193986.

-U.S. Army Acquisition Command (USAASC). 2022. Unstoppable plans. *Army.mil* [online]. Available at: https://asc.army.mil/armyalt/Summer2022/html/htmlArticles/index.html?origin=reader&page=88&article=/86_article.html [Accessed: 1 June 2023].

-U.S. Army Training and Doctrine Command. 2017. The U.S. Army Robotic and Autonomous Systems Strategy. *Monthly Review (MR Online)* [online]. Available at: https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf [Accessed: 1 June 2023].

Вызовы четвертой промышленной революции,
трансформация современных вооруженных сил
и моральная дилемма, связанная с роботизацией

Ненад М. Милорадович, Горан М. Вукадинович, корреспондент

Министерство обороны Республики Сербия, Сектор материальных
ресурсов, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 78.03.02 Общие проблемы войны,
78.19.13 Теория управления вооруженными силами,
78.25.00 Вооружение и военная техника,

ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Первая промышленная революция использовала энергию пара и воды для механизации производства. Вторая – использовала электроэнергию для массового производства. Третья промышленная революция использовала электронику и информационные технологии для автоматизации производства, в то время как четвертая промышленная революция направлена на стирание границ между физической, цифровой и биологической сферами, с целью достижения интеллектуальной автоматизации и увеличения взаимосвязи элементов системы. Таким образом, предыдущие промышленные революции изменили то, как мы работаем, а следующая меняет то, как мы размышляем. Нашему поколению выпала привилегия быть современником тектонических технологических изменений, стать свидетелем изменений, которые коренным образом преобразуют производственные процессы и отношения на производстве, а также свидетелем изменений, которые эти продукты приносят в функционирование человечества, начиная с отдельных людей и кончая государственными организациями, включая Вооруженные силы. Основная цель данной статьи – указать широкому военно-академическому сообществу на необходимость координации и взаимозависимого развития боевых систем, доктрин и организации.

Методы: В данной статье применялись общенаучные методы, которые используются или могут быть использованы для приобретения научных знаний во всех научных областях и дисциплинах. Между ними выделяются: гипотетико-дедуктивный метод, дедуктивно-аналитический метод и сравнительный метод.

Результаты: Настоящая технологическая революция повлекла за собой ускоренное вооружение и оснащение военной техникой и, безусловно, требует радикальных изменений в области обороны как в боевой части, то есть изменений в основных боевых подразделениях, которые должны оптимально использовать это оружие (доктрины, тактика, организация, подготовка и т.д.), так и в административно-бюрократической части системы национальной обороны, управляющей процедурами разработки, производства и закупок вооружения и военной техники, которые должны соответствовать скорейшему темпу внедрения инноваций в сфере коммерческой промышленности.

Выводы: Авторы статьи обращают особое внимание на взаимозависимость между возникающими вызовами Четвертой

промышленной революции и направлениями трансформации современных вооруженных сил.

Ключевые слова: промышленная революция, организация, трансформация, война, беспилотные/роботизированные платформы.

Изазови четврте индустријске револуције, трансформација савремених оружаних снага и морална дилема у вези са роботизацијом

Ненад М. Милорадовић, Горан М. Вукадиновић, аутор за преписку
Министарство одбране Републике Србије, Сектор за материјалне ресурсе, Београд, Република Србија

ОБЛАСТ: технологије, инжењерство, машинско учење и апликације
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: Прва индустријска револуција искористила је моћ паре и воде за механизацију производње, друга – електричну енергију за масовну производњу, трећа – електронику и информационе технологије за аутоматизацију производње, док четврта индустријска револуција тежи брисању граница између физичке, дигиталне и биолошке сфере у циљу паметне аутоматизације и повећања међусобне повезаности елемената система. Дакле, претходне индустријске револуције промениле су начин на који радимо, док последња мења начин на који мислимо. Данашња генерација има привилегију да буде сведок тектонских технолошких промена, промена које суштински мењају производне процесе и односе у производњи, али и промена које производи уносе у начине функционисања планете, од индивидуа до државних организација, укључујући и војну. Основни циљ овог рада јесте указивање на потребу усклађивања развоја борбених система, доктрине и организације.

Методe: У овом раду примењују се опште научне методе које се користе, или се могу користити, за стицање научног сазнања у свим научним областима и дисциплинама, као што су: хипотетичко-дедуктивна метода, аналитичко-дедуктивна метода и компаративна метода.

Резултати: Опремање (убрзано) наоружањем и војном опремом, проистеклом из актуелне технолошке револуције, захтева радикалне промене система одбране. То се односи како на борбени део, тј. основне борбене јединице које то наоружање треба оптимално да употребе (њихове доктрине, тактике, организације,

обуке...), тако и на административно-бирокуратски део система националне одбране који се бави процедурама његовог развоја, производње и набавке, који треба да прати никад бржи темпо иновација у сектору комерцијалне индустрије.

Закључак: Указано је на међузависност појавних изазова четврте индустријске револуције и праваца трансформације савремених оружаних снага.

Кључне речи: индустријска револуција, организација, трансформација, рат, беспосадне/роботизоване платформе.

Paper received on / Дата получения работы / Датум пријема чланка: 02.06.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 30.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 01.12.2023.

© 2023 The Authors. Published by *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).


© 2023 Авторы. Опубликовано в «Военно-технический вестник / *Vojnotehnički glasnik / Military Technical Courier*» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).


© 2023 Аутори. Објавио Војнотехнички гласник / *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Internet of Things in military applications

Vlada S. Sokolović^a, Goran B. Marković^b

^a University of Defence in Belgrade, Military Academy,
Department of Logistics, Belgrade, Republic of Serbia,
e-mail: vlada.sokolovic@va.mod.gov.rs, **corresponding author**,
ORCID iD:  <https://orcid.org/0000-0003-0782-0506>

^b University of Belgrade, School of Electrical Engineering,
Belgrade, Republic of Serbia,
e-mail: gmarkovic@etf.bg.ac.rs,
ORCID iD:  <https://orcid.org/0000-0002-6638-8058>

DOI:10.5937/vojtehg71-46785; <https://doi.org/10.5937/vojtehg71-46785>

FIELD: telecommunications, information technologies

ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: The term Internet of Things (IoT) usually refers to the collective network of connected devices and the technology that facilitates communication between these devices and the cloud, as well as among these devices. The IoT concept is lately considered and applied as the appropriate in design of systems intended for distribution of data and information between heterogeneous devices with the aim to improve efficiency and effectiveness of business and decision making. The IoT enables energy and supply chain monitoring, production coordination, equipment performance optimization, transportation, public health, and improves workers' safety and health. In addition to smart devices, IoT technology also enables the connection of various sensors as a source of data on various physical phenomena, and, based on the information obtained, it is possible to control the operation of devices, make predictions, make decisions, etc. In this paper, specific areas of the application of the IoT in the defense and security sector are analyzed in order to identify the possibilities of applying modern technologies in raising the defense potential of the state and define the directions of future research in the subject area.

Methods: The methods of content analysis of current research were applied, and then, with the deductive method, conclusions were reached about the future directions of the development of IoT technology.

Results: A detailed analysis of past and ongoing research in the defense and security sector was carried out, and potential directions of future research into the IoT were given in order to increase the operational capabilities of armed forces.

Conclusion: IoT services will certainly contribute to a greater degree of automation and improvement of the quality of military decisions on the

battlefield, especially in the conditions of unexpected scenarios in an unpredictable hostile environment, thus facilitating the reduction in both human and material losses in operations.

Key words: internet of things, defense and public safety, internet of things applications, localization and target detection, military logistics.

Introduction

The Internet of Things (IoT) presents an effective concept of a system for collecting and distributing data and information between heterogeneous IoT devices and application servers with the aim of efficiency and effectiveness improvement in all types of business and decision-making processes. The introduction of the Internet of Things enables huge improvements in a wide range of application areas, such as energy monitoring, supply chain monitoring, production coordination, equipment performance optimization, transportation, public health, infrastructure monitoring, and improvement of worker safety and health (Fraga-Lamas et al, 2016).

IoT based systems have a very broad field of applications and there are estimates that these connect several tens of billions of devices in machine-to-machine (M2M) communication. Also, it is widely assumed that IoT systems deployment will enable the automation of everything in the human environment. In addition to smart devices, Internet of Things technology also enables connecting various sensors as sources of data on various physical phenomena (Zhu et al, 2021). The gathered information that describes current events in the environment is then transmitted through communication networks to a computer – application server, where the gathered data is analyzed, classified and processed through various software applications. Based on the obtained information, monitoring of data distribution on the network, device operation control, forecasting, decision making, etc. are enabled.

IoT technology has been proven suitable for systems that manage a large number of disparate devices and equipment in order to facilitate more efficient coordination of complex processes. The increasing number of Internet connections, the rapid advance of sensor technology, and the increase in the flow in the distribution network has made IoT technology an interesting area for the research in the fields of defense and security (Pokorni, 2019).

The basic characteristics of IoT technology are (Vermesan & Friess, 2014):

- Interconnection: there is a possibility of connecting different devices (electronic and mechanical ones) in the global information infrastructure,
- Things-oriented services: online services are adapted to things due to physical limitations, security requirements or communication protocols,
- Heterogeneity: devices of different configurations and manufacturing technologies can communicate through different networks (using different open and proprietary protocols),
- Dynamic environment: online communication allows working with devices that change their physical location, speed of movement and with the temporary absence of connection, and
- Enormous scale: An increasing number of devices connected to the network is expected, as well as an enormous amount of data generated by these devices that need to be managed and adapted to the needs of applications - users.

In this paper, the specific areas of the application of the IoT in the defense and security sector were analyzed in order to identify the possibilities of modern technologies application in raising the defense potential of the state and define the directions of future research in the subject area.

The following Figure 1 presents the most important areas of the application of IoT technology for defense and public safety purposes.

The modern Network-Centric Warfare (NCW) paradigm aims to transform the conventional military concept through the policy shift towards expanded communications gateways, and by connecting battlefield assets with the command (headquarters) (Abdelzاهر et al, 2018a). In the NCW approach, through the sharing data between legacy assets and novel deployments, the significant advantages can be achieved through the force projection and the secure timely exchanged information among all entities. This way, the physical domain, in which data is generated regarding the event locations and operations, the information domain, in which the storage, processing and transmission of data and information is conducted, and the cognitive domain, in which all the gathered data is filtered, processed and analyzed in order to allow proper information extraction and support decision-making process, can be fully integrated in order to enable the joint operation of these domains including the ability to perform joint optimization related to specific tasks.

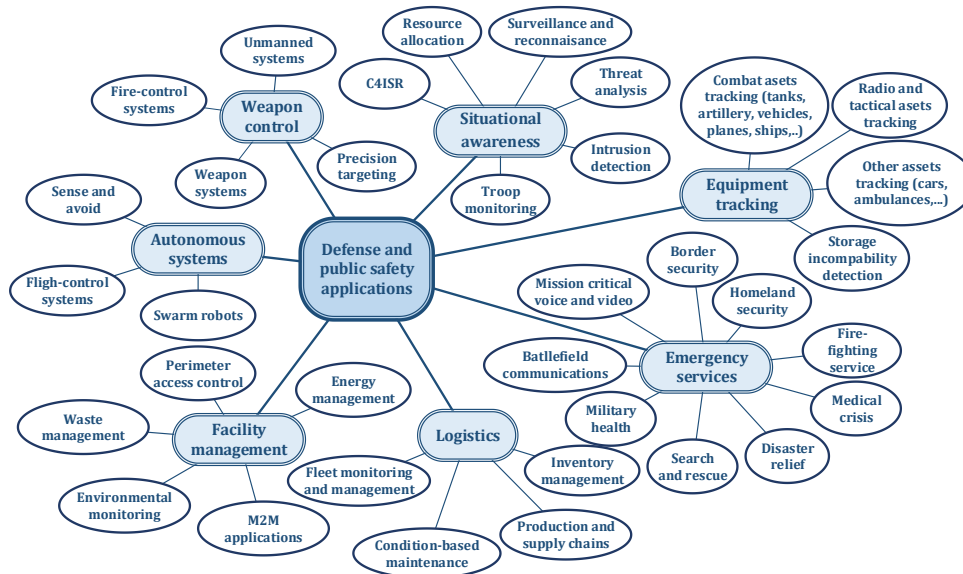


Figure 1 – The main application areas of IoT technology in defense and public safety sectors

Рис. 1 – Основные области применения технологий Интернета вещей в области обороны и общественной безопасности

Слика 1 – Главне области примене ИIoT технологије у сектору одбране и јавне безбедности

In fact, these three domains of the NCW paradigm can be directly translated into the basic elements of modern commercial IoT technology. As a result, the adoption of IoT-based systems in key areas of modern military and homeland security areas can be considered. This conclusion is additionally supported by the contemporary aspiration in defense sector to partially equip the units with the basic functionalities provided by the COTS (Commercial of the Shelf) solutions, such as smart phones, RFID (Radio-Frequency Identification), sensors, etc. Therefore, defense applications still present one of the main drives of innovations when the advanced sensors, various control systems, surveillance and reconnaissance drones, and satellite communication systems are concerned. Consequently, the defense sector is interested in adequate introduction of commercial communication and IoT solutions for its own purposes. However, the development of these is mainly driven by the private sector while the military often lags behind. Thus, adopting IoT-based solutions and business practices that satisfy the basic requirements of certain tactical systems, through partnerships with the private sector, presents an opportunity for defense and public safety

sectors. In scope of this, the comparison of basic technology stacks related to the defense and public safety sector with the private sector, as shown in Figure 2, can be of great interest in terms of possible IoT technology adoption.

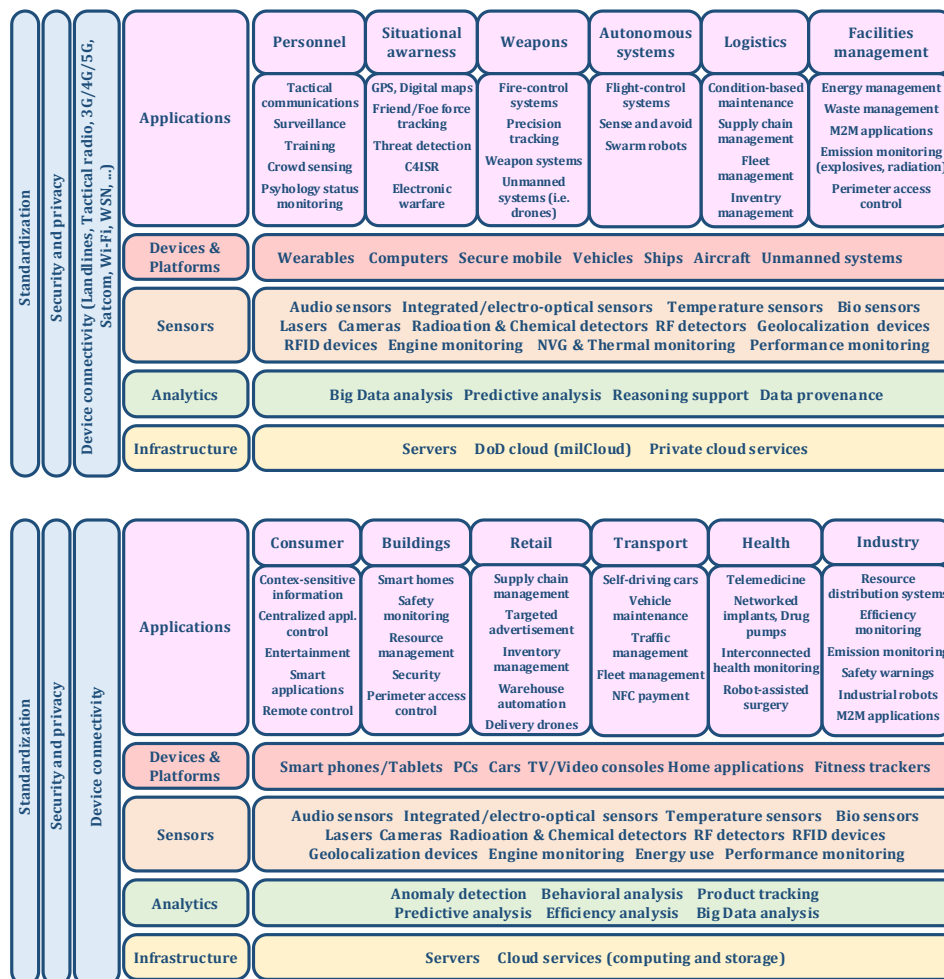


Figure 2 – The comparison of basic technology stacks suitable for the defense and public safety sectors (above) and for the private sector (under). Created by the authors based on (Fraga-Lamas et al, 2016)

Рис. 2 – Сравнение базовых технологических пакетов, подходящих для секторов обороны и общественной безопасности (сверху) и для частного сектора (снизу). Создано авторами на основе (Фрага-Ламас и др., 2016)

Слика 2 – Поређење основних технолошких пакета погодних за сектор одбране и јавне безбедности (изнад) и за приватни сектор (испод). Сачинили аутори на основу (Fraga-Lamas et al, 2016)

In addition to this introduction and conclusion section, the paper contains seven more sections. In the next section, the IoT architecture in the area of military technologies is described. The following sections describe the results and trends of research on the application of IoT in the areas of surveillance, target detection and threat localization, data collection and analysis for the purpose of aerospace forces, as well as in the area of monitoring health of soldiers and medical surveillance and logistics. A short summary of the paper is given in the concluding section.

General aspects of the IoT architecture for the support of military applications

The Internet of Things concept represents a revolution in the field of information technologies, and it creates fertile ground and enables special value for the application of artificial intelligence. Basically, the IoT concept assumes that everything can be connected and controlled using apps and sensors. IoT devices detect the observed phenomena and events through the sensor, collect data and forward it to the cloud for the further processing and analysis. Through the cloud, where the processing, analysis, controlling and decision-making entities are located, smart devices communicate with each other without the human intervention, which enables them to continuously learn (i.e. by employing machine learning) and implement their own solutions in the future. Obviously, all this presents an excellent basis for artificial intelligence. Given that there are a large number of devices that generate a huge amount of data, IoT technology is the driver of a special area, namely the analysis of Big Data in the real time.

However, although IoT systems connect a large number of heterogeneous devices, there is still no single standardized IoT system architecture.

The expansion of smart IoT devices creates new challenges for the cloud-based systems and cloud computing, especially because a large amount of data must be processed, particularly videos in real time, and the challenges related to the security and privacy. These problems are expressed both in humans and in devices intended for military applications. For this reason, the idea of applying federated learning (FL) as a privacy-preserving solution came up (Zhang et al, 2022). Federated learning for IoT implies that the raw data is not collected centrally but separately on each IoT device, thus protecting user's privacy since sensors can directly record data about users or devices. The idea of FL lies in the following: each IoT device processes the necessary amount of

data and forwards the finally extracted information through the network, whereby the raw data remains protected and does not leave the devices. Data processing through the use of artificial intelligence in the device itself can also be limited to the available data set, and for this reason, parallel learning between multiple devices and their mutual information exchange can be realized. In this way, the means to relieve the network resources is also created, which can be a limiting factor of the system, if not resolved, especially for low bandwidth IoT networks. However, several potential limitations have been identified for the full implementation of FL, which must be taken into account when these systems are designed and built. In the process of collecting and processing data on the device itself, there must be appropriate local resources that can support the collected data in terms of storage, handling and processing. The data transmission network must have adequate bandwidth so that there is no congestion or information delay in mutual communication between devices and communication with the central part of the system in the cloud. In a real environment, there is also a possibility that certain devices become temporarily absent from the network due to physical obstacles or malicious (i.e. enemy) attacks. However, the data handling capacities of various IoT devices are usually not uniform, and the dynamics of data distribution from individual devices is not uniform in the system. Thus, it is preferable to solve the mentioned potential problems during the system design and construction phase.

In the last few years, a lot of effort has been put into the research and development of IoT technology due to the need to improve military capabilities. In this effort, the one of the main task was created due to the fact that the generation of large amounts of data by IoT devices requires the protection of confidential data. Yet, blockchain technology allow IoT devices to exchange collected data with each other or send it to a cloud server safely and reliably (Fotia et al, 2023). Thus, blockchain-based solutions represents the decentralization of data storage, processing and distribution quickly and securely online without the need for a trusted authority. Given that in practice there is a need for both centralized and decentralized data storage, so-called hybrid blockchain platforms were developed, which achieved the existence of public and private blockchains in the same project, where anyone can access and view public data, and protected data cannot be accessed without the predefined permissions (Alkhateeb et al, 2022). Also, the hybrid blockchain platform is customizable so that the administrator can define which transactions will be public or who can participate in the specific blockchain. It should be also noticed that the research in this area

currently moves in several directions. The application of artificial intelligence for monitoring or control may have limitations in terms of energy efficiency, depending on the type of device. On the other hand, the interoperability requirements between two or more hybrid blockchains are not simple. Therefore, it is necessary to implement an effective mechanism of communication in order to simplify this process. Accordingly, data security for hybrid blockchains in IoT environments requires further research due to the existence of a broad range of sensitive and confidential data.

The military application of IoT technology is considered and developed in order to improve combat effectiveness and effective management of the resources. When IoT technology is used for defense applications it is often called the Internet of Battlefield Things (IoBT), (Wang et al, 2018b). In Internet of Battlefield Things, application requires the processing of a large amount of data, the validity and accuracy of which directly affect the quality of the military decision-making process. The existing architecture of data transmission and information on the battlefield is not able to support the current and future requirements of data collection and processing, which is why the IoBT has found its place and role in modern defense applications.

The first IoBT architecture was based on the data processing center placed in the cloud, the so-called "battle cloud", located far from the combat touch of tactical units. As such, it was highly susceptible to the communication congestion due to the bandwidth limitations and information transfer delays (i.e. end-to-end latency). Given that all data flows into one center, this center, as well as the associated communications links, would certainly become a target of attacks as such. Additionally, in practice there is a possibility of impairing the robustness of the data transmission network in case of deliberate attacks by the enemy due to the reduction of the number of one-way edges and nodes in the network (Feng et al, 2020). In order to overcome the mentioned problem, the idea of inserting another layer of the so-called "battle clouds-fog" came up (Bonomi et al, 2012; Hossain et al, 2019). However, due to heterogeneous equipment, load and delay in a distributed network, it is necessary to perform load balancing in order to allocate resources for assigned tasks, which is one of the important areas of the current research (Wang et al, 2018a).

The ability of IoT technology to create effects in the physical world through the use of actuators and other autonomous physical platforms enables management in the air, on the ground, at the sea and in the space through the cyber interfaces, using the intelligent command and

control (C2) (Russell et al, 2019). This means that the IoBT, in addition to provided help in the execution of the primary task, also makes valuable predictions and can suggest continuity in the action. These are integrated into the multi-dimensional environment through IoTs autonomous platforms, on the land, at the sea and in the air, with the intelligent command and control systems (C2), which ensure the execution of tasks and the fulfillment of the final desired state by enabling the monitoring of a wide range of human activities in a dynamic environment that the existing command and control systems are not able to provide (Russell & Abdelzaher, 2018). Due to the necessity to transfer a large amount of data, it is also necessary to build an appropriate telecommunications infrastructure that will support the C2 system. In that area, the research trend is the transfer of data from the still incompletely used 5G network capabilities to the new level of the 6G network (Qadir et al, 2023).

However, the question of the distribution of responsibilities between the commanders and the machines (devices) is also raised. Through the use of IoT technologies and C2 intelligent systems, a quick reconfiguration of forces and resources can be enabled in order to achieve the desired effect to satisfy the information the commander's needs to the unexpected resource losses or in the case of unfavorable land and weather environment (Abdelzaher et al, 2018a). This will certainly require changes in the operational concept, doctrine, tactics and structure of military units, which is the subject of further research in the subject area.

Decision making in the military systems is a hierarchical one and takes a certain amount of time. The needs of the practice are that this time should be as short as possible and the decision should be made in timely manner. Thus comes the need for a compromise between the delegation of decision-making authority and the predictability of risk, given that the higher level of delegation means the lower predictability level of aggregate behavior. The basic question how to design (place) the optimal solution between the human and an algorithm present one of the important directions of research in the subject area. IoT services will certainly contribute to a greater degree of automation and improvement of the quality of military decisions on the battlefield, especially in the conditions of unexpected scenarios in an unpredictable hostile environment, thus facilitating the reduction in both human and material losses in the operations. The main question to be considered here is the establishment of the relationship between reliability and artificial intelligence. A prerequisite for artificial intelligence is deployment of machine learning techniques, which inherently requires human-created

models of the specific environments. Therefore, in order to design the sensitive and safety-critical decisions, learning algorithms based on the deep neural networks are currently being researched, which must enable the flexibility of the structure that functions in an unknown environment and the generation of training and testing data in order to obtain guarantees, i.e. to manage risk (Abdelzaher et al, 2018b). Reducing the physical presence of a person in hostile environments and increasing the toughness of assets on the battlefield requires the necessary level of embedded intelligence able to detect and predict the behavior of the enemy, to define the necessary level of response to the threat, to properly adapt to sudden changes in the environment, to recover in case of attacks and losses, and to support continuous learning.

In the next several subsections, the most important IoT military application areas will be presented.

IoT-based surveillance applications

The IoT systems played a significant role in the field of surveillance and control of soldiers and units. The main characteristic of the so-called Military Assistance and Surveillance System (MASS) is to enable network-centric warfare, which requires linking individuals and units with unit command. As described in the paper (Raja & Bagwari, 2018), the MASS enables the reception and transmission of data, such as navigation elements, atmospheric conditions, state of health, command information, transmission of data from other devices (such as rangefinders) in real time, via a portable device with a user interface. In addition to these devices, the soldiers' equipment includes sensors for collecting data and recording the environment, and the transparent displays that allow the soldier to observe data in the form of augmented reality so that they do not require the soldier's attention to be diverted from the battlefield. In addition to the above, it is possible to connect several devices to the system, such as ammunition counters. With the help of the MASS, unit commanders have the ability to visualize the deployment of forces and to collect data independently of the engagement of individuals, which certainly makes it easier to make faster and better decisions related to the battlefield.

The application of IoT technology in the provision of smart cities through the services of traffic control, surveillance, management, police, etc., has also been transferred to the public security and defense sectors. Supervision and control of military facilities and facilities of importance for the national security is the application area of the systems in which

various data is collected and processed with the help of video cameras, microphones and various other sensors, while the protection and warning system are activated accordingly (Pahal et al, 2018). In practice, given that one sensor can detect a certain phenomenon under certain conditions, layering and synchronization of sensory data must be done in order to make more accurate decisions about the current state and the future activities. The system should also be capable of learning based on the past events, so that it can recognize false alarms and then performs modeling to predict the dynamic dependence between different entities in the overall picture. One important research direction in this area is the issue of smart reasoning and detection of image content in order to recognize a suspicious content (event) in real time.

One way to overcome the challenge related to the need to process a large amount of data in real time is based on the application of multilayer neural networks using the centralized (cloud) computing and the edge computing, as describe in (Zhao et al, 2019), where data is primarily processed at the edge devices and not on central servers. In this way, we can achieve significant savings in terms of deployed network resources, information delay is significantly reduced, and data leakage from source to source is prevented.

In the defense and security sector, the primary role is certainly played by the human itself, with his regulated characteristics and tendencies. However, that person must possess the required degree of integrity to perform important state and military affairs. Given that a person in his daily life does not carry out activities according to a checklist, but routinely performs many free activities, there is a possibility of non-intentional, and sometimes intentional, leakage of data and information of importance to the defense system. Preventing the outflow of confidential data and information is one of the areas of application of IoT (Fongen & Mancini, 2015) technology aimed at monitoring the various activities and behavior of personnel in the defense and security sector in their daily activities, with the aim of information leakage prevention. As an example, the terrorist attacks in Paris, India and the USA were possible due to security failures and the leakage of classified information through defense personnel (Bhatia & Sood, 2018), and it is concluded that the integrity of each individual directly affects national security.

The paper (Bhatia & Sood, 2018) presents a 4-phase IoT-based model for assessing staff activity. The proposed model is based on the collection of information on staff activities, analysis information and determining its integrity with regard to the national security. Activity

quantification is done in the form of determining the degree of integrity as an index that is compared with a defined value threshold. The proposed model was tested on multiple datasets and proved to be effective in terms of estimating the integral behavior of defense personnel. One of the research challenges in this area is the heterogeneity of input data, which would be a guideline for further research in the subject area.

Finally, one of the applications of IoT technology is the surveillance of robotic unmanned platforms used for military purposes (Telkar & Gadgay, 2020), such as aircraft, underwater and land vehicles. These platforms are equipped with sensors for detecting the primary target, such as mines, and other sensors for orientation, detection of atmospheric conditions, environmental imaging, etc. By recognizing the specific shape, the platform makes a decision about the upcoming action, movement, effect of weapons systems, etc. The primary data processing takes place on the crew platform, while the secondary processing takes place in the monitoring and supervision center. The application of the IoT concept on humanoid robots is particularly interesting, which is an area of interest for technologically developed countries.

Enemy localization and target detection

Locating the enemy on the battlefield is a question that is of great interest to commanders in order to direct forces and assets in combat operations. The collection of data on terrain, weather, the state of one's own units and the enemy through sensor networks has been discussed in several works (Akman et al, 2018). Data collection and location prediction was done through acoustic sensors and the application of the triangulation method as explained in (Sallai et al, 2011). There are also solutions for collecting data using helmet-mounted microphones which use time and angle of sound detection to determine the location of the enemy. However, data processing requirements have grown over time, such as to lower energy consumption, suppress echo signals, improve sensor calibration quality, increase detection distance, deploy information on weather conditions, etc. All these requirements took their toll, which is why most current and foreseen solution are switched to the IoT approach. Modern solutions also use micro electro-mechanical sensors (MEMS) which, among others, have GPS (Global Positioning System) receivers for determining the location of soldiers. The location of the enemy is determined according to the direction and direction of fire of own forces. Also, depending on the armament, laser rangefinders are used. The data is usually not processed at the source, but is distributed

to the application server where it is processed and returned to the user in the form of information, which creates the high demands related to the end-to-end delays.

Situation awareness

Military operations are carried out in complex environments which are highly dynamic and not quite predictable. The introduction of IoT technology significantly contributes to the exchange of data and information quality and makes it easier for commanders to make decisions and achieve a greater degree of efficiency (Michalski & Bernat, 2019). However, the integration of a large number of heterogeneous sensors for monitoring purposes contributes to the significant increase in the risk of cyber-attacks. Thus, the level of trust in incoming data presents an important challenge for researchers in this area (Glowacka et al, 2015). Certain entities in the network can become hostile, due to the capture by the enemy, and thus interfere with the operation of the network and the entire infrastructure. Therefore, given that wireless transmission is involved, special attention must be paid to the design and implementation of security mechanisms, encryption algorithms, secure routing protocols (especially due to entity mobility), and trust assessment. Trust assessment should be based on direct observations and received recommendations. Based on trust assessment, malicious and unintentional intrusions are detected and adequate measures are taken in order to prevent and eliminate threats. Trust assessment can be performed in several ways, such as: by direct monitoring (Sun et al, 2014), assessment based on received data, by weighting the evaluation function based on the history of entity behavior, or on the basis of exchange of certificates and risk assessment.

Air space applications

Airspace management requires strict coordination of aircraft by location and time in order to achieve the required level of flight safety. In combat operations, in addition to the own ones, the enemy aircraft of all types must be considered, while there is also the use of artillery armament, which additionally limits the corridors of movement for the own aircraft. Given that the use of enemy assets is stochastic in time, it is necessary to provide the pilot with the timely information about the regime and route of movement. The key limitations in the airspace management in the area of operations are (Singh et al, 2019):

- vertical separation, when aircraft have a low flight profile to avoid detection by the enemy,
- avoiding a collision with one's own armament during the over flight of one's own forces,
- avoiding collision with own aircraft, and
- unforeseen conflict with enemy aircraft.

Timely information, warning or command, is of crucial importance for pilots. Through the use of IoT technology, data collection, processing and distribution to interested parties, primarily pilots, will enable more efficient management of flight safety and overcoming most of the before mentioned problems. The processing of data collected from ground forces and air forces is performed centrally, in real time, so that the coordination of all subjects in the area of operation is enabled. Visualization of space through virtual or augmented reality, as part of suggestion of maneuvers process, will enable a new approach in solving highly demanding tactical situations in airspace.

Military health

A special field of application of the Internet of military things is the field of health care of soldiers. However, from justified works, the impact of electromagnetic radiation in the network itself on humans was also investigated (Nasim & Kim, 2019) where the research identified the safety distances of radiation sources necessary to maintain human health. In this area, the triage on the battlefield represents an extremely important task on which highly depends the degree of survival of soldiers due to wounds, injuries or illnesses. For this purpose, special sensors were developed with the task of collecting data on individuals in order to make proper decisions about the future treatment, namely Immediate Treatment, Delayed Treatment, Minimal Treatment or Expectant Treatment (Dyk et al, 2017). Besides the traditional triage on the battlefield, monitoring the health condition of soldiers in real time and responding to critical events in a timely manner has become particularly important (Reyes et al, 2017). For this reason, so-called medical networks are researched and developed, which should enable viable connections of devices and sensors from different sensor manufacturers, secure data transmission, the possibility of calling the call center for consultation, and also counseling between doctors in the field and specialists via telemedicine (Jarmakiewicz et al, 2016).

Another application of the IoT in military health is searching the terrain and finding the injured and sick soldiers, which, among other, requires special data transmission conditions to protect soldiers from the enemy. In addition to the requirements for authentication and biometrics of the soldiers, it is required that smart devices deployed possess enough energy to enable secure and reliable communication between soldiers and the nodes of the network, which must be maintained long enough, i.e. until the arrival of the care and evacuation team (Kang et al, 2020).

Military logistics

The application of the Internet of Things in military logistics has a very wide application in unifying logistical functional areas (supply, maintenance of weapons and military equipment, traffic and transport, quartermaster's office, healthcare, etc.) and in the realization of process functions (Zhong et al, 2012). The concept of network organization in the military logistics system is based on the organization of logistics system monitoring, and most often consists of several branches that monitor individual logistics functions due to different requirements in terms of data collection and analytic, as well as due to different ways of data generation (Wang et al, 2018a, Wei et al, 2012). In addition to collection, processing and distribution of data and information within the individual logistics functions, an important area of the application of the IoT is in the field of logistics of the asset itself. This enables the end user to initiate actions in order to preserve the operational capabilities of the weapon itself or mass service for a group of assets (Liang et al, 2014).

The construction of the logistics system is directly related to the construction of weapons. Project bureaus and institutes use so-called Product life-cycle management (PLM) software tools that enable connections at the national and international level with potential future manufacturers of the asset itself, manufacturers of components and spare parts, distributors, etc., for which the IoT infrastructure is necessary (Rondon et al, 2022).

Monitoring the flow of the production or the asset overhaul requires a very wide range of data and analytics to avoid downtime and to reduce business efficiency. For this purpose, IoT networks are being developed with the aim to monitor workforce capacity, consumption and demand for spare parts and consumables, energy, material distribution, work control and the entire quality system, etc. Since in many production plants these are realized manually, this actually presents the perfect area of the

application of the loBT in accordance with the visions of industry 4.0 (Salih et al, 2022).

For the successful management of weapons and military equipment in combat units, it is necessary to monitor the state of assets in real time, and to initiate maintenance activities in order to maintain the required level of operational availability of units. For this purpose, electronic identity cards of asset are being developed to record the state and status of particular assets, embedded computers inside equipment that collect and process data on the state of individual systems are deployed, as well as assemblies and parts which indicate a timely reaction to the user (Liu et al, 2022). For certain assets, devices are installed that alert the maintenance service in real time in order to shorten the response time in the so-called condition-based maintenance concept. Decision-makers in the function of maintenance and overhaul need timely knowledge about the state of maintenance capacity, both in the background and in the operational area, in the short term or for the operation as a whole.

Logistics personnel require information on the state of reserves of all classes of materials, the position of distributors, the movement of convoys, storage conditions, the possibility of delivery and evacuation of assets, the health status of personnel, etc. Finally, the question arises as to how to allocate logistics capacities for the optimal satisfaction of user needs in accordance with the place and role in combat operations. For such a thing, it is necessary to apply experiential and analytical tools of artificial intelligence based on multi-criteria decision making, which humans as individuals cannot do as successfully as machines do (Lei, 2022).

All the aforementioned areas are the ones in which modern armed forces invest significant resources in order to raise the level of effectiveness and efficiency of combat units based on loBT technology deployment.

Conclusion

The military application of IoT technology is considered and developed in order to improve combat effectiveness and effective management of the resources based on a large amount of data, the validity and accuracy of which directly affect the quality of the military decision-making process. The existing architecture of data transmission and information on the battlefield is not able to support the current and future requirements of data collection and processing, which is why the loBT has found its place and role in modern defense applications.

Given that all data flows into one center, such a center, as well as the associated communications links, would certainly become a target of attacks as such.

The ability of IoT technology to create effects in the physical world through the use of actuators and other autonomous physical platforms enables management in the air, on the ground, at the sea and in the space through cyber interfaces, using intelligent command and control. Due to the necessity to transfer a large amount of data, it is also necessary to build an appropriate telecommunications infrastructure that will support the C2 system. In that area, the research trend is the transfer of data from the still incompletely used 5G network capabilities to the new level of the 6G network.

Through the use of IoT technologies and C2 intelligent systems, the information needs of a commander can be satisfied in order to enable quick reconfiguration of forces and resources in response to unexpected resource losses or in case of unfavorable terrain and weather conditions. This will certainly require changes in the operational concept, doctrine, tactics and structure of military units, which is the subject of further research in the subject area.

References

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B., Nahrstedt, K. et al. 2018a. Toward an Internet of Battlefield Things: A Resilience Perspective. *Computer*, 51(11), pp.24-36. Available at: <https://doi.org/10.1109/MC.2018.2876048>.

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B., Nahrstedt, K. et al. 2018b. Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT. In: *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, pp.1129-1138, July 02-06. Available at: <https://doi.org/10.1109/ICDCS.2018.00112>.

Akman, Ç., Sönmez, T., Özüğür, Ö., Başlı, A.B. & Kemal Leblebicioğlu, M. 2018. Sensor fusion, sensitivity analysis and calibration in shooter localization systems. *Sensors and Actuators A: Physical*, 271, pp.66-75. Available at: <https://doi.org/10.1016/j.sna.2017.12.042>.

Alkhateeb, A., Catal, C., Kar, G. & Mishra, A. 2022. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors*, 22(4), art.number:1304. Available at: <https://doi.org/10.3390/s22041304>.

Bhatia, M. & Sood, S.K. 2018. Internet of Things based activity surveillance of defence personnel. *Journal of Ambient Intelligence and Humanized Computing*, 9, pp.2061-2076. Available at: <https://doi.org/10.1007/s12652-017-0507-3>.

Bonomi, F., Milito, R., Zhu, J. & Addepalli, S. 2012. Fog computing and its role in the internet of things. In: *MCC '12: Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, Helsinki, Finland, pp.13-16, August 17. Available at: <https://doi.org/10.1145/2342509.2342513>.

Dyk, M., Chmielewski, M. & Najgebauer, A. 2017. Combat triage support using the Internet of Military Things. In: *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Prague, Czech Republic, pp.835-842, September 03-06 [online]. Available at: <https://ieeexplore.ieee.org/abstract/document/8104646> [Accessed: 5 March 2023].

Feng, Y., Li, M., Zeng, C. & Liu, H. 2020. Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. *Entropy*, 22(10), art.number:1166. Available at: <https://doi.org/10.3390/e22101166>.

Fongen, A. & Mancini, F. 2015. Integrity attestation in military IoT. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, pp.484-489, December 14-16. Available at: <https://doi.org/10.1109/WF-IoT.2015.7389102>.

Fotia, L., Delicato, F. & Fortino, G. 2023. Trust in Edge-based Internet of Things Architectures: State of the Art and Research Challenges. *ACM Computing Surveys*, 55(9), pp.1-34. Available at: <https://doi.org/10.1145/3558779>.

Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. & González-López, M. 2016. A Review on Internet of Things for Defense and Public Safety. *Sensors*, 16(10), art.number:1644. Available at: <https://doi.org/10.3390/s16101644>.

Głowacka, J., Krygier, J. & Amanowicz, M. 2015. A trust-based situation awareness system for military applications of the internet of things. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, pp.490-495, December 14-16. Available at: <https://doi.org/10.1109/WF-IoT.2015.7389103>.

Hossain, M.S., Ramli, M.R., Lee, J.M. & Kim, D.-S. 2019. Fog Radio Access Networks in Internet of Battlefield Things (IoBT) and Load Balancing Technology. In: *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), pp.750-754, October 16-18. Available at: <https://doi.org/10.1109/ICTC46691.2019.8939722>.

Jarmakiewicz, J., Parobczak, K. & Maślanka, K. 2016. On the Internet of Nano Things in healthcare network. In: *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, pp.1-6, May 23-24. Available at: <https://doi.org/10.1109/ICMCIS.2016.7496572>.

Kang, J.J., Yang, W., Dermody, G., Ghasemian, M., Adibi, S. & Haskell-Dowland, P. 2020. No Soldiers Left Behind: An IoT-Based Low-Power Military

Mobile Health System Design. *IEEE Access*, 8, pp.201498-201515. Available at: <https://doi.org/10.1109/ACCESS.2020.3035812>.

Lei, N. 2022. Intelligent logistics scheduling model and algorithm based on Internet of Things technology. *Alexandria Engineering Journal*, 61(1), pp.893-903. Available at: <https://doi.org/10.1016/j.aej.2021.04.075>.

Liang, F., Bai, H.W. & Liu, G.D. 2014. Application of internet of things in military equipment logistics. *Applied Mechanics and Materials*, 556-562, pp.6723-6726. Available at: <https://doi.org/10.4028/www.scientific.net/AMM.556-562.6723>.

Liu, C., Su, Z., Xu, X. & Lu, Y. 2022. Service-oriented industrial internet of things gateway for cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, 73, art.number:102217. Available at: <https://doi.org/10.1016/j.rcim.2021.102217>.

Michalski, D. & Bernat, P. 2019. Internet of Things in Air and Missile Defence A System Solution Concept. In: *2019 International Conference on Military Technologies (ICMT)*, Brno, Czech Republic, pp.1-5, May 30-31. Available at: <https://doi.org/10.1109/MILTECHS.2019.8870070>.

Nasim, I. & Kim, S. 2019. Human EMF Exposure in Wearable Networks for Internet of Battlefield Things. In: *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, pp.1-6, November 12-14. Available at: <https://doi.org/10.1109/MILCOM47813.2019.9020889>.

Pahal, N., Mallik, A. & Chaudhury, S. 2018. An Ontology-based Context-aware IoT Framework for Smart Surveillance. In: *SCA '18: Proceedings of the 3rd International Conference on Smart City Applications*, Tetouan, Morocco, art.number:69, pp.1-7, October 10-11. Available at: <https://doi.org/10.1145/3286606.3286846>.

Pokorni, S.J. 2019. Reliability and availability of the Internet of things. *Vojnotehnički glasnik/Military Technical Courier*, 67(3), pp.588-600. Available at: <https://doi.org/10.5937/vojtehg67-21363>.

Qadir, Z., Le, K.N., Saeed, N. & Munawar, H.S. 2023. Towards 6G Internet of Things: Recent advances, use cases, and open challenges. *ICT Express*, 9(3), pp.296-312. Available at: <https://doi.org/10.1016/j.ict.2022.06.006>.

Raja, P. & Bagwari, S. 2018. IoT Based Military Assistance and Surveillance. In: *2018 International Conference on Intelligent Circuits and Systems (ICICS)*, Phagwara, India, pp.340-344, April 19-20. Available at: <https://doi.org/10.1109/ICICS.2018.00076>.

Reyes, Ch.R.P., Vaca, H.P., Calderón, M.P., Montoya, L. & Aguilar, W.G. 2017. MilNova: An approach to the IoT solution based on model-driven engineering for the military health monitoring. In: *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Pucon, Chile, pp.1-5, October 18-20. Available at: <https://doi.org/10.1109/CHILECON.2017.8229585>.

Rondon, L.P., Babun, L., Aris, A., Akkaya, K. & Uluagac, A.S. 2022. Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc*

Networks, 125, art.number:102728. Available at: <https://doi.org/10.1016/j.adhoc.2021.102728>.

Russell, S. & Abdelzaher, T. 2018. The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making. In: *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, pp.737-742, October 29-31. Available at: <https://doi.org/10.1109/MILCOM.2018.8599853>.

Russell, S., Abdelzaher, T. & Suri, N. 2019. Multi-Domain Effects and the Internet of Battlefield Things. In: *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, pp.724-730, November 12-14. Available at: <https://doi.org/10.1109/MILCOM47813.2019.9020925>.

Salih, K.O.M., Rashid, T.A., Radovanovic, D. & Bacanin, N. 2022. A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors*, 22(3), art.number:730. Available at: <https://doi.org/10.3390/s22030730>.

Sallai, J., Lédeczi, A. & Völgyesi, P. 2011. Acoustic shooter localization with a minimal number of single-channel wireless sensor nodes. In: *SenSys '11: Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, Seattle, Washington, pp.96-107, November 1-4. Available at: <https://doi.org/10.1145/2070942.2070953>.

Singh, K., Tripathi, G., Chullai, G.A., Kumar, J. & Kumar, P. 2019. Future Battlefield Air Space Management: An Internet of Things (IoT) Based Framework. In: *2019 International Conference on Signal Processing and Communication (ICSC)*, Noida, India, pp.15-21, March 7-9. Available at: <https://doi.org/10.1109/ICSC45622.2019.8938280>.

Sun, Z.F., Ma, X. & Sun, D.X. 2014. Construction of the Air Offensive Operation Battlefield Support System based on the Internet of Things Technology. *Advanced Materials Research*, 834-836, pp.1873-1876. Available at: <https://doi.org/10.4028/www.scientific.net/AMR.834-836.1873>.

Telkar, A.K. & Gadgay, B. 2020. IoT Based Smart Multi Application Surveillance Robot. In: *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp.931-935, July 15-17. Available at: <https://doi.org/10.1109/ICIRCA48905.2020.9183289>.

Vermesan, O. & Friess, P. (Eds.) 2014. *Internet of Things Applications - From Research and Innovation to Market Deployment, 1st edition*. New York: River Publishers. Available at: <https://doi.org/10.1201/9781003338628>.

Wang, J., Cao, L., Shen, Y. & Zheng, G. 2018a. Research on Design of Military Logistics Support System Based on IoT. In: *2018 Prognostics and System Health Management Conference (PHM-Chongqing)*, Chongqing, China, pp.829-832, October 26-28. Available at: <https://doi.org/10.1109/PHM-Chongqing.2018.00148>.

Wang, Y., Ren, Z., Zhang, H., Hou, X. & Xiao, Y. 2018b. "Combat Cloud-Fog" Network Architecture for Internet of Battlefield Things and Load Balancing Technology. In: *2018 IEEE International Conference on Smart Internet of Things*

(SmartIoT), Xi'an, China, pp.263-268, August 17-19. Available at: <https://doi.org/10.1109/SmartIoT.2018.00054>.

Wei, X., Wan, Y., Ding, H. & Xu, H. 2012. Conception of Intelligent Military Logistics Based on Internet of Things Technology. In: *ICLEM 2012: Logistics for Sustained Economic Development—Technology and Management for Efficiency*, Chengdu, China, pp.371-375, October 8-10. Available at: <https://doi.org/10.1061/9780784412602.0059>.

Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B. & Avestimehr, A.S. 2022. Federated learning for the internet of things: Applications, challenges, and opportunities. *IEEE Internet of Things Magazine*, 5(1), pp.24-29. Available at: <https://doi.org/10.1109/IOTM.004.2100182>.

Zhao, Y., Chen, Q., Cao, W., Jiang, W. & Gui, G. 2019. Deep Learning Based Couple-like Cooperative Computing Method for IoT-based Intelligent Surveillance Systems. In: *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, pp.1-4, September 08-11. Available at: <https://doi.org/10.1109/PIMRC.2019.8904229>.

Zhong, X.-H., Ding, H., Zhang, X.-M. & Zhang, F. 2012. Research on the Construction of the IOT System in the Field of Military Logistics. In: *ICLEM 2012: Logistics for Sustained Economic Development—Technology and Management for Efficiency*, Chengdu, China, pp.376-382, October 8-10. Available at: <https://doi.org/10.1061/9780784412602.0060>.

Zhu, L., Majumdar, S. & Ekenna, C. 2021. An invisible warfare with the internet of battlefield things: A literature review. *Human behavior and emerging technologies*, 3(2), pp.255-260. Available at: <https://doi.org/10.1002/hbe2.231>.

Интернет вещей в военном применении

Влада С. Соколович^а, корреспондент, Горан Б. Маркович^б

^а Университет обороны в г. Белград, Военная академия, Департамент логистики, Белград, Республика Сербия

^б Белградский университет, факультет электротехники, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 47.01.29 Информационная деятельность
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Термин „Интернет вещей“ (IoT) обычно относится к корпоративной сети подключенных устройств и технологии, которая облегчает связь между этими устройствами и облаком, а также между самими устройствами. Концепция Интернета вещей в последнее время рассматривается и применяется как при проектировании систем, предназначенных для распределения данных и информации между разнородными устройствами с целью

повышения эффективности деятельности и принятия решений. Интернет вещей обеспечивает мониторинг энергетики и цепочек поставок, координацию производства, оптимизацию производительности оборудования, транспортировку, здравоохранение, а также улучшает охрану труда и повышает безопасность. В дополнение к интеллектуальным устройствам технология Интернета вещей также позволяет подключать различные датчики в качестве источника данных о различных физических явлениях. Таким образом, основываясь на полученной информации, можно управлять работой устройств, делать прогнозы, принимать решения и пр. В данной статье анализируются конкретные области применения Интернета вещей в секторе обороны и безопасности с целью выявления возможностей применения современных технологий в повышении оборонного потенциала государства и определения направлений будущих исследований в предметной области.

Методы: В данной статье были применены методы контент-анализа текущих исследований, а затем с помощью дедуктивного метода были сделаны выводы о будущих направлениях развития технологии Интернета вещей

Результаты: Был проведен детальный анализ предыдущих и текущих исследований в секторе обороны и безопасности, а также даны потенциальные направления будущих исследований в области Интернета вещей с целью повышения оперативных возможностей вооруженных сил.

Выводы: Сервис Интернета вещей, безусловно, будет способствовать большей степени автоматизации и повышению качества военных решений на поле боя, особенно в условиях неожиданных сценариев в непредсказуемой вражеской среде, способствуя тем самым снижению как человеческих, так и материальных потерь в ходе военных действий.

Ключевые слова: интернет вещей, общественная безопасность и защита населения, приложения интернета вещей, локализация и обнаружение целей, военная логистика.

Интернет ствари у војној примени

Влада С. Соколовић^а, аутор за преписку, Горан Б. Марковић^б

^а Универзитет одбране у Београду, Војна академија, Катедра логистике, Београд, Република Србија

^б Универзитет у Београду, Електротехнички факултет, Београд, Република Србија

ОБЛАСТ: телекомуникације, информационе технологије
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод: Појам интернет ствари (ИС) најчешће се односи на свеукупну мрежу повезаних уређаја и технологија која погодује комуникацији између ових уређаја и централних елемената мреже у „облаку” (cloud), као и између ових уређаја. Концепт ИС се од недавно разматра и примењује као адекватан за развој система чија је намена размена података и информација између хетерогених уређаја ради унапређења ефикасности и ефективности пословања и доношења одлука. Интернет ствари омогућава праћење енергије и ланца снабдевања, координацију производње, оптимизацију перформанси опреме, транспорт, јавно здравље и побољшава безбедност и здравље радника. Поред паметних уређаја, ИС технологија омогућава и повезивање различитих сензора као извора података о различитим физичким појавама, а на основу добијених информација могуће је контролисати рад уређаја, предвиђати, доносити одлуке, итд. Анализирају се специфичне области примене ИС у сектору одбране и безбедности, како би се идентификовале могућности примене савремених технологија у подизању одбрамбеног потенцијала државе и дефинисали правци будућих истраживања. Методе: Примењене су методе анализе садржаја актуелних истраживања, а затим су дедуктивном методом донети закључци о будућим правцима развоја ИС технологије.

Резултати: Извршена је детаљна анализа досадашњих и текућих истраживања у сектору одбране и безбедности и предложени потенцијални правци будућих истраживања ИС ради повећања оперативних способности оружаних снага.

Закључак: Услуге интернет ствари ће свакако допринети већем степену аутоматизације и побољшању квалитета војних одлука на бојном пољу, посебно у условима неочекиваних сценарија у непредвидивом непријатељском окружењу. Тиме ће се смањити људски и материјални губици у операцијама.

Кључне речи: интернет ствари, одбрана и јавна безбедност, апликације за интернет ствари, локализација и детекција циљева, војна логистика.

Paper received on / Дата получения работы / Датум пријема чланка: 09.03.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 28.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 29.11.2023.

© 2023 The Authors. Published by *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / *Vojnotehnički glasnik / Military Technical Courier*» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / *Vojnotehnički glasnik / Military Technical Courier* (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



Enabling digital growth through continuous education of project managers: a framework for collaborative, complementary, sustained, and simultaneous learning in software engineering organizations

Srđan V. Atanasijević^a, Monika N. Zahar^b, Dejan D. Rančić^c,
Ivan B. Vulić^d, Tatjana J. Atanasijević^e

^a University of Kragujevac, Kragujevac, Republic of Serbia,
e-mail: srdjan.atanasijevic@kg.ac.rs, **corresponding author**,
ORCID iD: <https://orcid.org/0000-0003-4414-1799>

^b University of Kragujevac, Kragujevac, Republic of Serbia,
e-mail: monikazahar@gmail.com,
ORCID iD: <https://orcid.org/0000-0001-7620-9562>

^c University of Niš, Faculty of Electronic Engineering,
Department of Computer Science, Niš, Republic of Serbia,
e-mail: dejan.rancic@elfak.ni.ac.rs,
ORCID iD: <https://orcid.org/0000-0002-3579-5654>

^d University of Defence in Belgrade, Belgrade, Republic of Serbia,
e-mail: ivan.vulic@mod.gov.rs,
ORCID iD: <https://orcid.org/0000-0002-5161-5422>

^e University of Kragujevac, Kragujevac, Republic of Serbia,
e-mail: tatjana.atanasijevic@icloud.com,
ORCID iD: <https://orcid.org/0000-0001-6359-1723>

DOI: 10.5937/vojtehg71-46100; <https://doi.org/10.5937/vojtehg71-46100>

FIELD: computer sciences, IT

ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: This paper introduces a novel PMO EDUCT framework that encompasses Collaborative, Complementary, Sustained, and Simultaneous learning explicitly tailored for the dynamic landscape of software engineering.

This paper contributes to the ongoing discourse on education and professional development in the digital era by illuminating the challenges faced, the framework developed, and the measurable outcomes achieved. The presented framework underscores the need for agility, adaptability, and a relentless pursuit of knowledge as fundamental tenets for success in an ever-evolving landscape.

Methods: Focusing on a large software engineering organization, this study explores the multifaceted aspects of project management education, methodology enhancement, and team optimization. The proposed methodology combines qualitative and quantitative approaches to explore the educational process area in a global organization and generate a flexible and measurable framework to improve corporate knowledge growth. The framework aims to provide learners the most flexibility about learning paths, schedules, collaboration, and best practice exchange while guaranteeing proper alignment with frequent market changes and emerging PM skills.

Results: Findings indicate that personalised, continuous learning, facilitated through collaborative environments and custom-tailored content, yields significant benefits. Through analysis of key performance indicators (KPIs), this study showcases improved project onboarding, enhanced team collaboration, and the cultivation of a culture of innovation.

Conclusion: This paper presents the PMO EDUCT framework that organizations can use to create a learning culture and empower their employees to succeed in the constantly evolving field of software development. By adopting collaborative, complementary, sustained, and simultaneous learning principles, organizations can develop a workforce with the essential skills of critical thinking, collaboration, and adaptability necessary for success in the digital era.

Key words: software engineering, learning framework, digital transformation, project management, knowledge competences, agile methodology, learning strategy, competency building.

Introduction

The rapid and transformative wave of digitalization has ushered in an era of unprecedented change, challenging traditional business models and reshaping industries across the globe. Organizations are faced with the imperative to adapt, innovate, and continuously evolve to remain competitive in this dynamic landscape. For software engineering companies, the impact of this digital transformation is particularly profound, as their core revolves around technology and innovation (Atanasijevic, 2016). The digital age has disrupted business models and redefined the skills and competencies required of professionals in the software engineering domain.

Organizations must rethink their growth, development, and education strategies in response to these transformative shifts. The traditional learning and skill acquisition paradigms no longer suffice in a landscape characterized by rapid technological advancements, frequent market changes, and evolving customer expectations. Within this context, we

introduce a comprehensive framework for continuous education and knowledge growth tailored to the intricacies of the software engineering industry. This framework embodies the principles of Collaborative, Complementary, Sustained, and Simultaneous learning, designed to empower professionals to thrive in the digital era.

In this paper, we delve into the nuances of this framework and its application within a large software engineering organization. We explore the multifaceted realm of project management education, methodology enhancement, and team optimization – critical pillars in pursuing digital growth. Leveraging qualitative and quantitative methodologies, we present a holistic approach that equips professionals with the requisite skills and fosters a culture of collaboration, innovation, and continuous improvement.

The subsequent sections of this paper detail the foundation of our framework, the context within which it operates, and the methodology employed to assess its effectiveness. We highlight the significance of tailored and personalized learning, the benefits of collaborative environments, and the measurement of outcomes through a carefully defined set of key performance indicators (KPIs). Through this study, we aim to provide insights and a blueprint for software engineering organizations seeking to embrace the digital age and harness the power of continuous education to drive growth, innovation, and lasting success.

This paper contributes to the ongoing discourse on education and professional development in the digital era by illuminating the challenges faced, the framework developed, and the measurable outcomes achieved. The presented framework underscores the need for agility, adaptability, and a relentless pursuit of knowledge as fundamental tenets for success in an ever-evolving landscape.

Enabling knowledge growth was a massive demand for the large software engineering organization like Comtrade Project Management Organization (PMO), which engages over 200 experts located in 10 locations on over 400 active projects with different roles in project management: Project Managers, Scrum Masters, Program Managers, and Engagement Managers.

To master and understand the change, our people and organization had to consider learning and development a never-ending cycle of continuous improvement. A college degree is no longer sufficient to develop the skills needed to respond to rapidly changing business processes and technologies that change multiple times a year.

Collaborative: We need to change how we teach and what we teach to engage learners. Teacher-student relationships shift from expert-disciple towards peer-based collaborative learning.

Complementary: A development program should target complementary skills in the sense that technical, functional, and behavioural skills work together. These skills are interdependent. They should be learned and acquired simultaneously.

Sustained: If a training program is intended to sustainably bridge this digital skills gap, learning cannot be a one-time affair. The new paradigm for learning and development in the 21st century differs significantly from past models because organizations must address what people learn and how they learn. We can achieve fundamental digital transformation by designing sound strategies integrating changing content and delivery needs.

Simultaneous: digital skillsets should be addressed concurrently, all infused into core content as both process and outcome.

Background and related work

Project Management favourably impacts the software engineering business outcomes. It is defined as "*applying knowledge, skills, tools, and techniques to project activities to meet the project requirements. Project management enables organizations to execute projects effectively and efficiently.*" In the age of globalization, software engineering companies have to define the range of skills and knowledge needed for successful project management to remain competitive.

By studying scientific literature, it was discovered that a vast amount of literature explores the education topic for PMs. However, *not many articles focus on the learning design framework and the conceptual model for development, especially project management education monitoring. This paper aims to contribute to this study and emphasize the importance of project management education in large software engineering companies, presenting a framework for its custom development and measurement.*

Many studies prove that project management relevant technical and soft skills are not appropriately taught in undergraduate and master's degree programs.

Research (Fioravanti & Barbosa, 2019) investigates how project management education is taught in undergraduate degree programs of higher education in computing and its disassociation between theory and practice. A survey that is conducted with software PM educators indicates that there is a particular gap between academic and software industry expectations. As a result, there is a need to improve the project management curriculum, courses, and even student evaluation. However,

the challenge of keeping pace with a rapidly changing business environment and technological advances remains since it requires constant adjustment of academic PM education with software industry trends. Therefore, a well-established corporate education process that will provide continuous PM professional development and customized and complementary competence growth is fundamental in every software engineering company.

Existing research in project management explores how digital innovation changes project management professional development.

In (Bierwolf et al, 2017), the authors present how digital transformation impacts project management performance and whether the current PM curricula match the market's needs. This research explores how PM professional bodies such as IPMA and PMI embrace PM competence development and propose several PM education actions as lifelong learning. The authors suggested organizing and adopting these ongoing PM learnings by PM in practice.

The paper (Braun et al, 2020) identified that Project Management is vital in driving and implementing digital transformation, reflecting changes in their career path, qualification, and certification programs.

In this paper, the authors point out that one of the pillars of the organization's adaptability to market failures is introducing systematic education. Systematic education and sharing experiences from past projects are imperative for the organization's success.

In a series of papers, the authors try to answer how effective and efficient digital education channels are through case studies and analysis based on the target group's research. The authors investigate the eLearning platform's effectiveness in preparing candidates for software engineering companies (Atanasijević et al, 2013). After five years of application, they conclude that it has fully justified its place as a tool in harmonizing knowledge acquired at universities and the experience needed to work effectively on fundamental problems in modern engineering practice. In (Atanasijević et al, 2019a), the authors describe a complex education and knowledge exchange solution in a software engineering company. The authors present the essential requirements that the portal solution should enable: acquiring knowledge, sharing good and bad practices through exchanging experience, and unifying software engineering processes and procedures. In the paper (Stevanović et al, 2020), the authors conclude that educational training for employee development within an IT company should efficiently increase professional knowledge. In this paper, the authors share their experiences and explain how to leverage that knowledge through project-based learning, active and

collaborative learning, delivered as face-to-face, self-paced learning, and online training courses under the mentorship of experienced business analysts.

According to research published in this domain, authors affirmed the importance of custom-tailored, lifelong PM education in software engineering companies, which has to be aligned with frequent market changes and measured through the metric system's framework on the corporate level.

The literature review revealed that academic and professional education provides extensive coverage of planning and teaching methodologies for both universities and colleges.

The current literature on planning employee education to improve engineering knowledge and skills is lacking in-depth analysis and research.

The general opinion is that in software companies, after academic education, continuing education for the profession is just beginning.

Project goals

The existing studies presented in the literature review do not sufficiently explain how companies needing intensive education can implement Collaborative, Complementary, Sustained, and Simultaneous learning and monitor the effects of such an education process. No one has measured the effectiveness and efficiency and, based on that, made conclusions on improving the process further.

Digital transformation unlocked organizations' opportunities to increase performance and efficiency, which was unachievable a few years ago before new digital solutions.

Hypothesis 1 – Disruptive digital business

To ideate, create, and manage disruptive digital businesses, people and organizations need to be immediately and strategically prepared for a set of skills that will be continually changing and evolving.

Hypothesis 2 – Rapid changes in technologies

New technologies positively impact companies' performance, giving them a competitive edge to innovations and distinguishing between them. Efficient software engineering organizations always need a laser focus on emerging technologies to deliver a sustainable and competitive supply of new products, services, and processes which impact our client's business and market structures.

Hypothesis 3 – "Follow the sun" business model

Large software engineering companies are part of a globally distributed software engineering workflow and simultaneously work in several time zones. Consequently, PMO needs to resolve geographical and time spread along all projects to design specific steps that we can take to be more successful in project management and, consequently, on the market.

Hypothesis 4 – Survey findings

In data sources (Atanasijevic et al, 2016b), the 2016 PM Insights Survey diagnostic showed that the main pain points were Education & Knowledge, Methodology, and Teams. The organization needs to establish a few new or improved processes to increase efficiency and effective project execution support effectiveness with an active role in the project environment success.

Expected results / outcomes

We live in a world where software is everything; 'Software is eating the world,' Marc Andreessen said ten years ago. Successful software engineering organizations have adjusted their Agile-SCRUM development cycles to a rhythm of two to three weeks. After each cycle, the existing software platform will have new or improved functionalities. This starkly contrasts the former software development paradigm, which involved months of analysis, planning, and design until the final delivery of software products to customers.

A widely accepted agile approach is based on moving fast, releasing often, and reacting to our users' real needs. In the Agile project management world, the main goal of PMO is to ensure improvements in the following aspects:

- Enable rapid deployment of solutions,
- Minimize waste by minimizing resources,
- Enhance flexibility and adaptability to change,
- Reduce turnaround cycles,
- Contribute to the optimization of delivery processes,
- Optimize project control,
- Increase focus on specific customer needs, and
- Improve collaboration and feedback.

As emerging priorities, based on new market demands and survey results mentioned in the previous paragraph, we recognized three main project goals or areas with expected outcomes:

Education and Knowledge

- Support creating and tracking education plans;
- Promote internal events;
- Raise awareness of certification; and
- Simplify learning, bring closer education.

Methodology

- Standardization and KPIs;
- Formal PM processes improvement; and
- Best practice sharing.

Teams

- Business growth (more people in projects);
- Team optimization for an agile approach; and
- PM and TM education.

Methodology

The research intended to apply research that combines qualitative and quantitative approaches. The aim is an exploratory study to explore the educational process area in a global organization without offering final and conclusive answers to research questions. Desirable solutions to the research question are obtained by following the steps below (Atanasijević et al, 2023):

1. We applied a quantitative research approach to gather the state of education in the company. It includes setting up the survey, summarising the results, and drawing inferences from the data. The survey also provided a sorted list of wanted educational content.
2. We used qualitative methods to recognize the most utilized communicational channels to enable the sharing of educational content. PM community provides several communication channels (existing company portals, newsletter, skype, slack, emails, audio conferences, video conferences, and live meetings). We selected those channels with the highest utilization rate to include in PMO Education Roadmap.
3. Generating a graphical and collaborative roadmap that supports strategic alignment and dialogue between Software Company departments and stakeholders should provide a transparent stakeholder relationship matrix.
4. Assessment of process/framework effects on corporate efficiency.
5. Repeating the above steps enables a flexible framework approach to corporate knowledge growth deeply rooted in learners' needs. The primary objective is to provide them with the most flexibility about the

learning paths, schedules, collaboration, and best practice exchange possible.

- The targeted framework has to provide measurable outcomes that guarantee proper alignment with frequent market changes causing emerging PM skills.

Problem-solving framework

With an active role in the project success, in 2016, Comtrade Project Management Office designed and conducted the PM Insights Survey (Atanasijevic et al, 2016a) about various aspects of project management practice and needs in their company. The survey aimed to get the project management state and, through analytics, gap analysis to identify improvement priorities.

The project managers who participated in the research provided valuable information that we will use in this paper. With their willingness to share their opinions on important matters in the project management profession and attitudes towards PM practice in Comtrade, we identified gaps, recognized key improvement factors, and defined a Roadmap for executing specific action plans.

The radar diagram and the gap bars are presented in Figure 1. Figure 2 shows the survey results across seven primary categories compared to desired values. The most significant gap emerged in the "Education and Knowledge" category, followed by the "Methodology" and "Team" categories.

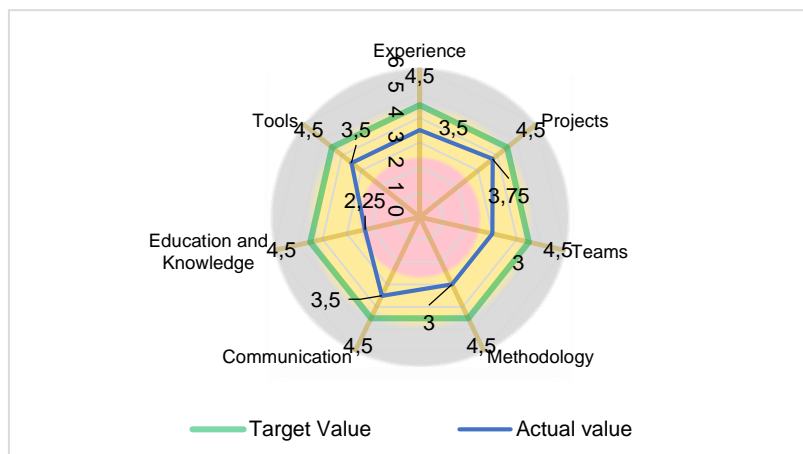


Figure 1 – PM Insights Survey results - Radar diagram
 Рус. 1 – Результаты опроса PM Insights — радарная диаграмма
 Слика 1 – ПМ резултати истраживања – радарски дијаграм

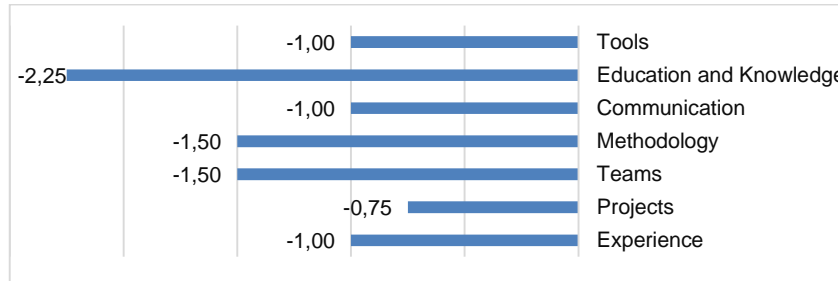


Figure 2 – PM Insights Survey results – GAP Analysis
 Рус. 2 – Результаты опроса PM Insights – GAP-анализ
 Слика 2 – ПМ резултати истраживања – ГАП анализа

Solution

The shift to a digital, knowledge-based economy imposed the solution for establishing an effective learning and growth process as the PM Framework for scaling the educational process at the enterprise level, presented in Figure 3.

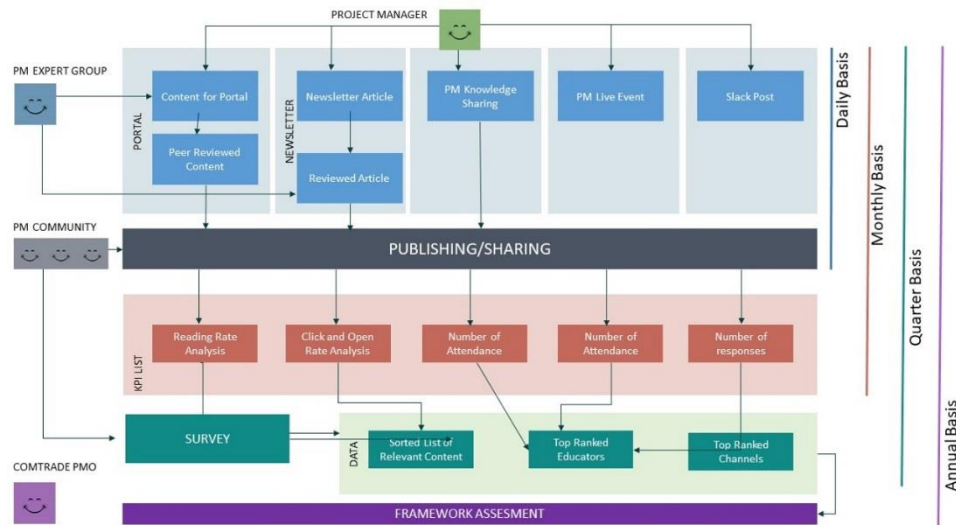


Figure 3 – Graphical representation of the established process – PM framework
 Рус. 3 – Графическое изображение установленного процесса – PM Framework
 Слика 3 – Графички приказ успостављеног процеса – ПМ оквир

The framework supports vital business priorities by developing and joining people on ongoing challenges. Persistent uncertainty, a multi-geographical workforce, and shorter shelf life for knowledge have placed

precedence on reskilling and upskilling. These are very narrow niches of education that companies cannot buy on the market as ready-to-use training programs but are forced to develop their own and then change them as practices evolve.

Multiple PM, Digital communication channels, are available within the framework. Their effectiveness and benefits for learning, collaboration, and teamwork rely on communication and stakeholders' engagement.

Such an established framework provides a relational database containing data from all stakeholders in the process, all sources, and all channels across all project life cycle phases. A combination of that data provides plenty of metrics and lists of KPIs that unambiguously show whether a process is effective.

The Comtrade PMO EDUCT portal (Janković et al, 2020) is a landing page, core for corporate knowledge sharing, collaboration, project resource libraries, aggregator of all initiatives, and a portal around which all additional PM Digital communication channels are developed, as shown in Figure 4. Our approach facilitates unlimited reach, is cost-effective, and addresses the needs of varied and globally widespread learners, keeping us on track to achieve business and project goals.

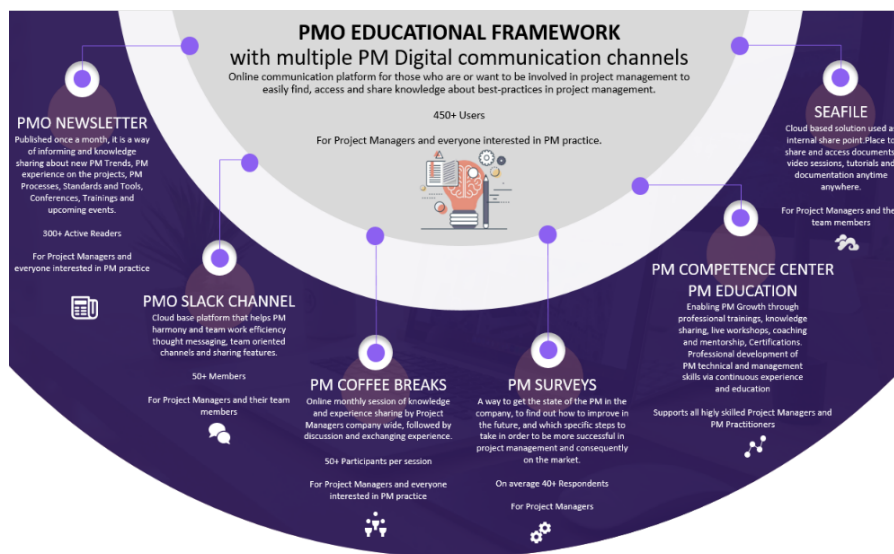


Figure 4 – PM Educational framework with digital channels of communication and knowledge sharing

Рис. 4 – Образовательная система PM с цифровыми каналами общения и обмена знаниями

Слика 4 – ПМ образовни оквир са дигиталним каналима комуникације и размене знања

The PMO EDU portal is structured in the following way:

- **Courses** focus on highly specialized training and tutorials for PMs, Scrum Masters, BAs, and project teams, as custom corporate eLearning content. Each activity includes lessons part and, in the end, knowledge validation through test exams and certification. Tutorials help learners master a chosen process and tools.
- To ensure effective project onboarding, **Coaching Corners** are for everyone interested in Scrum Master and BA, with mentorship program plans, shared personal experience, solutions for everyday Scrum and BA problems, best practices, and tool recommendations.
- **Knowledge database vocabulary** – short educational content:
- **WHAT IS:** basic concepts of project management terms, tools, or techniques. The subject is explained to help PM practitioners easily understand and apply new knowledge.
- **HOW TO:** provides step-by-step information about some specific concept. These materials are tutorials that lead the user through the key features, functions, or stages that progress through a logical sequence to understand the user's elements.
- **Certificates database:** The place where our colleagues' certificates are transparent and continuously updated– our hall of fame. The base contains Scrum Master, Product Owner, and PMO EDU certificates. We are always up to date with the knowledge and competencies of our employees.
- **PM Brochures:** Corner, where our project managers generously shares their knowledge and experience with others, is about global PM practices or internal expertise and skills.
- **PMO Forum:** Place for discussion and sharing knowledge peer to peer.
- **Support:** Place with frequently asked questions, contacts, and calls to action to contribute by sharing content and ideas.

Other Multiple PM Digital communication channels available within the framework are:

- To gather community feedback - **Comtrade PM surveys:** Survey questions and results lead us to find out the best improvements for the future, so as the concrete next steps that we can take to be more successful in project management and consequently on the market.
- **The PM Knowledge Sharing initiative** is realized through PM Coffee Breaks and BA Coffee Breaks, held once a month as a delight for the whole PM community. Topics from the best PM/BA practices and

knowledge are discussed and shared within the community. Video and audio recordings from every session are always available here.

- To promote team culture - **PMO Newsletter**: As part of the monthly updating community with upcoming trends in the industry, news, internal and external events, conferences, trainings, or achievements in a for-on newsletter are uploaded into the archive, so no information is left out.
- To foster collaboration - **PM Slack channel**: Helps PM harmony and teamwork efficiency throughout messaging and team-oriented channels.
- To encourage community exchange - **Seafile**: PM internal share point for all documents, video sessions, tutorials, and templates.

Results

We monitor the results we have accomplished through the benefits we have achieved in our daily work and measure them through the metric system we have established.

Outcomes and Benefits

Tailoring for Custom Needs

Corporate education requires highly specialized content, usually related to the latest methodologies or technologies. Very often, there are still no courses for such topics in the market by educational providers, or they are too basic, i.e., they do not have enough content for quick starting of implementation.

As custom corporate eLearning content is built on demand, it is tailored for specific requirements and corresponds to certain corporate practices (Dimic et al, 2019).

The PMO EDUCT platform provides tailored learning content, design, and delivery to suit learners, companies, and personal goals. Once the company had experienced the benefits of using content tailored to learners' needs, they never went back to pre-made courses but chose to shift to blended learning (Ashleigh et al, 2012) by:

- Engaging external professors/experts or pre-made systems whenever necessary and
- Continuing with internal education to build skills and verify readiness for project onboarding.

Turning Knowledge into Practice

Training has a lasting impact on achieving learning and development goals. Once training is complete, trainees will be challenged to test their newly acquired knowledge and workplace skills.

Testing in the real world could be hazardous for project tasks and frustrating for employees not confident enough to take responsibility for outcomes and delivery in a new role (Predić et al, 2018).

To succeed in competence building, PMO usually establishes labs and sandboxes for exercise and assignments like actual project tasks to practice their workplace skills.

Competency Building

When the external consultant completes the training, he leaves, and the PMO staff cannot verify knowledge and continue to support the implementation of new skills in practice. To prevent this shortcoming, the PMO has designed a mentoring program for fast onboarding on a project, including tasks similar to those that probationers will face on an actual project.

Effectiveness in Project Onboarding

They designed and developed PMO training to ensure that project teams understand projects thoroughly and have the information and skills to successfully deliver products and services (Zahar et al, 2020).

- The main benefit of agile delivery is that approach is rapid. It is possible to create courses and provide project training to project teams as soon as a project is launched or during the presales process.
- It delivers all the relevant project knowledge that will bring project managers up to speed on new methodologies, skills, or technologies and help them score over competitors.
- It enables simultaneous education of our globally widespread employees at the same time.
- It provides knowledge refreshing and follow-up inquiry since employees can retrieve and review learning materials whenever they want.

Efficiency in Competence Growing

- PMO EDUCT proved the best results in support of more efficient operations and enhanced productivity:
- Trains employees for new roles and speedy deployment of new systems and processes.

- Provides narrowly targeted training to help employees adapt and respond to new challenges.
- Significantly reduces costs with self-paced learning that optimizes the degree of employee time utilization.

Personalized and Targeted

Corporate-related training courses are developed considering the company goals, strategy, and career paths so they align with the business and employee's personal goals altogether (Stevanović et al, 2019).

- We control their learning pace by allowing employees to follow interactive multimedia lessons.
- Participants can access bite-sized learning chunks, illustrations, short videos, and mobile phones. The Microlearning concept allows them to learn what they need when needed, just in time.
- PMs, BAs, and developers spend countless hours in neophytes training, introducing new procedures and mandatory training sessions during the year required to meet project or personal goals.

Encouraging Collaboration

Practical corporate training should provide the mission-critical skills and knowledge necessary for everyday work and should be interconnected with employees via shared project tasks.

Employees often learn more through interactions with their peers in an agile environment than by reading a book.

Collaboration on the training strengthens team connectivity and reinforces communication and openness, especially because excellent communication and collaboration tools are in place (wikis, forums, discussions, chats, etc.)

Community Exchange and Ideation

Our corporate learning is not designed to be an individual's journey but rather a driver for enhancing employee cooperation and trust.

- Bringing employees together often leads to debates and discussions that lead to innovation, too.
- The emerging community provides a playground for social exercise in the internal environment before a customer faces circumstances.

Fostering Engagement

Collaborative learning and community further raise new benefits in better immersing and motivating employees preoccupied with daily

challenges. Employees have live exchange and immediate access to others in the learning community through features like discussion forums and web conferences. Engagement with other employees fosters collaboration and team culture, which has benefits beyond the training environment.

Monitoring KPIs

We monitored the framework usefulness and effectiveness as part of our performance monitoring within the Balanced Scorecard methodology under the Learning and Growth perspective.

The PMO Framework Radar Diagram in Figure 5 represents the effectiveness expressed through the KPI results and improvements achieved in the monitoring period. The results comparison between the years 2017 and 2019 is shown in Table 1.

To ensure the ecosystem sustainability and further improvements, we monitor achievements through the following KPIs in Table 2.

The KPIs that reflect outcomes of education are derived from the PMO EDU portal KPIs (Atanasijević et al, 2019b), and they are:

- Knowledge validation rate,
- Follow up support, and
- Geographical coverage.

The readiness for a project as a measure of employability is expressed with the following KPIs that we obtain from the dataset recorded in the Project Dashboard tool for project management:

- Onboarding cycle,
- PM readiness, and
- SM readiness.

For a review of the improvements related to the values-based, innovative, and collaborative culture, we use a targeted survey representing a measuring system for the following KPIs:

- Ideation & innovation initiatives and
- Attrition behavioural change.

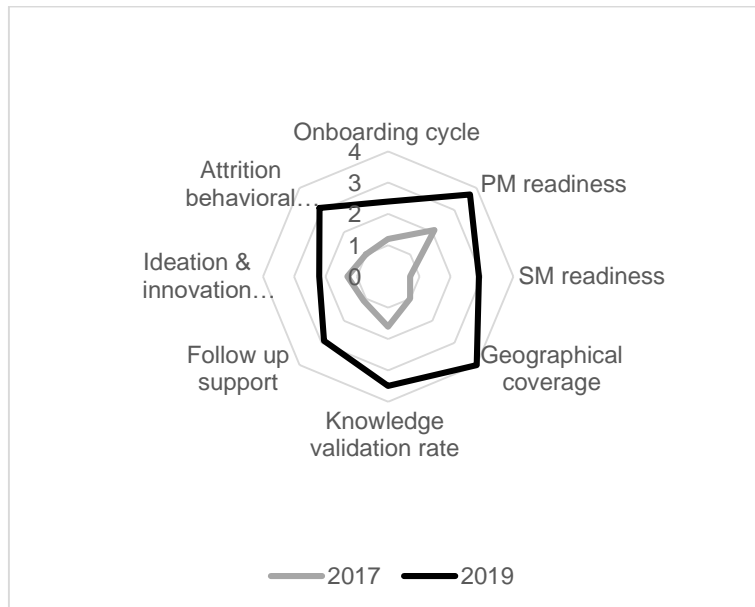


Figure 5 – PMO EDU platform Radar Diagram of the KPI results from 2017 and 2019
 Рис. 5 – PMO EDU Радарна диаграма резултатов КПИ за 2017 и 2019 годы
 Слика 5 – PMO EDU платформа Радарски дијаграм КПИ резултата из 2017. и 2019. године

Table 1 – PMO EDU platform KPI results in 2017 and 2019
 Таблица 1 – Резултати КПИ платформе PMO EDU в 2017 и 2019 годах
 Табела 1 – PMO EDU платформа КПИ, резултати у 2017. и 2019. години

KPIs/Results	2017	2019
Onboarding cycle	1.2	2.4
PM readiness	2.1	3.7
SM readiness	0.7	2.9
Geographical coverage	1.0	4.0
Knowledge validation rate	1.6	3.5
Follow up support	1.1	2.9
Ideation & innovation initiatives	1.3	2.2
Attrition behavioural change	1.0	3.1

Table 2 – PMO EDU platform KPI metrics
 Таблица 2 – Показатели KPI платформы PMO EDU
 Табела 2 – KPI метрике ПМО ЕДУ платформе

KPI metrics			
1	2	3	4
Onboarding cycle			
over a month	half a month to a month	up to half a month	within a week
PM readiness <i>Project and agile knowledge</i>			
over a month	half a month to a month	up to half a month	within a week
SM readiness <i>Agile and technology knowledge</i>			
over a month	half a month to a month	up to half a month	within a week
Geographical coverage cycle <i>Time for educational cycle per all locations</i>			
over a month	half a month to a month	up to half a month	within a week
Knowledge validation rate			
exam on training	practical assignment	grade from project	candidature for promotion
Follow up support			
no materials	learning materials from the training	additional materials for reading continuously on an online repository	consultancy from specialists through the platform
Ideation & innovation initiatives			
1-2 per year	3-5 per year	6-10 per year	over 10 per year
Attrition behavioural change <i>Self-initiated and voluntary actions for improvement</i>			
1-2 per year	3-5 per year	6-10 per year	over 10 per year

Atanasijević, S. et al, Enabling digital growth through continuous education of project managers: a framework for collaborative, complementary, sustained, and simultaneous learning in software engineering organizations, pp.1172-1197

Conclusion

In the digital age, where change is constant and innovation is imperative, organizations must proactively embrace learning and development as core strategies for growth and resilience. This paper has presented a comprehensive framework for continuous education and knowledge growth, tailored explicitly to the intricate demands of software engineering organizations. Collaborative, Complementary, Sustained, and Simultaneous learning principles have been dissected and applied within project management education, methodology enhancement, and team optimization.

Through a combined qualitative and quantitative approach, this study has demonstrated the efficacy of the framework in fostering personalized learning, team collaboration and cultivating a culture of innovation. Applying key performance indicators (KPIs) has yielded tangible outcomes, showcasing improved project onboarding, enhanced skills readiness, and increased engagement. As a result, software engineering organizations are better equipped to navigate the challenges of digital disruption and leverage education as a strategic tool for success.

The literature review found good coverage for academic education and professional training provided by various educational institutions or companies for vocational education, with plenty of practices and methodologies for effectiveness and speeding.

However, the literature does not sufficiently explain how companies needing intensive education, especially software companies, can implement Collaborative, Complementary, Sustained, and Simultaneous learning and growth and monitor the effects of such practices.

This paper contributes to applying such a solution in practice and has an original contribution as an authentic approach.

This framework allows us to pivot and adjust KPIs anytime, respond to business priorities, or adapt to any company's situation.

A company achieved digital growth goals in all key PMO areas by:

- Standardizing processes, unifying project management tools, and onboarding and training new PMs.
- Creating a common language for all stakeholders, sharing knowledge and experience, and providing continuous professional development for PMs, Scrum Masters, and project teams.
- Accelerating professional training while balancing discipline with agility, promoting personal competences, and assessing PM capabilities.

In other words, the company:

- Created a consistent and standardized approach to project management, making it easier for everyone to collaborate and share information.
- Invested in its people, providing them with the training and support they need to be successful.
- Promoted a culture of continuous learning and improvement.
- Created a more transparent and equitable environment for PMs to develop and grow their careers.

The following survey and the framework assessment will show the directions for further development.

The digital growth journey is ongoing, marked by evolution, adaptation, and continuous improvement. The framework presented in this paper offers a blueprint for organizations to instil a learning-centric culture where professionals are empowered to stay ahead of technological shifts, seize opportunities, and drive innovation. By embracing this approach, organizations can transcend traditional boundaries, bridge the gap between academia and industry, and cultivate a workforce adept at utilizing the latest tools and equipped with the critical thinking, collaboration, and adaptability skills essential for success.

This paper aims to encourage organizations to create their own and adopt a framework exposed to its realistic priorities and needs in SW development that depend on: the dynamics and requirements of their clients, the capabilities and performance of their employees, and government expectations and investments.

In conclusion, the digital era demands a paradigm shift in how organizations approach education and growth. The framework proposed in this paper serves as a guiding light, illuminating a path where education is not a one-time endeavour but an ongoing journey of exploration, collaboration, and transformation. As software engineering organizations evolve, continuous education will remain pivotal in shaping their destiny, propelling them towards a future characterized by innovation, resilience, and enduring excellence.

References

Ashleigh, M., Ojiako, U., Chipulu, M. & Wang, J. K. 2012. Critical learning themes in project management education: Implications for blended learning. *International Journal of Project Management*, 30(2), pp.153-161. Available at: <https://doi.org/10.1016/j.ijproman.2011.05.002>.

Atanasijevic, S. 2016. Inovativni modeli digitalne transformacije poslovanja-iskustva lidera. In: *Naučna konferencija INFORMATIKA 2016: Novi trendovi u razvoju informacionih sistema*, Belgrade, Serbia, pp.28-33, May 17 (in Serbian) [online]. Available at:

https://www.researchgate.net/publication/326208718_Inovativni_modeli_digitaln_e_transformacije_poslovanja_-_iskustva_lidera [Accessed: 5 June 2023].

Atanasijević, S., Atanasijević, T., Janković, V. & Zahar, M. 2019a. Application of e-Learning technology in corporate education - Case Study of Comtrade's PMO EDUCT portal. In: *The 10th International Conference on e-Learning (eLearning-2019)*, Metropolitan University, Belgrade, Serbia, pp.74-80, September 26-27 [online]. Available at: https://www.metropolitan.ac.rs/files/2020/03/eConference-2019-Zbornik_FINAL.pdf [Accessed: 5 June 2023].

Atanasijević, S., Atanasijević, T. & Zahar, M. 2019b. PMO Approach in Choosing the Optimal Project Governance Framework for Contracted Engagement Model. In: *3rd International Scientific Conference on Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture – ITEMA*, Bratislava, Slovakia, pp.171-177, October 24. Available at: <https://doi.org/10.31410/ITEMA.2019.171>.

Atanasijević, S., Perić, T. & Bošković, I. 2013. Usage of moodle e-learning portal in the recruitment process for new comers comtrade group case study. In: *The Fourth International Conference on e-Learning (eLearning-2013)*, Metropolitan University, Belgrade, Serbia, pp.109-113, September 26-27 [online]. Available at: <https://elearning.metropolitan.ac.rs/files/pdf/2013/14-srdjan-atanasijevic-tanja-peric-ivana-boskovic-usage-of-moodle-e-learning-portal-in-the-recruitment-process-for-newcomers-comtrade-group-case-study.pdf> [Accessed: 5 June 2023].

Atanasijevic, S., Zahar, M., Janković, V., Fimic-Rakovic, M., Zubac Numić, A. & Sabljic, S. 2016a. PM Insights Survey 2016 Radar Diagram Framework with Survey Responses. *ResearchGate*, June. Available at: <https://doi.org/10.13140/RG.2.2.10684.26243>.

Atanasijevic, S., Zahar, M., Janković, V., Zubac Numić, A., Sabljic, S. & Fimic-Rakovic, M. 2016b. PM Insights Survey Analysis 2016. *ResearchGate*, July. Available at: <https://doi.org/10.13140/RG.2.2.26203.18725>.

Atanasijević, S., Zahar, M., Rančić, D., Atanasijević, T. & Đorđević, M. 2023. Creating an Educational Framework for Project Managers at a Software Company: A Sample Approach. In: *Sinteza 2023 - International Scientific Conference on Information Technology and Data Related Research*, Singidunum University, Belgrade, Serbia, pp.199-205, May 27. Available at: <https://doi.org/10.15308/sinteza-2023-199-205>.

Bierwolf, R., Romero, D., Pelk, H. & Stettina, C.J. 2017. On the future of project management innovation: A call for discussion towards project management 2030 In: *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Madeira, Portugal, pp.689-698, June 27-28. Available at: <https://doi.org/10.1109/ice.2017.8279952>.

Braun, T., Ekstedt, E., Lundin, R.A., & Sydow, J. 2020. Digital Transformations of Traditional PBOs and Modern PNWs: Changing Management Practices in Project Society (Final Report). *PMI Sponsored Research* [online]. Available at: <https://www.pmi.org/learning/library/digital-transformation-pbo-pnw-11997> [Accessed: 5 June 2023].

Dimic, G., Rancic, D., Macek, N., Spalevic, P. & Drasute, V. 2019. Improving the prediction accuracy in blended learning environment using synthetic minority oversampling technique. *Information Discovery and Delivery*, 47(2), pp.76-83. Available at: <https://doi.org/10.1108/idd-08-2018-0036>.

Fioravanti, M.L. & Barbosa, E.F. 2019. Outlining Software Project Management Education by Surveying Educators. In: *2019 IEEE Frontiers in Education Conference (FIE)*, Covington, KY, USA, pp.1-8, October 16-19. Available at: <https://doi.org/10.1109/fie43999.2019.9028366>.

Janković, V., Atanasijević, S., Atanasijević, T., & Zahar, M. 2020. How to Establish a Project Management Education Process in a Software Company: From Defining a Roadmap to Effective Implementation. In: *10th International Conference on Information Society and Technology (ICIST 2020)*, Kopaonik, Serbia, pp.60-63, March 8-11 [online]. Available at: <https://www.eventiotic.com/eventiotic/library/paper/585> [Accessed: 5 June 2023].

Predić, B., Dimić, G., Rančić, D., Štrbac, P., Maček, N. & Spalević, P. 2018. Improving final grade prediction accuracy in blended learning environment using voting ensembles. *Computer Applications in Engineering Education*, 26(6), pp.2294-2306. Available at: <https://doi.org/10.1002/cae.22042>.

Stevanović, J., Atanasijević, S., Atanasijević, T. & Zahar, M. 2020. Expanding the level of engineer knowledge for software modeling within corporate education by active and collaborative learning. In: *2020 IEEE Global Engineering Education Conference (EDUCON)*, Porto, Portugal, pp. 1807-1814, April 27-30. Available at: <https://doi.org/10.1109/educon45650.2020.9125250>.

Stevanović, J., Atanasijević, S., Atanasijević, T. & Zahar, M. 2019. Raising the Skills of Business Analysts – The Benefits of eLearning Technologies in Corporate Education. In: *The 10th International Conference on e-Learning (eLearning-2019)*, Metropolitan University, Belgrade, Serbia, pp.25-30, September 26-27 [online]. Available at: https://www.metropolitan.ac.rs/files/2020/03/eConference-2019-Zbornik_FINAL.pdf [Accessed: 5 June 2023].

Zahar, M., Atanasijevic S. & Vasilijevic, M. 2020. How To Leverage Corporate eLearning Platform, For Making Tool Used In Creating Candidates' Profile, Which Turns Business Opportunities Into Prospective Clients. *ResearchGate*, September. Available at: <https://doi.org/10.13140/RG.2.2.10727.68005>.

Обеспечение цифрового роста посредством непрерывного образования менеджеров проектов: основа для совместного, дополнительного, устойчивого и одновременного обучения в организациях, занимающихся разработкой программного обеспечения

Срджан В. Атанасиевич^а, **корреспондент**, Моника Н. Захар^а, Деян Д. Ранчич^б, Иван Б. Вулич^в, Татьяна Я. Атанасиевич^а

^а Крагуевацкий университет, г. Крагуевац, Республика Сербия

^б Нишский университет, факультет электронной инженерии, департамент компьютерных наук, г. Ниш, Республика Сербия

^в Университет обороны в г. Белград, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 14.01.85 Автоматизация и автоматизированные системы в образовании,
14.37.09 Методика обучения взрослых,
20.15.13 Информационные службы на предприятиях и в учреждениях,
28.29.59 Программированное обучение,
50.49.37 Автоматизированные системы управления предприятиями и организациями,
82.05.09 Основы теории и принципы организации и управления,
06.81.25 Научно-технический прогресс на предприятии

ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: В данной статье представлена новая структура РМО EDUCT, которая включает в себя совместное, дополнительное, устойчивое и одновременное обучение. Эта структура специально приспособлена к динамичной среде разработки программного обеспечения. Данная статья вносит вклад в актуальную дискуссию об образовании и профессиональном развитии в цифровую эпоху, освещая стоящие перед ним проблемы, представляет разработанную структуру и измеримые достигнутые результаты. Представленная концепция подчеркивает необходимость гибкости, адаптируемости и неустанного стремления к знаниям как фундаментальных принципов успеха в постоянно меняющейся среде.

Методы: В данном исследовании, посвященном крупным организациям, занимающимся разработкой программного обеспечения, рассматриваются многогранные аспекты образования в области управления проектами, совершенствования методологии и оптимизации команды. Предлагаемая методология сочетает в себе качественные и количественные подходы для изучения области

образовательного процесса в глобальной организации и создания гибкой и измеримой структуры для улучшения развития корпоративных знаний. Такая структура нацелена на предоставление учащимся максимальной гибкости в плане обучения, планирования, сотрудничества и обмена опытом, гарантируя при этом соответствующую адаптируемость к частым изменениям рынка и новым навыкам управления проектами.

Результаты: Результаты показывают, что персонализированное непрерывное обучение, которому способствует совместная рабочая среда и специально подобранный контент, дает значительные преимущества. На основании анализа ключевых показателей эффективности (KPI) данное исследование показывает: улучшение адаптации на проектах, улучшение взаимодействия сотрудников и развитие культуры инновационной деятельности.

Выводы: В данной статье представлена структура РМО EDUCT, которую организации могут использовать для создания культуры обучения и расширения возможностей своих сотрудников с целью достижения успеха в постоянно развивающейся области разработки программного обеспечения. Приняв принципы совместного, взаимодополняющего, устойчивого и одновременного обучения, организации могут развивать компетенции сотрудников и необходимые навыки критического мышления, их направленность на сотрудничество и адаптивность, которые необходимы для успеха в цифровую эпоху.

Ключевые слова: разработка программного обеспечения, структура обучения, цифровая трансформация, управление проектами, компетенция, гибкая методология, стратегия обучения, формирование компетенций.

Омогућавање дигиталног раста кроз континуирану едукацију менаџера пројеката: оквир за колаборативно, комплементарно, одрживо и истовремено учење у организацијама за софтверско инжењерство

Срђан В. Атанасијевић^а, аутор за преписку, Моника Н. Захар^а, Дејан Д. Ранчић^б, Иван Б. Вулић^в, Татјана Ј. Атанасијевић^а

^а Универзитет у Крагујевцу, Крагујевац, Република Србија

^б Универзитет у Нишу, Електронски факултет, Департман за рачунарство, Ниш, Република Србија

^в Универзитет одбране у Београду, Београд, Република Србија

ОБЛАСТ: рачунарске науке, информационе технологије
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: Овај рад представља ПМО ЕДУКТ оквир који обухвата колаборативно, комплементарно, одрживо и симултано учење креирано за динамичко окружење софтверског инжењеринга. Доприноси текућој дискусији о образовању и професионалном развоју у дигиталној ери осветљавањем изазова са којима се суочава, представља развијен оквир и постиже мерљиве резултате. Представљени оквир наглашава потребу за агилношћу, прилагодљивошћу и потрагом за знањем, као основним принципима успеха у окружењу које се стално развија.

Метод: Фокусирајући се на велику организацију софтверског инжењеринга, ова студија истражује вишеструке аспекте образовања за управљање пројектима, побољшање методологије и оптимизацију тима. Предложена методологија комбинује квалитативне и квантитативне приступе за истраживање образовног процеса у глобалној организацији и генерисање флексибилног и мерљивог оквира за побољшање раста корпоративног знања. Оквир има за циљ да пружи ученицима највећу флексибилност у погледу учења, распореда, сарадње и размене најбоље праксе, а гарантује и правилно усклађивање са честим променама на тржишту и новим вештинама ПМ-а.

Резултати: Налази показују да персонализовано, континуирано учење, олакшано кроз колаборативно окружење и прилагођени садржај, доноси значајне предности. Кроз анализу кључних индикатора учинка (КПИ), представљена је побољшана имплементација пројекта, бољатимска сарадња и неговане културе иновација.

Закључак: Овај рад представља оквир ПМО ЕДУКТ који организације могу да користе за стварање културе учења и оснаживање својих запослених да успеју у области развоја софтвера која се стално развија. Усвајањем принципа колаборативног, комплементарног, одрживог и истовременог учења, оне могу развити радну снагу са основним вештинама критичког мишљења, сарадње и прилагодљивости неопходних за успех у дигиталној ери.

Кључне речи: софтверски инжењеринг, оквир учења, дигитална трансформација, управљање пројектима, компетенције знања, агилна методологија, стратегија учења, изградња компетенција.

Paper received on / Дата получения работы / Датум пријема чланка: 07.06.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 30.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 01.12.2023.

© 2023 The Authors. Published by *Vojnotehnički glasnik / Military Technical Courier*
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Авторы. Опубликовано в «Военно-технический вестник / *Vojnotehnički glasnik / Military
Technical Courier*» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутори. Објавио Војнотехнички гласник / *Vojnotehnički glasnik / Military Technical Courier*
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



ПРИКАЗИ

ОБЗОРЫ

REVIEWS

Review of the book entitled
Discrete Communication Systems
by Stevan Berber,
Oxford University Press, 2021

Nebojša N. Gaćeša

University of Defence in Belgrade, Military Academy,
Belgrade, Republic of Serbia,
e-mail: nebojsa.gacesa@mod.gov.rs,
ORCID iD: <https://orcid.org/0000-0003-3217-6513>

DOI: [10.5937/vojtehg71-45887](https://doi.org/10.5937/vojtehg71-45887); <https://doi.org/10.5937/vojtehg71-45887>

FIELD: telecommunications

ARTICLE TYPE: reviews of a book

Abstract:

The book contains the theory of discrete communication systems that are presented in the form of block schematics defined by mathematical operators. For the sake of comparison, the theory of digital communication systems is added to understand better the relations between the two theories. Two generic schemes of the systems are designed that are used to develop specific discrete and digital systems as their special cases. The complementary chapters of the book contain the theory of the continuous-time and discrete-time processing of the deterministic and stochastic signal that is necessary for understanding the main chapters presenting communication systems.

Key words: discrete communication system, digital communication system, discrete modulation, digital modulation, theory of information and coding, discrete-time signal processing, continuous-time signal processing deterministic signals, random signals.

Book title: Discrete Communication Systems

Book author: Stevan Berber, The University of Auckland,
Auckland, New Zealand, Senior member of IEEE,
s.berber@auckland.ac.nz.

Place of publication: New York, USA

Publisher: Oxford University Press

Copyright date: Stevan Berber, 2021

Number of pages in the book: 928 pages, plus index.
Number of pages in the supplementary material:
Solutions to the Problems 356 pages, Projects 204 pages.

Purpose and the main features of the book

This book primarily presents the theoretical base of discrete communication systems with a reference to digital communication systems. The contents of the book solely address problems in the design of a communication system that includes a transmitter, a transmission channel, and a receiver. The signals processed in the system are presented in two domains of time, the continuous-time domain and the discrete-time domain, as well as in two corresponding domains of frequency, the Fourier series and transforms for continuous-time and discrete-time signals. A system operating in the continuous-time domain is named *the digital system*, while a system operating in the discrete-time domain is named *a discrete system*. The theory of discrete systems is the focus of this book because of the existing theory of digital communication systems; however, it is not sufficient to work on the design and implementation of the communication system transceiver blocks in modern DSP technology. The purpose of the book is not to explain all existing modulation techniques, but to make a firm foundation of communications systems operating in the discrete-time domain covering the basic discrete modulation methods.

The writing of this book is additionally motivated by modern trends in the design of communication systems on the FPGA and DSP platforms. These trends were heavily supported by advances in the theory of discrete-time signal processing. These trends will continue in the future supported by the everlasting increase in the processing ability of digital technology allowing the development of sophisticated communication algorithms we could not dream of in the past. For these reasons, it is necessary to know how to use the discrete-time signal processing theory and how to apply it in the design of modern communication devices. Even more important is to make available the theory of discrete-time communication systems to researchers, practicing engineers, and designers of communications devices in the industry. Practically all modern communication devices such as wireless and cable modems, TV modems, consumer entertainment systems, satellite modems, and similar, are based on the use of digital processing technology and the principles of the discrete-time signal processing theory.

The distinguishing features of the book are:

1. This is the first book that presents the essential theory and practice of discrete communication systems design. In contrast to already published books, the operation of the discrete communication systems is expressed in terms of the theory of discrete-time stochastic processes and related to the existing theory of digital communication systems.

2. Based on the presented orthogonality principles, a generic structure of a communication system, based on correlation demodulation and optimum detection, is developed and presented in the form of mathematical operators.

3. Due to the random nature of the signals processed, the theory of continuous-time and discrete-time stochastic signal processing is extensively and consequently applied to present the signals at the inputs and outputs of the transceiver blocks and to develop the general system named the generic system.

4. Based on the generic system, the traditionally defined phase shift keying (PSK), frequency shift keying (FSK), quadrature amplitude modulation (QAM), orthogonal frequency division multiplexing (OFDM), and code division multiple access (CDMA) systems are deduced as its special cases.

5. Having in mind the controversial nature of the continuous-time white Gaussian noise process having infinite power, a separate chapter is dedicated to noise discretization by introducing the notions of noise entropy and the truncated Gaussian density function.

6. The book is self-sufficient because it uses a unified notation and terminology, both in the main ten chapters explaining communications systems theory and in nine complementary chapters dealing with the continuous and discrete-time signal processing for both deterministic and stochastic signals. Therefore, readers do not need to go to various books on signal processing and struggle with their different notations to understand them in the context of the operation of communication systems.

7. The unified notation and unified terminology allow clear distinction of deterministic signals from stochastic ones, power signals from energy signals, as well as discrete-time signals and processes from continuous-time signals and processes.

8. For the sake of explanation and clarity, the theory of digital communication systems is presented to a certain extent and related to the main theory of discrete communication systems.

9. The text of the book is accompanied by solutions to about 300 problems and five Projects.

Content of the book

The book contains two parts, as it can be seen in Fig. 1.

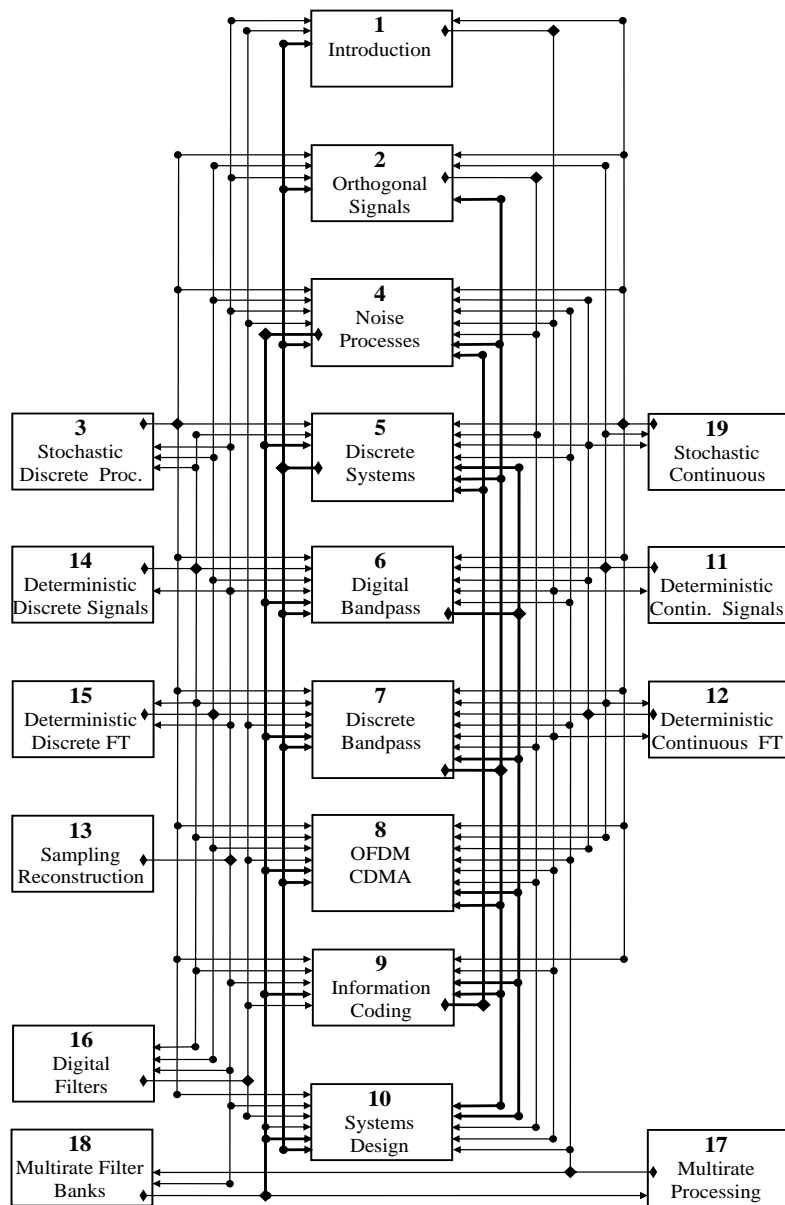


Figure 1 – Book structure and the relations between chapters

Рис. 1 – Структура книги и взаимосвязь между главами.

Слика 1 – Структура књиге и концепција поглавља

The First Part has ten main chapters and presents an essential theory of discrete and digital communication systems, the operation of their building blocks, and in the first place the operation of modulators and demodulators/detectors. Due to the importance of the theory of discrete and continuous-time signal processing, for both deterministic and random signals, nine chapters containing this theory are incorporated into the Second Part of the book containing nine complementary chapters.

The main chapters are in the middle of the diagram (1 to 10, including Chapter 3 on the left). The complementary chapters, containing the theory of signal sampling and reconstruction, and the necessary theory in deterministic discrete-time signal processing, are on the left-hand side (13, 14, and 15). The chapters containing the theory of continuous-time signal processing are on the right-hand side (11, 12, and 19). Chapters 16 to 18, at the bottom of Fig. 1, contain the essential theory of digital filters and multi-rate signal processing that is relevant for nearly all chapters of the book and for Chapters 7 and 10. The chapters are interconnected by the input arrow and output diamond lines.

Description of chapters in the main part

Chapter 1 introduces the subject of the book, defines the main terms in communication systems, and presents the main objectives for writing this book.

Chapter 2 is dedicated to the principle of discrete-time signals orthogonalization. Understanding this chapter is a prerequisite to understanding Chapters 4 to 10.

Chapter 3 contains the theory of discrete-time stochastic processes, which is a prerequisite for the chapters related to the theory of discrete communication systems exposed in Chapters 4 to 10.

Chapter 4 addressed the issues related to the theory of noise in communication systems. Adding the entropy and truncated density functions to already used autocorrelation and power spectral density functions allowed mathematical modeling of the discrete noise generators and regenerators. This chapter is in close relation to Chapters 3, 19, 13, 16, 17, and Project 3.

Chapter 5 is a vital part of this book presenting the generic communication system operating in the discrete-time domain, which is based on the implementation of orthogonal modulators, correlation demodulators, and optimum detectors, following the definition of signal synthesizers and analyzers in Chapter 2.

The generic discrete system is shown in Fig. 2, to be used to deduce the practical systems as its special cases.

Chapter 6 presents mathematical models of the traditional baseband and bandpass digital communication systems based on the BPSK, QPSK, FSK, and QAM modulation methods.

Chapter 7 presents the operation of a discrete system that processes pure discrete-time signals.

The vital characteristics of the system and its blocks are expressed in terms of amplitude spectral density, autocorrelation functions, power and energy spectral densities, and bit error probability.

This chapter presents mathematical models of the discrete baseband and bandpass communication systems based on the BPSK and QPSK, FSK, and QAM modulation methods, which are deduced from the generic system structure presented in Chapter 5, which confirms the basic idea of this book that the practical communication systems are special cases of the generic system. An example of a derived BPSK system is shown in Fig. 3 operating at the intermediate frequency.

Chapter 8 presents modern multiuser and multicarrier CDMA and OFDM systems, and Project 4 demonstrates the procedure of mathematical modeling, simulation, and design of a CDMA system in FPGA technology.

Chapter 9 presents the fundamentals of information theory, including the theory of iterative and turbo channel coding that is demonstrated in Project 5.

Chapter 10 presents some practical aspects of discrete communication systems design in digital technology, primarily in DSP and FPGA.

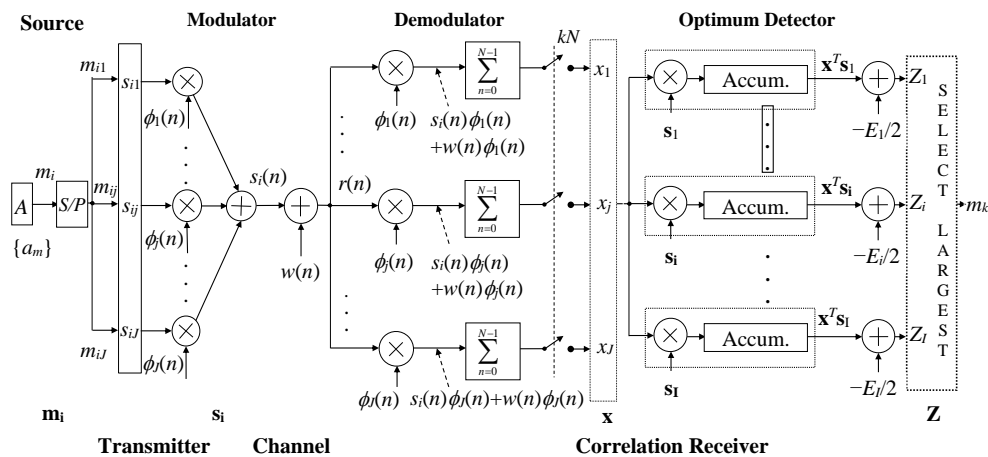


Figure 2 – Generic discrete communication system operating in the discrete-time domain
 Рис. 2 – Обобщенная дискретная система связи, работающая в дискретном времени
 Слика 2 – Генерички дискретни комуникациони систем који ради у домену дискретног времена

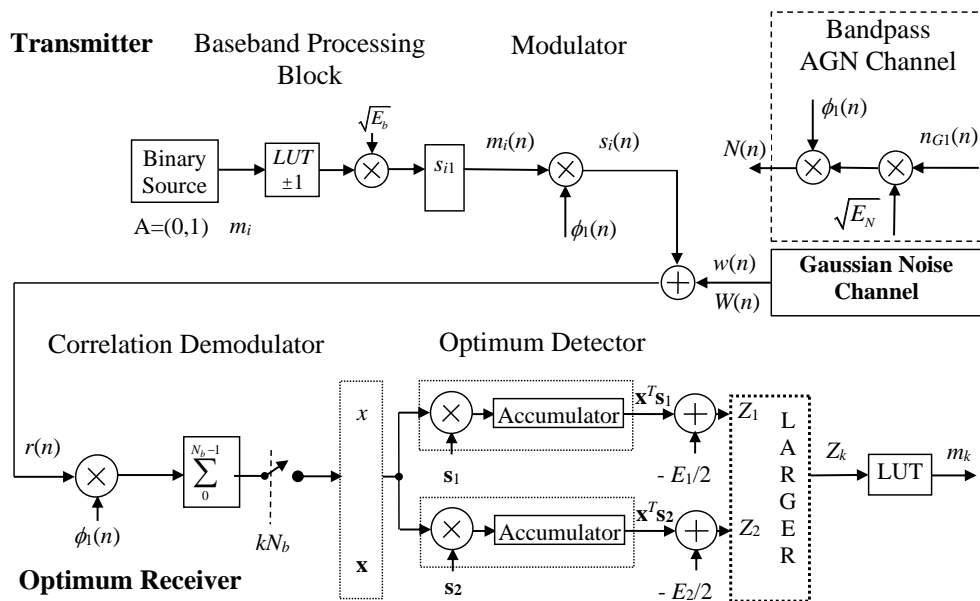


Figure 3 – Discrete BPSK, an example of a special case of the generic discrete system
 Рис. 3 – Дискретный BPSK, пример частного случая обобщенной дискретной системы
 Слика 3 – Дискретни BPSK, пример посебног случаја генеричког дискретног система

Description of chapters in the complementary part

Complementary Chapters 11 to 19 are added for three reasons. Firstly, they contain the basic theory of continuous-time and discrete-time signal processing that is essential for the understanding of mathematical models and operations of the digital and discrete transceivers, where the theory of deterministic and stochastic signal processing is used. Secondly, the unified notation and terminology in all 19 chapters simplify the understanding of their content. Thirdly, presenting the signal processing and communication systems theory with a unified notation makes this book self-sufficient, allowing readers to avoid wasting time and getting confused by reading various books with different notations. Even though a reader can be very familiar with the signal processing theory contained in the complementary chapters, it is advisable to read them before starting to work on the main 10 chapters.

Target audience of the book

The book is intended for undergraduate and graduate students doing courses in communication systems, and also for practicing engineers working on the design of transceivers in discrete communication systems. A one-semester senior-level course, for students who have had prior exposure to classical communication systems covering passband and baseband signal transmission, can use the material in Chapters 1 to 6, as well as the material in Chapter 9 supported with related complementary Chapters 11 to 15, Chapter 19 and Projects 1, 2 or 3. In a first-year postgraduate level course, the first six chapters provide students with a good review of the digital and discrete communication systems theory and the main lecturing will cover Chapters 2 to 5 and Chapters 7 to 10 that present the discrete communications systems and their design, and related Projects 1 to 5. The background theory for this course is contained in complementary Chapters 13 to 18.

For practicing engineers, who are experienced in the theory of digital communication systems, the material covered in Chapters 2 to 5 and Chapters 7 to 10 supported by complementary Chapters 13 to 18 is a good base for understanding the vital concepts in discrete communication systems. All Projects are relevant for them, Projects 4 and 5 in particular.

Supplementary material

The book contains the Supplementary Material that is composed of two parts: Solutions to the Problems in the book, and Research Projects

with offered solutions. To master the theory, key chapters contain sets of problems for students' exercises. The solutions to the problems are inside a separate book belonging to the Supplementary Material for readers. In addition to the solved problems, the book contains several real-world case studies in the form of Projects related to the advanced modeling and designs of modern communication systems based on digital and discrete-time signal processing and the application of modern technologies like DSP and FPGA. None of these Projects is a laboratory exercise but a self-contained piece of research work related to a particular book chapter, and as such can be a part of a one-semester project inside the course in discrete and digital communication systems.

Обзор книги «Дискретные системы связи»,
Автор: Стивен Бербер,
Издательство Оксфордского университета, 2021г.

Небойша Н. Гачеша
Университет обороны в г. Белград, Военная академия,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 49.00.00 Связь
ВИД СТАТЬИ: обзор книги

Резюме:

В книге приведена теория дискретных систем связи, которые представлены в виде блочных схем, определяемых математическими операторами. Для того чтобы лучше понять и сравнить взаимосвязь между двумя теориями, приведена также теория цифровых систем связи. Были определены обобщенные схемы обеих систем, которые использовались для разработки отдельных дискретных и цифровых систем в качестве их специальных случаев. В некоторых главах представлена теория обработки детерминированных и стохастических сигналов непрерывного и дискретного времени, которая способствует пониманию основных глав, в которых описаны системы связи.

Ключевые слова: дискретные системы связи, цифровые системы связи, дискретная модуляция, цифровая модуляция, теория информации и кодирования, обработка сигналов дискретного времени, обработка сигналов непрерывного времени, детерминированные сигналы, случайные сигналы.

Приказ књиге Discrete communication systems,
аутор Стеван Бербер,
Oxford University Press, 2021

Небојша Н. Гаћеша

Универзитет одбране у Београду, Војна академија,
Београд, Република Србија

ОБЛАСТ: телекомуникације
КАТЕГОРИЈА (ТИП) ЧЛАНКА: приказ књиге

Сажетак:

Ова књига садржи теорију дискретних телекомуникационих система који су приказани у облику блок шема дефинисаних помоћу математичких оператора. У циљу поређења система, додата је теорија дигиталних телекомуникационих система ради бољег разумевања односа наведених теорија. Дефинисане су генеричке шеме оба система које су коришћене да се развију појединачни дискретни и дигитални системи као њихови специјални случајеви. Комплементарна поглавља књиге садрже теорију обраде детерминистичких и стохастичких сигнала континуалног и дискретног времена која је неопходна за разумевање главних поглавља која приказују телекомуникационе системе.

Кључне речи: дискретни телекомуникациони системи, дигитални телекомуникациони системи, дискретна модулација, дигитална модулација, теорија информација и кодовања, обрада сигнала дискретног времена, обрада сигнала континуалног времена, детерминистички сигнали, случајни сигнали.

Paper received on / Дата получения работы / Датум пријема чланка: 08.08.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 24.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 25.11.2023.

© 2023 The Author. Published by Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Автор. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2023 Аутор. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons лиценцом (<http://creativecommons.org/licenses/by/3.0/rs/>).



САВРЕМЕНО НАОРУЖАЊЕ И ВОЈНА ОПРЕМА
 СОВРЕМЕННОЕ ВООРУЖЕНИЕ И ВОЕННОЕ ОБОРУДОВАНИЕ
 MODERN WEAPONS AND MILITARY EQUIPMENT

Највећи француски дрон¹



Беспосадна летелица Aarok

Прототип француске беспосадне летелице *Aarok* био је потпуно изненађење на француском аеро-митингу у Паризу. Беспосадни ваздухопловни систем *Aarok* или *UAS* представља ново појачање у домену средњих висина и дугих летова (или *MALE*). Намењен је за обавештајне, надзорне и извиђачке мисије (*intelligence, surveillance, and reconnaissance – ISR*), али и за нападне летове. У оквиру нападаких летова летелица је наоружана прецизном ракетом *AASM Hammer* која обезбеђује напад на циљеве са безбедне дистанце различитим бојевим главама.

Ову летелицу произвела је мало позната компанија *Turgis & Gaillard*, која израђује пројекте у оквиру одбрамбене индустрије. Ова фирма убрзано проширује своје капацитете за производњу разних војних средстава, од којих кулминацију представља прототип *Aarok*. Летелица има масу од 5,4 тоне при максималној полетној тежини. Величина летелице је импресивна, јер распон крила износи чак до 21 метра, тако да је она већа и од америчке беспосадне летелице *MQ-9A Reaper*. Летелицу погони турбо-пропелерски мотор *Pratt & Whitney Canada PT6* који развија снагу до 1200 КС. У компанији се размишља да се у будућности инсталирају турбо-пропелерски мотори *Safran Ardiden 3* или *GE Aviation Catalyst*. Максимална полетна тежина од 5,4 тоне укључује и носивост од 2721 кг, од чега отприлике половина отпада на убојна средства.

¹ The War Zone, June 16 2023



Компјутерска обрада слике беспосадне летелице Aarok наоружане ракетом AASM Hammer, као и противтенковским ракетама Hellfire

Беспосадна летелица може летети више од 24 сата. Ови параметри постављају Aarok у сличну категорију као што је амерички MQ-9A Reaper који се налази у наоружању француске ратне авијације.

Дизајн летелице омогућава јој полетно-слетне операције са неприпремљених површина с обзиром на врло робустан сјајни трап.

Компанија *Turgis & Gaillard* извештава да развија летелицу већ три године. Директор компаније изјавио је да је дрон намењен за извршавање разних мисија међу којима су, осим извиђачких, обавештајних и нападачких мисија, и поморско извиђање, као и извршавање мисија комуникационих релеја. Ради се о борбеном ваздушном комуникационом чворишту (*Battlefield Airborne Communications Node*) или *BACN*. То значи да летелица у овој улози може размењивати информације са великим бројем разних ваздухопловних платформи и снага на копну и мору. Овакав комуникациони систем је монтиран на авионима *E-11A*, модификованим серијама пословних млазњака типа *Bombardier Global Express* и летелице *EQ-4B Global Hawk*, која је већ ван употребе.

Компанија даље наводи да пакет опреме *ISR* укључује оптроничке и електромагнетске сензоре високих перформанси, а вероватно се ради о сензорима *Wescam MX-25* или *Euroflir 610*. Величина беспосадне летелице са великим капацитетима подвесног терета значи да ће моћи да носи

велики електро-оптички сензор (камеру), мултифункционални радар и разне обавештајне сензоре.



Доњи део трупа летелице опремљен је сензорском куполом

С друге стране, оружје чији је циљ извођење нападних мисија укључује *AASM Hammer* и има неколико начина вођења, укључујући инерцијално, сателитско и инфрацрвено. Бојеве главе се испоручују у неколико величина, од 125 кг, 250, 500 и 1000 кг.



*Летелица са ракетама *AASM Hammer* и *Hellfire**

Домет *Hammera* износи до 35 км, тако да не би требало да буде у домету руског противваздухопловног система кратког домета *Pantsir*. Ова опаска произвођача вероватно је наведена због напада руског система *Pantsir-S1* на америчку летелицу *MQ-9* у региону источне Сирије, у новембру 2022. године. Иако *Pantsir-S1* тада није успео да обори дрон, на Западу се закључило да се ради о опасном приближавању радијусу дејства руских противваздухопловних система.

И поред тога што носи ракете већег домета, беспосадна летелица *Aarok* поседује и опрему за самоодбрану, иако није јасно да ли се ради о противмерама као што су радарски или инфрацрвени мамци или о неким ометачима или дирекционалним инфрацрвеним противмерама или, можда, о комбинацији оба система.

Компанија *Turgis & Gaillard* основана је 2011. године, и њен први посао је био развој система за интеграцију француске прецизне наводећене муниције *Gerfaut*, конкретно пројектила *Hammer* испод крила транспортног авиона *C-130 Hercules*. Циљ је био да се обезбеди јефтинија ваздушна подршка и стопирају устаничке операције, као што су оне у Авганистану и Малију. Систем *Gerfaut* на крају није финализован у облику уговора за компанију, али је искуство развијања оваквог система помогло при наоружавању летелице *Aarok*. Треба поменути да је систем америчког моринског корпуса *Harvest HAWK* нудио сличан концепт систему *Gerfaut* и доживео интензивну оперативну употребу.



Лансери система *Gerfaut* за муницију *AASM Hammer* испод крила транспортног авиона *C-130 Hercules*

Компанија *Turgis & Gaillard* успела је да се брзо наметне у оквиру француске одбрамбене индустрије путем многих иновативних пројеката, нарочито у области ваздухопловства. Ради се производњи опреме за ловце *Dassault Rafale*, одржавању авиона *DHC-6* и *PC-6* француских специјалних снага, па чак и изради неке опреме за ловца *F-35*.

Ипак, *Aarok* представља најамбициознији програм компаније, а развој је финансирала сама. Компанија ради на новој беспосадној летелици која би се могла користити за поморско надгледање ексклузивних економских зона, нарочито у индо-пацифичком региону.

Француска традиционално успешно продаје оружје државама у Африци и на Блиском истоку. С обзиром на велику тражњу за средствима осматрања, и уз агресивну извозну политику, могла би убедити државе клијенте да купе њену беспосадну летелицу уместо америчких.

У смислу конкуренције, *Aarok* се налази на прилично пребункираном тржишту. Француска већ управља америчким дроном *MQ-9A Reaper*. Купила је шест дрона типа *Reaper Block 1* и шест типа *Reaper Block 5*. Летелице типа *Reaper Block 5* могу бити наоружане прецизним навођеним бомбама *GBU-12 Paveway*, као и ракетама ваздух-земља типа *AGM-114 Hellfire*.



Француски војници скидају ласерски вођену бомбу са беспилотне летелице *Reaper* у француској бази у Нигерији.

Француске летелице типа *Reaper* набављене су због хитних захтева за дејства у области *ISR* у оквиру француских војних операција у Малију,

укључујући и дуге летове преко северног дела земље у потрази за милитантима.

У будућности, француска компанија *Turgis & Gaillard* нада се да ће успети да обезбеди, за француске потребе, наследника америчке летелице *Reaper*, који би могао бити ефикасан у пару са будућим евродроном.

Евродрон је беспосадна летелица са два турбо-пропелерска мотора и врши активности на великим удаљеностима. Ради се о летелици са максималном полетном масом до 10886 кг, корисним теретом до 2247 кг и распоном крила од преко 29 метара.


Овај дрон развијају компанија *Airbus*, *Dassault Aviation* и *Leonardo*, а набавиће га Француска, Италија и Шпанија. Први лет се очекује средином 2027. године, али увођење у оперативну употребу се не очекује пре 2030. године.

Као и амерички *Reaper*, *Aarok* ће бити у конкуренцији са турском летелицом *Baykar Bayraktar Akinci*, која припада истој класи. Овај дрон се већ налази у наоружању турских оружаних снага, Пакистана и Либије, а наручили су га Азербејџан и Киргистан.

Што се тиче временских рокова, француска компанија је најавила да се први лет очекује до краја 2023. године. То би значило да би увођење у оперативну употребу могло да се очекује средином 2025. године.

У рату у Украјини се показало да беспилотне летелице опстају чак и у оспореном окружењу. С друге стране, у западним земљама споро се развијају наоружани дрoнови, па Француска зависи од америчких беспосадних летелица *Reaper* за ударне нападе. Оваква ситуација обезбеђује државама као што су Турска и Кина да доминирају у продаји наоружаних дрoнова на тржишту с обзиром на то да је тешко доћи до америчких наоружаних дрoнова.

Уколико би компанија *Turgis & Gaillard* успела да на тржиште избаци наоружану летелицу класе *MALE* у наведеним роковима, то би било од интереса не само за француске оружане снаге већ и за друге заинтересоване. Поред тога, уколико се за *Aarok* понуди нижа цена од цене ривалских летелица, то би представљало врло атрактивну понуду на овом тржишту.

Драган М. Вучковић (*Dragan M. Vučković*),
e-mail: draganvuckovic64@gmail.com,
ORCID iD:  <https://orcid.org/0000-0003-1620-5601>

Руски Okhotnik у оперативној употреби²

Америчка беспилотна летелица *Sentinel RQ-170* постала је позната као невидљиви ненаоружани дрон за осматрање терена на неким од најопаснијих области.



X-45B demonstrator

Није познато у којој је фази амерички невидљиви борбени дрон. Пре неколико година Американци су започели програм под називом *UCLASS* који је развијао морнаричку беспилотну летелицу која је требало да учествује у више различитих мисија, у улози нападача, беспилотног ваздушног танкера или осматрача. На основу овог програма, дошло се до интересантне иновације под називом *X-45B demonstrator*. То је прва невидљива беспилотна летелица која полеће са носача авиона. Овај програм је изнедрио први морнарички беспилотни танкер.

Русија званично има само два прототипа невидљивих беспилотних летелица *S-70 Okhotnik*. Према информацијама доступних Западу, два прототипа руских дрона *S-70 Okhotnik* су у току летног тестирања, а још два су у фази израде/летног тестирања. Први прототип полетео је први пут у августу 2019. У фебруару 2021. године, из руског војноиндустријског комплекса је објављено да Новосибирски авио-завод Чкалов (НАЗ) гради још три прототипа тешких дрона *S-70 Okhotnik*.

² Warrior Maven, Jun 30, 2023, The War Zone, December 14, 2021



S-70 Okhotnik

По руским изворима, поменути авио-завод прави још три прототипа беспилотне летелице S-70.

Други прототип је унео измене у аеродинамику и електронику на основу оперативног искуства са првим S-70.

У марту 2021. године објављено је да је у току производња другог прототипа S-70

Поред побољшане електронике и софтвера, дрон би имао посебно пројектовану млазницу за побољшану невидљивост задњег аспекта.



Првобитна млазница дрона која ће у наредним верзијама бити промењена ради бољих стелт карактеристика

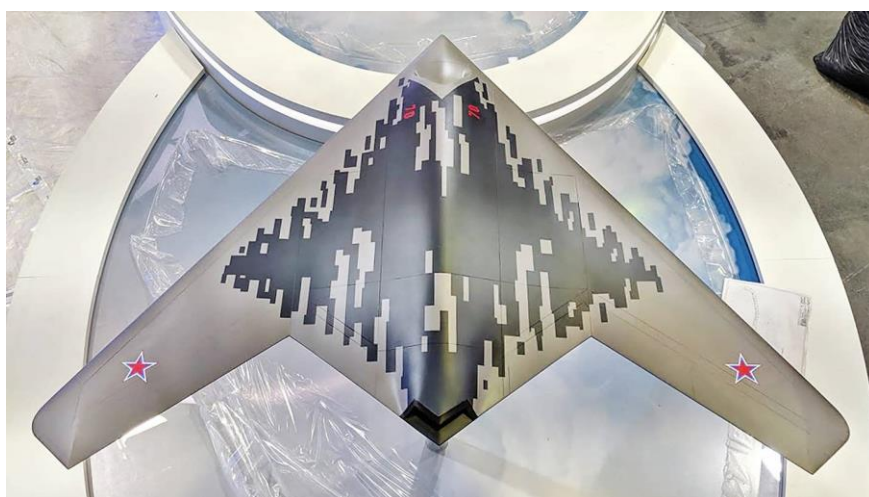
Године 2021. руски извори навели су да ће серијски уговор за набавку *S-70 Okhotnik* бити закључен у року од шест месеци. Летно тестирање другог прототипа почело је у јулу 2022. године.

Русија је можда оперативно распоредила две беспилотне летелице *S-70*. Такође, могуће је да ће два додатна прототипа, у развоју од 2021. године, бити доступна руским снагама. Могуће је чак и да су већ оперативно распоређени.

Руски извори наводе да је *S-70 Okhotnik* развијен да делује под контролом пилота невидљивог ловца *Su-57*, који може да контролише већи број ових дронава.



Su-57 може да контролише већи број дронава *S-70*



S-70 Okhotnik

Руска беспилотна борбена летелица *S-70 Okhotnik* (ловац) наоружана је пројектилама ваздух-земља и једрећим као и навођеним бомбама које се налазе у трупку летелице, што не нарушава стелт карактеристике.

Ова летелица делује као „крилни колега” ловцу *Su-57*, има функције вештачке интелигенције и може да стигне до свемира када је опремљена одговарајућим моторима.

Сједињене Државе су покушале да развију беспилотну летелицу са сличним карактеристикама и перформансама, али су одустале од пројекта након што њени инжењери нису успели да превазиђу техничке препреке.

Летелица *S-70 Okhotnik* има турбомлазни мотор *AL-31*, лети брзином од 1.000 км на сат и има долет до 6.000 километара. Опремљена је електро-оптичким нишанима, радио-везом и „другим врстама опреме за извиђање”, како, наводи руско Министарство одбране. Треба рећи и да је већа од западних летелица тог типа. Са распоном крила од 20 м и дужином од 14 м, маса дрона је, наводно, око 20 тона (у поређењу са 4,9 т колико има *Dassault Neuron* и 6,3 т *X-47B*, компаније *Northrop Grumman*). У два унутрашња спремника ове беспилотне летелице требало би да стане до 2,8 тона оружја.

Први борбени дрон *S-70 Okhotnik* требало би да буде испоручен руским оружаним снагама 2024. године. Међутим, Министарство одбране је очигледно захтевало да се убрза експериментални рад, тако да су већ одавно примећене две верзије на сателитским снимцима.

Амерички стручњак за беспилотне летелице и руско-војну технологију, иако је скептичан у погледу способности *S-70* у свемиру, изјавио је да је ова летелица првобитно дизајнирана за „продор непријатељског ПВО”.

Основна идеја јесте да *Su-57* и група дрона *Okhotnik* уништи велике стратешке циљеве, као што су командни центри или ПВО комплекси, како би олакшали пут великим бомбардерима као што су *Tu-160*, *Tu-22* или *MiG-31* који носе крстарећу ракету *X-101* или хиперсоничну ракету *Кинџал*.

Русија је можда почела да користи своје ударне беспилотне летелице *S-70 Okhotnik* против Украјине. То се може констатовати на основу фотографија дрона који лети изнад Украјине, које су објавили украјински телеграм канали и пренели бројни медији.


Спекулише се да је дрон погодио војне објекте оружаних снага Украјине у Сумској области.

У јуну 2022. године, часопис *Janes* извештава, цитирајући РИА Новости, да је *S-70* извео своје прво пробно лансирање прецизно навођене муниције на земаљске циљеве 28. маја 2022. године. Дрон је лансирао ракете ваздух-земља развијене за Сухој *Su-57* са посадом.

Такође, часопис наводи да је ракета вероватно била крстарећа ракета *Kh-59Mk2* (*X-59* верзије 2), нови развој тешке тактичке ракете серије *X-59* која је ушла у употребу почетком осамдесетих година.

Процене домета и носивости *X-59Mk2* увелико варирају, али је вероватно да може да погоди циљеве удаљене најмање 250 километра док носи бојеву главу од 220 килограма. Модуларна природа дизајна може омогућити вишеструке конфигурације, као што су већи одељци за гориво или замене мањим бојевим главама.

„Известија” је, у фебруару 2020, писала да је планирајућа бомба *Grom 9-A-7759* интегрисана са летелицом *Okhotnik*. Она може да носи четири ракете *Grom* у свом унутрашњем одељку за бомбе. У међувремену, *Okhotnik* је на провери у Украјини.

Драган М. Вучковић (*Dragan M. Vučković*),
e-mail: draganvuckovic64@gmail.com,
ORCID iD:  <https://orcid.org/0000-0003-1620-5601>

Унапређена верзија хеликоптера *Ка-52М* у Украјини³



Ка-52М

Појавиле су се прве фотографије нове верзије модернизованог борбеног хеликоптера *Ка-52М* у руској служби, па постоји велика вероватноћа да већ учествује у сукобу у Украјини. Док је основни *Ка-52М Nokut* постао препознатљиво оружје руских снага, претрпевши велике губитке, али и наносећи их украјинском оклопу, ова верзија побољшане верзије *Ка-52М* нигде није виђена до прошле недеље.

Хеликоптер *Ка-52М* представљен је на три фотографије постављене на обично добро обавештеном каналу *Fighterbomber* на Телеграму. Поред

³ The War Zone, Jul 21, 2023

осталих, овај канал врши прикупљање средстава за руске авијатичаре који су учествовали у украјинским ратним летовима: одела, ципеле, радио-апарате, навигационе уређаје, комплете прве помоћи итд. На фотографијама објављеним 14. јула, виде се авијатичари са поклонима у позадини нове верзије *Ка-52*.



Руски пилот испред унапређене верзије хеликоптера Ка-52М

Хеликоптер који се види на фотографијама сајта *Fighterbomber* свеже је офарбан, што указује да је недавно испоручен. Фотографије ове врсте, на овом каналу, раније су, углавном, настајале на распоређеним локацијама у Украјини, или у ваздушним базама у Русији које се користе за подршку тамошњој кампањи. Иако не можемо бити сигурни да ове фотографије потичу из Украјине, или из руске ваздушне базе коришћене у сукобу, веза са напорима телеграм канала *Fighterbomber* да набаве опрему за посаде сугерише да је то бар вероватно.

Медијски извештаји о употреби *Ка-52М* у Украјини већ су се појавили, али нису били поткрепљени никаквим доказима. На пример, у септембру 2022, руска државна новинска агенција ТАСС описала је „успешне тестове овог модернизованог хеликоптера током специјалне операције у Украјини”.

Компанија Камов је, 5. априла 2019. године, добила уговор од Министарства одбране Русије за истраживачко-развојне радове Avangard-4, чији је циљ био развој модернизованог Ка-52М (хеликоптер Ми-28НМ који се развија у исто време носи кодни назив Avangard-3). Стварни радови су почели много раније од доделе уговора, а нова опрема и наоружање који се сада користе у хеликоптеру Ка-52М до тада су били скоро спремни.

У јуну 2020. године, фабрика Прогрес у Арсењеву на руском Далеком истоку, која производи Ка-52, добила је наруџбину да два хеликоптера конвертује у верзије Ка-52М ради тестирања. Први Ка-52М је извео свој први лет после конверзије 10. августа 2020. године. Према уговору, Ка-52М је требало да заврши сва испитивања и да буде спреман за серијску производњу до краја септембра 2022. године.

Први Ка-52М је приказан јавности током руског Међународног сајма авијације и свемира (МАКС), у јулу 2021. године, а затим на изложби Армија-2021 следећег августа. Хеликоптер је добио модернизовану куполу за електро-оптичко нишањење *GOES-451M*, ажурирани комуникациони пакет *BKS-50M (Bortovoi Kompleks Svyazi)*, као и систем управљања спремницима *SUO-806PM (Sistema Upravleniya Oruzhiyem)*, што му омогућава коришћење новог оружја. Најзначајнији додатак наоружању хеликоптера јесте увођење вођене ракете *LMUR* са дометом до петнаест километара (која је описана у претходним бројевима Војнотехничког гласника).



Вођена ракета LMUR



Тестна верзија Ка-52М са вођеном ракетом LMUR

Уведене су и друге надоградње самог хеликоптера. Лопатице ротора Ка-52М имају снажнији грејни елемент, који омогућава хеликоптеру да ради у ширем температурном опсегу, укључујући и Арктик, што је у посебном фокусу недавне руске војне стратегије. Стајни трап има тачкове са повећаном носивошћу и отпорношћу на хабање, а хеликоптер има и спољно ЛЕД осветљење. Кокпит за посаду има побољшану ергономију и такође је боље прилагођен летењу са наочарима за ноћно посматрање (НВГ).

Што се тиче спецификација, Ка-52М (познат у фабрици као *izdeliye 800.50*) има максималну масу при полетању од око 12 500 кг, максималну брзину од 300 км на сат, плафон од 5500 м и долет од 460 км.

Производња се повећава

Уговор за прву партију од 30 хеликоптера Ка-52М за Ваздушно-космичке снаге Русије потписан је 24. августа 2021. године, током форума Армија-2021; 15 хеликоптера је требало да буде испоручено 2022. и 15 2023. године. Вероватно је овај уговор већ реализован. Током следећег форума Армија-2022, руско Министарство одбране дало је још једну поруџбину за непознати број ових хеликоптера. У јулу 2023. године, руски министар одбране Сергеј Шојгу изјавио је да су испоруке Ка-52 у 2023. „удвостручене” у односу на 2022. годину, односно око 30 хеликоптера, ако је то тачно.

После око 18 месеци борби, Русија је у Украјини изгубила скоро 40 борбених хеликоптера Ка-52 од око 140 колико их је имала на почетку рата (у погледу свих типова јуришних хеликоптера, Русија је изгубила око 70 од преко 400 на почетку рата). Поред Ка-52, у Русији се производе још два типа борбених хеликоптера – *Mi-28N/NM* и *Mi-35M* који се производе у фабрици Роствертол у Ростову на Дону. Уз информацију о удвостручењу

производње хеликоптера *Ka-52*, руски министар Шојгу је рекао да је производња *Mi-28* повећана за фактор три у 2023. у односу на 2022. годину (тј. на приближно 50 годишње).

Нови циљни терет *GOES-451M*

На новој фотографији хеликоптера *Ka-52M* стрелица број један показује електрооптичку подвесну куполу *GOES-451M* која је инсталирана испод предњег дела трупа; стандардна верзија хеликоптера има у овом положају куполу *GOES-451*. У куполи се налази термовизијска камера, ТВ камера, ласерски даљиномер/озрачивач, излаз ласерског снопа за противтенковске ракете, као и ласерски трагач.



GOES-451 (лево) и модернизована електрооптичка купола *GOES-451M* (десно).
Извор: Piotr Butowski

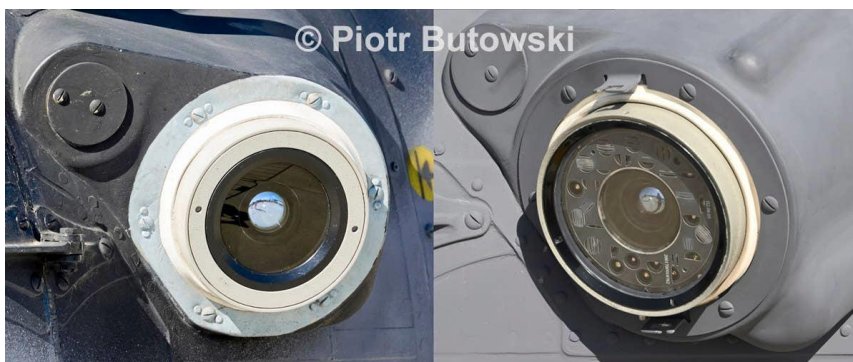


Сензори куполе *GOES-451M* имају повећан домет детекције и препознавања како би одговарали дометима нових типова оружја, укључујући пројектил *LMUR*. Произвођач корисног терета, УОМЗ из Јекатеринбурга, објављује домет детекције тенка од 15 км помоћу ТВ канала и 12 км за термовизијски канал; домет препознавања циља је 12 км и 7,5 км и 8 км респективно.

Нови *L418 monobloc* пакет за самоодбрану

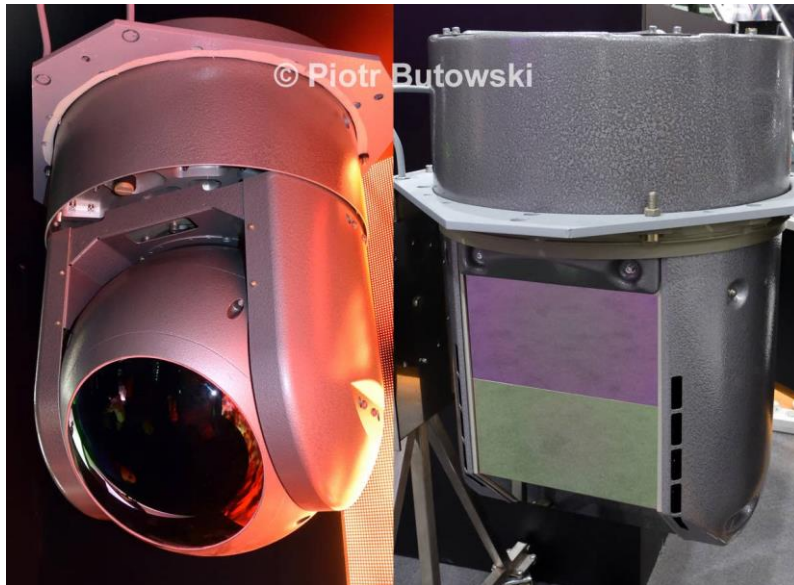
Стрелица број два показује ултраљубичасти сензор упозорења о приближавању пројектила (*MAWS*) *L418-2*, који производи компанија ГИПО у Казању, и представља део пакета за самоодбрану *L418 monobloc*. Обични *Ka-52*, као и раније виђени прототипови *Ka-52M*, имају систем *L370P2 Vitebsk* са *L370-2 MAWS* на овој позицији. Четири таква сензора су постављена на бочним странама предњег трупа и репног носача, покривајући читавих 360 степени око хеликоптера.

Сензоре *L418 monobloc* производи компанија НИИ Екран у Самари. То је модернизација система *L370 Vitebsk*, који ради на ширем опсегу фреквенција и на већим дометима.



Ултраљубичасти сензори за упозорење на долазеће пројектиле – стандардни *L370-2* (лево) и модернизовани *L418-2*. Извор: *Piotr Butowski*

Иако се на новим фотографијама то не види, хеликоптер *Ka-52M* највероватније има и друге нове компоненте пакета *L418*, пре свега два система усмерених инфрацрвених противмера (*DIRCM*) *L418-5*, произвођача компаније СКБ Зенит у Зеленограду, постављена на бочним странама доњег дела трупа, непосредно испред главног стајног трапа. Нови ометач *L418-5* је угаоног облика, док је претходни *L370-5* изгледао као ротирајућа сфера (под надимком „јаје живота”); унутра се налази нова лампа *SP3-1500* (раније *SP2-1500*) која генерише модулирано инфрацрвено и ултраљубичасто зрачење ради ометања инфрацрвених трагача ракета ваздух-ваздух и земља-ваздух.



Стандардни систем за усмерене инфрацрвене противмере L370-5 (лево) и модернизовани L418-5 (десно). Извор: Piotr Butowski

Занимљиво је да су сензори *L418 monobloc* уграђени на хеликоптере *Ka-52E* који су продати Египту много пре него што су се појавили на руским хеликоптерима. То је резултат строжих формалних захтева руског Министарства одбране за увођење нове опреме, а можда и због додатних функција које захтева руска војска. Увођење нове опреме ове врсте у Русији захтева вишестепена испитивања која нису нужно потребна страном купцу. На сличан начин су хеликоптери *Mi-28NE* који су испоручени Ираку добили радаре, у фебруару 2015. године, док су испоруке хеликоптера са радарима ваздушно-космичким снагама Русије почеле тек крајем 2017. године.

Сада, у ратним условима, Русија је знатно смањила такве захтеве и уводи у борбу опрему која очигледно још није потпуно проверена, као што је, на пример, *УМПК* крилни комплет/модул за навођење, инсталиран на бомбама опште намене.

Нови радар

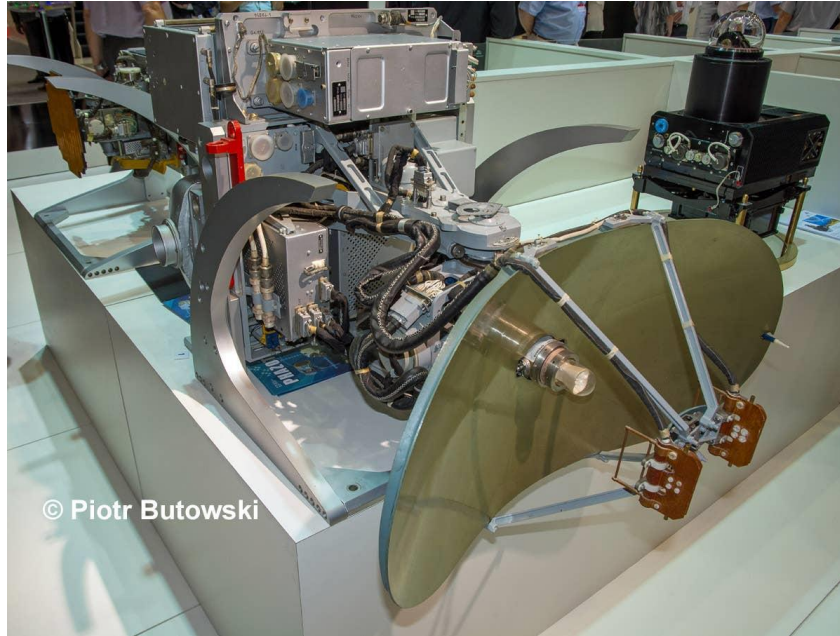
Најинтересантнији је нови радар на хеликоптеру *Ka-52M*, који се види на недавно објављеним фотографијама. Стрелица број три показује мали отвор за ваздух на доњој страни радара у предњем делу трупа, док се на другој страни, симетрично, налази још један сличан усисник ваздуха. Таквих улаза нема ни у једном од раније виђених хеликоптера *Ka-52*.



Један већи улаз, али иначе сличан, види се у прототипу поморског борбеног хеликоптера *Ka-52K* под бројем „103”, што доводи до вероватног закључка о сврси ових улаза. На хеликоптеру *Ka-52K* „103” овај улаз се користи за хлађење антене радара са активним електронским скенирањем *Rezets (AESA)* који се тестира на овом хеликоптеру.

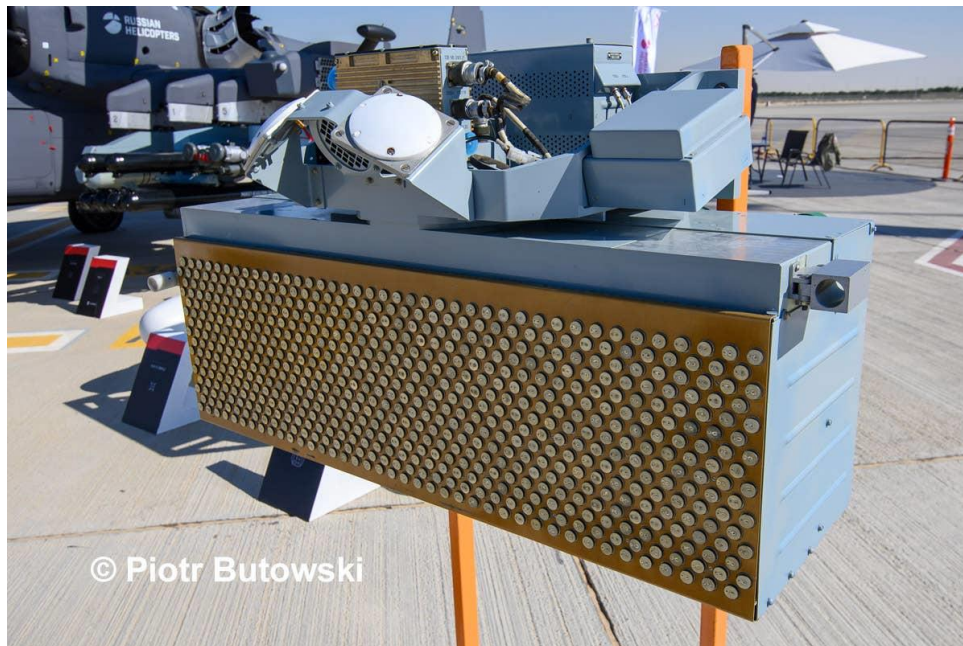
Прототипови *Ka-52M* имају исти радар као и обични *Ka-52*, *FH01 Arbalet-52*, који производи компанија Фазотрон-НИИР из Москве. То је радар Ка-таласа (таласне дужине 8 мм) са широком механичком антеном од 80 цм у носу хеликоптера. Даљина детекције за велики земаљски циљ (нпр. железнички мост) износи 25 км, или 12,5 км за тенк. Недостатак радара *FH01* јесте немогућност директног вођења навођених пројектила. За навођење оружја, информација о циљу преноси се са радара на електрооптички систем *GOES-451*, који је главни сензор циљања *Ka-52*.

Што се тиче радара на новој верзији хеликоптера *Ka-52M*, највероватније се ради о радару *V006 Rezets*, компаније Заслон из Санкт Петербурга (исте компаније која израђује радар *V004* који користи ловац-бомбардер *Su-34 Fullback*). Радар *V006*, или *RZ-001 Rezets* (резач), има фиксну *AESA* антену са 640 примопредајних модула. Ради у X-опсеги и, према произвођачу, може да открије групу тенкова на 40 км и борбену летелицу до 50 км. Радар *Rezets* је ваздушно хлађен, због чега су му потребни додатни усисници ваздуха.



© Piotr Butowski

FH01 Arbalet-52 радар са Ка-52. Извор: Piotr Butowski



© Piotr Butowski


*Радар V006, или RZ-001 Rezets, у новој конфигурацији на хеликоптеру Ка-52М.
Извор: Piotr Butowski*

Иако је радар *Rezets* највероватнија опција за *Ka-52M*, није и једина. Компанија Фазотрон-НИИР, произвођач актуелног радара *FH01*, такође има своју понуду. Модернизовани радар *FH02* има две одвојене антене: механичку за *Ka* таласни опсег и *AESA* за *X* таласни опсег. То решење омогућава истовремено скенирање циљева на површини и ваздушном простору, имплементацију напредних алгоритама за детекцију и праћење циљева, као и већу поузданост. *X*-опсег даје много већи домет, иако на рачун ниже резолуције. Према тврдњама компаније, тенк се може открити на удаљености до 20 км у домету *Ka* опсега или до 35 км у домету *X* таласа.

Потребно је сачекати објављивање нових фотографија хеликоптера *Ka-52M* у његовој новој варијанти, како би била јаснија конфигурација ове нове верзије и сазнало се да ли је већ у Украјини. У овом тренутку, то се, свакако, чини вероватним. У сваком случају, јасно је да ће хеликоптер, генерално, укључујући и његову оригиналну варијанту *Ka-52*, остати кључни систем наоружања за руске ваздушно-космичке снаге све док украјинска кампања траје.

Иначе, *Ka-52* је хеликоптер који је највише коришћен у украјинском сукобу, као што је то био *Mil-24* у Авганистану. Нажалост, и губици су велики (на интернету се појављују подаци о око 40 уништених апарата). На почетку рата ови хеликоптери нису ни употребљавани у својој основној намени. На интернету су се, углавном, појављивали снимци испљивања невођених ракета, што је значило да хеликоптер мора дубоко да уђе у украјински ваздушни простор, што га је чинило врло рањивим на лаке преносне противваздухопловне системе. С друге стране, испљивање невођених ракета под одређеним нападним углом није прецизно, а ни његове противмере нису се чиниле ефикасним.

У другом делу сукоба, током 2023. године, нарочито око украјинског покушаја пробоја „Суровикинове” линије, *Ka-52* је коначно почео да се користи како су то конструктори и замислили, што значи превасходно у противоклопној борби са противтенковским навођеним ракетама домета и преко 10 километара. Хеликоптер *Ka-52* је, заједно са осталим видовима и родовима војске, врло ефикасно допринео уништењу великог броја (углавном НАТО) оклопних возила са већих даљина, не доводећи своју посаду у опасност. Модернизација је уследила након борбених искустава, али је хеликоптер коначно употребљен у својој правој сврси.

Драган М. Вучковић (*Dragan M. Vučković*),
e-mail: draganvuckovic64@gmail.com,
ORCID iD:  <https://orcid.org/0000-0003-1620-5601>

ПОЗИВ И УПУТСТВО АУТОРИМА

ПРИГЛАШЕНИЕ И ИНСТРУКЦИЈА ДЛЈА АВТОРОВ РАБОТ

CALL FOR PAPERS AND INSTRUCTIONS FOR AUTHORS

ПОЗИВ И УПУТСТВО АУТОРИМА О НАЧИНУ ПРИПРЕМЕ ЧЛАНКА

Упутство ауторима о начину припреме чланка за објављивање у *Војнотехничком гласнику* урађено је на основу Правилника о категоризацији и рангирању научних часописа Министарства просвете, науке и технолошког развоја Републике Србије ("Службени гласник РС", број 159/20). Примена овог Правилника првенствено служи унапређењу квалитета домаћих часописа и њиховог потпунијег укључивања у међународни систем размене научних информација.

Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (втг.мо.упр.срб, www.vtg.mod.gov.rs, ISSN 0042-8469 – штампано издање, e-ISSN 2217-4753 – online, UDC 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; <https://doi.org/10.5937/VojnotehnickiGlasnik>), јесте рецензирани научни часопис.

Власници часописа су Министарство одбране Републике Србије и Војска Србије. Издавач и финансијер часописа је Универзитет одбране у Београду (Војна академија).

Програмска оријентација часописа заснива се на годишњој категоризацији часописа, коју врши надлежно државно министарство у одређеним областима, као и на његовом индексирању у међународним индексним базама.

Часопис обухвата научне, односно стручне области у оквиру образовно-научног поља **природно-математичких наука**, као и у оквиру образовно-научног поља **техничко-технолошких наука**, а нарочито области **одбрамбених наука и технологија**. Објављује теоријска и практична достигнућа која доприносе усавршавању свих припадника српске, регионалне и међународне академске заједнице, а посебно припадника војски и министарстава одбране. Публикује радове са уравнотеженим извештавањем о аналитичким, експерименталним и примењеним истраживањима, као и нумеричким симулацијама, обухватајући различите дисциплине. Објављени материјали су високог квалитета и релевантности, написани на начин који их чини доступним широкој читалачкој публици. Сви радови који извештавају о оригиналним теоријским и/или практично оријентисаним истраживањима или проширеним верзијама већ објављених радова са конференција су добродошли. Радови за објављивање одабирају се двоструко слепим поступком рецензије како би се осигурала оригиналност, релевантност и читљивост. Притом циљ није само да се квалитет објављених радова одржи високим већ и да се обезбеди правовремени, темељни и уравнотежени поступак рецензије.

Уређивачка политика *Војнотехничког гласника* заснива се на препорукама Одбора за етичност у издаваштву (COPE Core Practices) и заједничким принципима транспарентности и најбоље праксе у издаваштву COPE, DOAJ, OASPA и WAME, као и на најбољим прихваћеним праксама у научном издаваштву. *Војнотехнички гласник* је члан COPE (Committee on Publication Ethics) од 2. маја 2018. године и члан OASPA (Open Access Scholarly Publishers Association) од од 27. новембра 2015. године.

Министарство просвете, науке и технолошког развоја Републике Србије утврдило је дана 25. 10. 2022. године категоризацију *Војнотехничког гласника*, за 2022. годину:

- на листи часописа за рачунарске науке:
категирија врхунски часопис националног значаја (M51),
- на листи часописа за електронику, телекомуникације и информационе технологије:
категирија врхунски часопис националног значаја (M51),
- на листи часописа за машинство:
категирија врхунски часопис националног значаја (M51),
- на листи часописа за материјале и хемијске технологије:
категирија врхунски часопис националног значаја (M51).

Усвојене листе домаћих часописа за 2022. годину могу се видети на сајту *Војнотехничког гласника*, страница *Категоризација часописа*.

Детаљније информације могу се пронаћи и на сајту Министарства просвете, науке и технолошког развоја Републике Србије.

Подаци о категоризацији могу се пратити и на сајту КОБСОН-а (Конзорцијум библиотека Србије за обједињену набавку).

Категоризација часописа извршена је према Правилнику о категоризацији и рангирању научних часописа Министарства просвете, науке и технолошког развоја Републике Србије ("Службени гласник РС", број 159/20).

Часопис се прати у контексту Српског цитатног индекса – СЦиндекс (база података домаћих научних часописа), Научно-информационог система Redalyc и Руског индекса научног цитирања (РИНЦ). Подвргнут је сталном вредновању (мониторингу) у зависности од утицајности (импакта) у самим базама. Детаљи о индексирању могу се видети на сајту *Војнотехничког гласника*, страница *Индексирање часописа*.

Војнотехнички гласник, у погледу свог садржаја, пружа могућност отвореног приступа (DIAMOND OPEN ACCESS) и примењује Creative Commons (CC BY) одредбе о ауторским правима. Детаљи о ауторским правима могу се видети на сајту часописа, страница *Ауторска права и политика самоархивирања*.

Радови се предају путем онлајн система за електронско уређивање АСИСТЕНТ, који је развио Центар за евалуацију у образовању и науци (ЦЕОН).

Приступ и регистрација за сервис врше се на сајту www.vtg.mod.gov.rs, преко странице АСИСТЕНТ или СЦИНДЕКС, односно директно на линку aseestant.ceon.rs/index.php/vtg.

Детаљно упутство о регистрацији и пријави за сервис налази се на сајту www.vtg.mod.gov.rs, страница *Упутство за АСИСТЕНТ*.

Потребно је да се сви аутори који подносе рукопис за објављивање у *Војнотехничком гласнику* региструју у регистар ORCID (Open Researcher and Contributor ID), према упутству на страници сајта *Регистрација за добијање ORCID идентификационе шифре*.

Војнотехнички гласник објављује чланке на енглеском језику (arial, величина слова 11 pt, проред Single).

Поступак припреме, писања и уређивања чланка треба да буде у сагласности са *Изјавом о етичком поступању* (<http://www.vtg.mod.gov.rs/izjava-o-etickom-postupanju.html>).

Чланак треба да садржи сажетак са кључним речима, увод (мотивацију за рад), разраду (адекватан преглед репрезентативности рада у његовој области, јасну изјаву о новини у представљеном истраживању, одговарајућу теоријску



позадину, један или више примера за демонстрирање и дискусију о представљеним идејама), закључак и литературу (без нумерације наслова и поднаслова). Обим чланка треба да буде до једног ауторског табака (16 страница формата А4 са проредом Single), а највише 24 странице.

Чланак треба да буде написан на обрасцу за писање чланка, који се у електронској форми може преузети са сајта на страници *Образац за писање чланка*.

Наслов

Наслов треба да одражава тему чланка. У интересу је часописа и аутора да се користе речи прикладне за индексирање и претраживање. Ако таквих речи нема у наслову, пожељно је да се придода и поднаслов.

Текући наслов

Текући наслов се исписује са стране сваке странице чланка ради лакше идентификације, посебно копија чланака у електронском облику. Садржи презиме и иницијал имена аутора (ако аутора има више, преостали се означавају са „et al.“ или „и др.“), наслове рада и часописа и колацију (година, волумен, свеска, почетна и завршна страница). Наслови часописа и чланка могу се дати у скраћеном облику.

Име аутора

Наводи се пуно име и презиме (свих) аутора. Веома је пожељно да се наведу и средња слова аутора. Имена и презимена домаћих аутора увек се исписују у оригиналном облику (са српским дијакритичким знаковима), независно од језика на којем је написан рад.

Назив установе аутора (афилијација)

Наводи се пун (званични) назив и седиште установе у којој је аутор запослен, а евентуално и назив установе у којој је аутор обавио истраживање. У сложеним организацијама наводи се укупна хијерархија (нпр. Универзитет одбране у Београду, Војна академија, Катедра природно-математичких наука). Бар једна организација у хијерархији мора бити правно лице. Ако аутора има више, а неки потичу из исте установе, мора се, посебним ознакама или на други начин, назначити из које од наведених установа потиче сваки од наведених аутора. Афилијација се исписује непосредно након имена аутора. Функција и звање аутора се не наводе.

Контакт подаци

Адреса или е-адреса свих аутора даје се поред имена и презимена аутора.

Категорија (тип) чланка

Категоризација чланака обавеза је уредништва и од посебне је важности. Категорију чланка могу предлагати рецензенти и чланови уредништва, односно уредници рубрика, али одговорност за категоризацију сноси искључиво главни уредник. Чланци у *Војнотехничком гласнику* класификују се на научне и стручне чланке.

Научни чланак је:

- оригиналан научни рад (рад у којем се износе претходно необјављени резултати сопствених истраживања научним методом);
- прегледни рад (рад који садржи оригиналан, детаљан и критички приказ истраживачког проблема или подручја у којем је аутор остварио одређени допринос, видљив на основу аутоцитата);

– кратко или претходно саопштење (оригинални научни рад пуног формата, али мањег обима или прелиминарног карактера);

– научна критика, односно полемика (расправа на одређену научну тему, заснована искључиво на научној аргументацији) и осврти.

Изузетно, у неким областима, научни рад у часопису може имати облик монографске студије, као и критичког издања научне грађе (историјско-архивске, лексикографске, библиографске, прегледа података и сл.), дотад непознате или недовољно приступачне за научна истраживања.

Радови класификовани као научни морају имати бар две позитивне рецензије.

Ако се у часопису објављују и прилози ваннаучног карактера, научни чланци треба да буду груписани и јасно издвојени у првом делу свеске.

Стручни чланак је:

– стручни рад (прилог у којем се нуде искуства корисна за унапређење професионалне праксе, али која нису нужно заснована на научном методу);

– информативни прилог (уводник, коментар и сл.);

– приказ (књиге, рачунарског програма, случаја, научног догађаја, и сл).

Пожељно је да обим кратких саопштења буде 4 до 7 страница, научних чланака и студија случаја 10 до 14 страница, док прегледни радови могу бити и дужи. Број страница није строго ограничен и, уз одговарајуће образложење, пријављени чланци такође могу бити дужи или краћи.

Ако су радови који су претходно објављени на конференцији проширени, уредници ће проверити да ли је додато довољно новог материјала који испуњава стандарде часописа и квалификује поднесак за поступак рецензије. Додати материјал не сме бити претходно објављен. Нови резултати нису нужно потребни, али су пожељни. Међутим, поднесак треба да садржи проширене кључне идеје, примере, разраде, итд., који су претходно били садржани у поднеску са конференције.

Језик рада

Језик рада треба да буде енглески.

Текст мора бити језички и стилски дотеран, систематизован, без скраћеница (осим стандардних). Све физичке величине морају бити изражене у Међународном систему мерних јединица – SI. Редослед образаца (формула) означава се редним бројевима, са десне стране у округлим заградама.

Сажетак

Сажетак јесте кратак информативан приказ садржаја чланка који читаоцу омогућава да брзо и тачно оцени његову релевантност. У интересу је уредништава и аутора да сажетак садржи термине који се често користе за индексирање и претрагу чланака. Саставни делови сажетка су увод/циљ истраживања, методи, резултати и закључак. Сажетак треба да има од 100 до 250 речи и треба да се налази између заглавља (наслов, имена аутора и др.) и кључних речи, након којих следи текст чланка.

Кључне речи

Кључне речи су термини или фразе које адекватно представљају садржај чланка за потребе индексирања и претраживања. Треба их доделивати ослањајући се на неки међународни извор (попис, речник или тезаурус) који је најшире прихваћен или унутар дате научне области. За нпр. науку уопште, то је листа кључних речи Web of Science. Број кључних речи не може бити већи од 10, а у

интересу је уредништва и аутора да учесталост њихове употребе буде што већа. У чланку се пишу непосредно након сажетка.

Систем АСИСТЕНТ у ту сврху користи специјалну алатку KWASS: аутоматско екстраховање кључних речи из дисциплинарних тезауруса/речника по избору и рутине за њихов одабир, тј. прихватање односно одбацавање од стране аутора и/или уредника.

Датум прихватања чланка

Датум када је уредништво примило чланак, датум када је уредништво коначно прихватило чланак за објављивање, као и датуми када су у међувремену достављене евентуалне исправке рукописа наводе се хронолошким редоследом, на сталном месту, по правилу на крају чланка.

Захвалница

Назив и број пројекта, односно назив програма у оквиру којег је чланак настао, као и назив институције која је финансирала пројекат или програм, наводи се у посебној напомени на сталном месту, по правилу при дну прве стране чланка.

Претходне верзије рада

Ако је чланак у претходној верзији био изложен на скупу у виду усменог саопштења (под истим или сличним насловом), податак о томе треба да буде наведен у посебној напомени, по правилу при дну прве стране чланка. Рад који је већ објављен у неком часопису не може се објавити у *Војнотехничком гласнику* (прештампати), ни под сличним насловом и измењеном облику.

Табеларни и графички прикази

Пожељно је да наслови свих приказа, а по могућству и текстуални садржај, буду дати двојезично, на језику рада и на енглеском језику.

Табеле се пишу на исти начин као и текст, а означавају се редним бројевима са горње стране. Фотографије и цртежи треба да буду јасни, прегледни и погодни за репродукцију. Цртеже треба радити у програму word или corel. Фотографије и цртеже треба поставити на жељено место у тексту.

За слике и графиконе не сме се користити снимак са екрана рачунара програма за прикупљање података. У самом тексту чланка препоручује се употреба слика и графикона непосредно из програма за анализу података (као што су Excel, Matlab, Origin, SigmaPlot и други).

Навођење (цитирање) у тексту

Начин позивања на изворе у оквиру чланка мора бити једнообразан.

Војнотехнички гласник за референцирање (цитирање и навођење литературе) примењује Харвардски систем референци, односно Харвардски приручник за стил (Harvard Referencing System, Harvard Style Manual). У самом тексту, у обичним заградама, на месту на којем се врши позивање, односно цитирање литературе набројане на крају чланка, обавезно у обичној загради написати презиме цитираног аутора, годину издања публикације из које цитирате и, евентуално, број страница. Нпр. (Petrović, 2012, pp.10–12).

Детаљно упутство о начину цитирања, са примерима, дато је на страници сајта *Упутство за Харвардски приручник за стил*. Потребно је да се позивање на литературу у тексту уради у складу са поменутиим упутством.

Систем АСИСТЕНТ у сврху контроле навођења (цитирања) у тексту користи специјалну алатку CiteMatcher: откривање изостављених цитата у тексту рада и у попису референци.

Напомене (фусноте)

Напомене се дају при дну стране на којој се налази текст на који се односе. Могу садржати мање важне детаље, допунска објашњења, назнаке о коришћеним изворима (на пример, научној грађи, приручницима), али не могу бити замена за цитирану литературу.

Листа референци (литература)

Цитирана литература обухвата, по правилу, библиографске изворе (чланке, монографије и сл.) и даје се искључиво у засебном одељку чланка, у виду листе референци. Референце се не преводe на језик рада и набрајају се у посебном одељку на крају чланка.

Војнотехнички гласник, као начин исписа литературе, примењује Харвардски систем референци, односно Харвардски приручник за стил (Harvard Referencing System, Harvard Style Manual).

Литература се обавезно пише на латиничном писму и набраја по абecedном редоследу, наводећи најпре презимена аутора, без нумерације.

Детаљно упутство о начину пописа референци, са примерима, дато је на страници сајта *Упутство за Харвардски приручник за стил*. Потребно је да се попис литературе на крају чланка уради у складу са поменутиm упутством.

Нестандардно, непотпуно или недоследно навођење литературе у системима вредновања часописа сматра се довољним разлогом за оспоравање научног статуса часописа.

Систем АСИСТЕНТ у сврху контроле правилног исписа листе референци користи специјалну алатку RefFormatter: контрола обликовања референци у складу са Харвардским приручником за стил.

Изјава о ауторству

Поред чланка доставља се *Изјава о ауторству* у којој аутори наводе свој појединачни допринос у изради чланка. Такође, у тој изјави потврђују да су чланак урадили у складу са *Позивом и упутством ауторима* и *Изјавом о етичком поступању часописа*.

Сви радови подлежу стручној рецензији.

Списак рецензената *Војнотехничког гласника* може се видети на страници сајта *Списак рецензената*. Процес рецензирања објашњен је на страници сајта *Рецензентски поступак*.

Уредништво

Адреса редакције:
Војнотехнички гласник
Вељка Лукића Курјака 33
11042 Београд
e-mail: vojnotehnicki.glasnik@mod.gov.rs.
тел: војни 40-260 (011/3603-260), 066/8700-123

ПРИГЛАШЕНИЕ И ИНСТРУКЦИЯ ДЛЯ АВТОРОВ О ПОРЯДКЕ ПОДГОТОВКИ СТАТЬИ

Инструкция для авторов о порядке подготовки статьи к опубликованию в журнале «Военно-технический вестник» разработана согласно Регламенту о категоризации и ранжировании научных журналов Министерства образования, науки и технологического развития Республики Сербия («Службени гласник РС», № 159/20). Применение этого Регламента способствует повышению качества отечественных журналов и их более полному вовлечению в международную систему обмена научной информацией.

Военно-технический вестник (Vojnotehnički glasnik / Military Technical Courier), втг.мо.упр.срб, www.vtg.mod.gov.rs/index-ru.html, ISSN 0042-8469 – печатное издание, e-ISSN 2217-4753 – online, UDK 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; <https://doi.org/10.5937/VojnotehnickiGlasnik>, является рецензируемым научным журналом.

Собственники журнала: Министерство обороны и Вооруженные силы Республики Сербия.

Издатель журнала: Университет обороны в г. Белград (Военная академия).

Программная ориентация журнала основана на ежегодной категоризации журнала, которая производится соответствующим отраслевым министерством, в зависимости от области исследований, а также на его индексировании в международных наукометрических базах данных.

Журнал охватывает научные и профессиональные сферы в рамках учебно-научной области **естественно-математических наук**, а также в рамках учебно-научной области **технико-технологических наук**, особенно в области **оборонных наук и технологий**. В журнале публикуются теоретические и практические достижения, которые способствуют повышению квалификации представителей сербского, регионального и международного академического сообщества, особенно служащих Министерств Обороны и Вооруженных сил. В журнале публикуются статьи со соответствующими обзорами об аналитических, экспериментальных и прикладных исследованиях, а также о численном моделировании, охватывая различные дисциплины. Публикуемые материалы отличаются высоким качеством и актуальностью. Они написаны научным, но понятным и доступным для широкого круга читателей языком. Приветствуются все статьи, сообщающие об оригинальных теоретических и/или практических исследованиях и/или расширенные версии ранее опубликованных статей, представленных на конференциях. Статьи для публикации отбираются путем двойного слепого рецензирования, которое гарантирует оригинальность, актуальность и удобочитаемость. Цель состоит не только в поддержании высокого качества публикуемых статей, но и в обеспечении своевременного, тщательного и соответствующего процесса рецензирования.

Редакционная политика журнала «Военно-технический вестник» основана на рекомендациях Комитета по этике научных публикаций (COPE Core Practices), общих принципах прозрачности и лучшей практике издательской деятельности COPE, DOAJ, OASPA и WAME, а также на лучшей практике научно-издательской деятельности. Журнал «Военно-технический вестник» является членом COPE (Комитет по этике научных публикаций) со 2 мая 2018 года и членом OASPA (Ассоциация научных издателей открытого доступа) с 27 ноября 2015 года.

Министерством образования, науки и технологического развития Республики Сербия утверждена 25 октября 2022 г. категоризация журнала «Военно-технический вестник» за 2022 год:

- **Область компьютерные науки:**
ведущий журнал государственного значения (M51),
- **Область электроники, телекоммуникаций и информационных технологий:**
ведущий журнал государственного значения (M51),
- **Область машиностроения:**
ведущий журнал государственного значения (M51),
- **Область материалов и химической технологии:**
ведущий журнал государственного значения (M51).

С информацией относительно категоризации за 2022 год можно ознакомиться на странице сайта «Военно-технического вестника» *Категоризация Вестника*.

Более подробную информацию можно найти на сайте Министерства образования, науки и технологического развития Республики Сербия.

С информацией о категоризации можно ознакомиться и на сайте КОБСОН (Консорциум библиотек Республики Сербия по вопросам объединения закупок).

Категоризация Вестника проведена согласно Регламенту о категоризации и ранжировании научных журналов Министерства образования, науки и технологического развития Республики Сербия («Службени гласник РС», № 159/20)

Журнал соответствует стандартам Сербского индекса научного цитирования (СЦИндекс/SCIndex) - наукометрической базы данных научных журналов Республики Сербия, Научно-информационного система Redalyc, а также Российского индекса научного цитирования (РИНЦ). Журнал постоянно подвергается мониторингу и оценивается количественными наукометрическими показателями отражающими его научную ценность.

С информацией об индексировании можно ознакомиться на странице сайта журнала *Индексирование Вестника*.

«Военно-технический вестник» относительно своего содержания предоставляет пользователям возможность открытого доступа (DIAMOND OPEN ACCESS) и положениями об авторских правах, утвержденными Creative Commons (CC BY). С инструкцией об авторских правах можно ознакомиться на странице сайта журнала *Авторские права и политика самоархивирования*.

Рукописи статей направляются в редакцию журнала с использованием online системы ASSISTANT, запущенной Центром поддержки развития образования и науки (ЦПРОН). Регистрация в системе и оформление прав доступа выполняется по адресу <http://www.vtg.mod.gov.rs/index-ru.html>, через страницу ASSISTANT или СЦИНДЕКС (aseestant.ceon.rs/index.php/vtg). С инструкцией по регистрации и правам доступа можно ознакомиться по адресу <http://www.vtg.mod.gov.rs/index-ru.html>, на странице *Инструкция по ASSISTANT*.

Все авторы, предоставляющие свои рукописи для публикации в редакцию журнала «Военно-технический вестник» должны пройти предварительную регистрацию в реестре ORCID (Open Researcher and Contributor ID). Эта процедура осуществляется в соответствии с инструкцией, размещенной на странице сайта *Регистрация в реестре ORCID для присвоения идентификационного кода*.

«Военно-технический вестник» публикует статьи на английском языке (Arial, шрифт 11 pt, пробел Single). Процесс подготовки, написания и редактирования статьи

должен осуществляться в соответствии с принципами *Этического кодекса* (<http://www.vtg.mod.gov.rs/eticheskiy-kodyeks.html>). Статья должна содержать резюме с ключевыми словами, введение (цель исследования), основную часть (соответствующий обзор представительного исследования в данной области, четкое изложение научной новизны в представленном исследовании, соответствующую теоретическую основу, один или несколько примеров для демонстрации и обсуждения представленных тезисов), заключение и список литературы (без нумерации заголовков и подзаголовков). Объем статьи не должен превышать один авторский лист (16 страниц формата А4 с одинарным интервалом, максимум до 24 страниц, включая ссылки и приложения). Статья должна быть набрана на компьютере с использованием специально подготовленного редакцией макета, который можно скачать на странице сайта *Правила и образец составления статьи*.

Заголовок

Заголовок должен отражать тему статьи. В интересах журнала и автора необходимо использовать слова и словосочетания, удобные для индексации и поиска. Если такие слова не содержатся в заголовке, то желательно их добавить в подзаголовок.

Текущий заголовок

Текущий заголовок пишется в титуле каждой страницы статьи с целью упрощения процесса идентификации, в первую очередь копий статьей в электронном виде. Заголовок содержит в себе фамилию и инициал имени автора (в случае если авторов несколько, остальные обозначаются с «et al.» или «и др.»), название работы и журнала (год, том, выпуск, начальная и заключительная страница). Заголовок статьи и название журнала могут быть приведены в сокращенном виде.

ФИО автора

Приводятся полная фамилия и полное имя (всех) авторов. Желательно, чтобы были указаны инициалы отчеств авторов. Фамилия и имя авторов из Республики Сербия всегда пишутся в оригинальном виде (с сербскими диакритическими знаками), независимо от языка, на котором написана работа.

Наименование учреждения автора (аффилиация)

Приводится полное (официальное) наименование и местонахождение учреждения, в котором работает автор, а также наименование учреждения, в котором автор провёл исследование. В случае организаций со сложной структурой приводится их иерархическая соподчинённость (напр. Военная академия, кафедра военных электронных систем, г. Белград). По крайней мере, одна из организаций в иерархии должна иметь статус юридического лица. В случае если указано несколько авторов, и если некоторые из них работают в одном учреждении, нужно отдельными обозначениями или каким-либо другим способом указать в каком из приведённых учреждений работает каждый из авторов. Аффилиация пишется непосредственно после ФИО автора. Должность и специальность по диплому не указываются.

Контактные данные

Электронный адрес автора указывается рядом с его именем на первой странице статьи.

Категория (тип) статьи

Категоризация статьей является обязанностью редакции и имеет особое значение. Категорию статьи могут предлагать рецензенты и члены редакции, т.е.

редакторы рубрик, но ответственность за категоризацию несет исключительно главный редактор. Статьи в журнале распределяются по следующим категориям:

Научные статьи:

– оригинальная научная статья (работа, в которой приводятся ранее неопубликованные результаты собственных исследований, полученных научным методом);

– обзорная статья (работа, содержащая оригинальный, детальный и критический обзор исследуемой проблемы или области, в который автор внёс определённый вклад, видимый на основе автоцитат);

– краткое сообщение (оригинальная научная работа полного формата, но меньшего объёма или имеющая предварительный характер);

– научная критическая статья (дискуссия-полемика на определённую научную тему, основанная исключительно на научной аргументации) и научный комментарий.

Однако, в некоторых областях знаний научная работа в журнале может иметь форму монографического исследования, а также критического обсуждения научного материала (историко-архивного, лексикографического, библиографического, обзора данных и т.п.) – до сих пор неизвестного или недостаточно доступного для научных исследований. Работы, классифицированные в качестве научных, должны иметь, по меньшей мере, две положительные рецензии. В случае если в журнале объявляются и приложения, не имеющие научный характер, научные статьи должны быть сгруппированы и четко выделены в первой части номера.

Профессиональные статьи:

– профессиональная работа (приложения, в которых предлагаются опыты, полезные для совершенствования профессиональной практики, но которые не должны в обязательном порядке быть обоснованы на научном методе);

– информативное приложение (передовая статья, комментарий и т.п.);

– обзор (книги, компьютерной программы, случая, научного события и т.п.).

Объем кратких сообщений составляет 4-7 страниц, исследовательские статьи и тематические исследования с проблемно-ситуационным анализом – 10-14 страниц, однако объем обзорных статей может быть больше. Ограничения по количеству страниц не являются строгими, следовательно при соответствующем обосновании предоставленные работы могут быть длиннее или короче. В случае подачи расширенных версий ранее опубликованных докладов, представленных на конференции, редакция проверит было ли добавлено достаточно новых материалов для того, чтобы статья соответствовала стандартам журнала и условиям рецензирования. Добавленный материал должен быть новым, неопубликованным ранее. Новые результаты приветствуются, но не являются обязательным условием; однако ключевые тезисы, примеры, разработки и пр. должны быть более подробно представлены в статье по сравнению с первичным докладом на конференции.

Язык работы

Статья должна быть написана на английском языке. Текст должен быть в лингвистическом и стилистическом смысле упорядочен, систематизирован, без сокращений (за исключением стандартных). Все физические величины должны соответствовать Международной системе единиц измерения – СИ. Очередность формул обозначается порядковыми номерами, проставляемыми с правой стороны в круглых скобках.

Резюме

Резюме является кратким информативным обзором содержания статьи, обеспечивающим читателю быстроту и точность оценки её релевантности. В интересах редакции и авторов, чтобы резюме содержало термины, часто используемые для индексирования и поиска статьей. Составными частями резюме являются введение/цель исследования, методы, результаты и выводы. В резюме должно быть от 100 до 250 слов, и оно должно находиться между титулами (заголовков, ФИО авторов и др.) и ключевыми словами, за которыми следует текст статьи.

Ключевые слова

Ключевыми словами являются термины или фразы, адекватно представляющие содержание статьи, необходимые для индексирования и поиска. Ключевые слова необходимо выбирать, опираясь при этом на какой-либо международный источник (регистр, словарь, тезаурус), наиболее используемый внутри данной научной области. Число ключевых слов не может превышать 10. В интересах редакции и авторов, чтобы частота их встречи в статье была как можно большей. В статье они пишутся непосредственно после резюме.

Программа ASSISTANT предоставляет возможность использования сервиса KWASS, автоматически фиксирующего ключевые слова из источников/словарей по выбору автора/редактора.

Дата получения статьи

Дата, когда редакция получила статью; дата, когда редакция окончательно приняла статью к публикации; а также дата, когда были предоставлены необходимые исправления рукописи, приводятся в хронологическом порядке, как правило, в конце статьи.

Выражение благодарности

Наименование и номер проекта, т.е. название программы благодаря которой статья возникла, совместно с наименованием учреждения, которое финансировало проект или программу, приводятся в отдельном примечании, как правило, внизу первой страницы статьи.

Предыдущие версии работы

В случае если статья в предыдущей версии была изложена устно (под одинаковым или похожим названием, например, в виде доклада на научной конференции), сведения об этом должны быть указаны в отдельном примечании, как правило, внизу первой страницы статьи. Работа, которая уже была опубликована в каком-либо из журналов, не может быть напечатана в «Военно-техническом вестнике» ни под похожим названием, ни в изменённом виде.

Нумерация и название таблиц и графиков

Желательно, чтобы нумерация и название таблиц и графиков были исполнены на двух языках (на языке оригинала и на английском). Таблицы подписываются таким же способом как и текст и обозначаются порядковым номером с верхней стороны. Фотографии и рисунки должны быть понятны, наглядны и удобны для репродукции. Рисунки необходимо делать в программах Word или Corel. Фотографии и рисунки надо поставить на желаемое место в тексте. Для создания изображений и графиков использование функции снимка с экрана (скриншота) не допускается. В самом тексте статьи рекомендуется применение изображений и графиков, обработанных такими компьютерными программами, как: Excel, Matlab, Origin, SigmaPlot и др.

Ссылки (цитирование) в тексте

Оформление ссылок на источники в рамках статьи должно быть однообразным. «Военно-технический вестник» для оформления ссылок, цитат и списка использованной литературы применяет Гарвардскую систему (Harvard Referencing System, Harvard Style Manual). В тексте в скобках приводится фамилия цитируемого автора (или фамилия первого автора, если авторов несколько), год издания и по необходимости номер страницы. Например: (Petrović, 2010, pp.10-20). Рекомендации о способе цитирования размещены на странице сайта *Инструкция по использованию Гарвардского стиля*. При оформлении ссылок, цитат и списка использованной литературы необходимо придерживаться установленных норм. Программа ASSISTANT предоставляет при цитировании возможность использования сервиса CiteMatcher, фиксирующего пропущенные цитаты в работе и в списке литературы.

Примечания (сноски)

Примечания (сноски) к тексту указываются внизу страницы, к которой они относятся. Примечания могут содержать менее важные детали, дополнительные объяснения, указания об использованных источниках (напр. научном материале, справочниках), но не могут быть заменой процедуры цитирования литературы.

Литература (референции)

Цитированной литературой охватываются, как правило, такие библиографические источники как статьи, монографии и т.п. Вся используемая литература в виде референций размещается в отдельном разделе статьи. Названия литературных источников не переводятся на язык работы. «Военно-технический вестник» для оформления списка использованной литературы применяет Гарвардскую систему (Harvard Style Manual). В списке литературы источники указываются в алфавитном порядке фамилий авторов или редакторов. Рекомендации о способе цитирования размещены на странице сайта *Инструкция по использованию Гарвардского стиля*. При оформлении списка использованной литературы необходимо придерживаться установленных норм. При оформлении списка литературы программа ASSISTANT предоставляет возможность использования сервиса RefFormatter, осуществляющего контроль оформления списка литературы в соответствии со стандартами Гарвардского стиля. Нестандартное, неполное и непоследовательное приведение литературы в системах оценки журнала считается достаточной причиной для оспаривания научного статуса журнала.

Авторское заявление

Авторское заявление предоставляется вместе со статьей, в нем авторы заявляют о своем личном вкладе в написание статьи. В заявлении авторы подтверждают, что статья написана в соответствии с *Приглашением и инструкциями для авторов*, а также с *Кодексом профессиональной этики журнала*.

Все рукописи статей подлежат профессиональному рецензированию.

Список рецензентов журнала «Военно-технический вестник» размещён на странице сайта *Список рецензентов*. Процесс рецензирования описан в разделе *Правила рецензирования*.

Редакция

Почтовый адрес редакции:

«Војнотехнички гласник»

ул. Велька Лукича Куряка 33, 11042 Белград, Республика Сербия

e-mail: vojnotehnicki.glasnik@mod.gov.rs,

тел: +381 11 3603 260, +381 66 8700 123

CALL FOR PAPERS AND ARTICLE FORMATTING INSTRUCTIONS

The instructions to authors about the article preparation for publication in the *Military Technical Courier* are based on the Regulations on categorization and ranking of scientific journals of the Ministry of Education, Science and Technological Development of the Republic of Serbia (Official Gazette of the Republic of Serbia, No 159/20). This Regulations aims at improving the quality of national journals and raising the level of their compliance with the international system of scientific information exchange.

The Military Technical Courier / Vojnotehnički glasnik (www.vtg.mod.gov.rs/index-e.html, втг.мо.упр.срб, ISSN 0042-8469 – print issue, e-ISSN 2217-4753 – online, UDC 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; https://doi.org/10.5937/VojnotehnickiGlasnik), is an peer-reviewed scientific journal.

The owners of the journal are the Ministry of Defence of the Republic of Serbia and the Serbian Armed Forces. The publisher and financier of the *Military Technical Courier* is the University of Defence in Belgrade (Military Academy).

The program of the journal is based on the annual classification of journals performed by a relevant Ministry as well as on its indexing in international indexing databases.

The journal covers scientific and professional fields within the educational-scientific field of **Natural-Mathematical Sciences**, as well as within the educational-scientific field of **Technical-Technological Sciences**, and especially the field of **defense sciences and technologies**. It publishes theoretical and practical achievements leading to professional development of all members of Serbian, regional and international academic communities as well as members of the military and ministries of defence in particular. It publishes papers with balanced coverage of analytical, experimental, and applied research as well as numerical simulations from various disciplines. The material published is of high quality and relevance, written in a manner that makes it accessible to a wider readership. The journal welcomes papers reporting original theoretical and/or practice-oriented research as well as extended versions of already published conference papers. Manuscripts for publication are selected through a double-blind peer-review process to validate their originality, relevance, and readability. This being so, the objective is not only to keep the quality of published papers high but also to provide a timely, thorough, and balanced review process.

The editorial policy of the *Military Technical Courier* is based on the COPE Core Practices, common COPE, DOAJ, OASPA and WAME Principles of Transparency and Best Practice in Scholarly Publishing as well as on the best accepted practices in scientific publishing. The *Military Technical Courier* has been a COPE (Committee on Publication Ethics) member since 2nd May 2018 and a member of OASPA (Open Access Scholarly Publishers Association) since 27th November 2015.

The Ministry of Education, Science and Technological Development of the Republic of Serbia classified the *Military Technical Courier* for the year 2022, on October 25, 2022

- **on the list of periodicals for computer sciences**,
category: reputed national journal (M51),
- **on the list of periodicals for electronics, telecommunications and IT**,
category: reputed national journal (M51),
- **on the list of periodicals for mechanical engineering**,
category: reputed national journal (M51),
- **on the list of periodicals for materials and chemical technology**,
category: reputed national journal (M51).

The approved lists of national periodicals for the year 2022 can be viewed on the website of the *Military Technical Courier*, page *Journal categorization*.

More detailed information can be found on the website of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

The information on the categorization can be also found on the website of KOBSON (Consortium of Libraries of Serbia for Unified Acquisition).

The periodical is categorized in compliance with the Regulations on categorization and ranking of scientific journals of the Ministry of Education, Science and Technological Development of the Republic of Serbia (Official Gazette of the Republic of Serbia, No 159/20). More detailed information can be found on the website of the Ministry of Education, Science and Technological Development.

The journal is in the Serbian Citation Index – SCIndex (data base of national scientific journals), in the Scientific Information System Redalyc, and in the Russian Index of Science Citation/Российский индекс научного цитирования (RINC/РИНЦ) and is constantly monitored depending on the impact within the bases themselves. More detailed information can be viewed on the website of the *Military Technical Courier*, page *Journal indexing*.

The *Military Technical Courier*, in terms of its content, offers the possibility of open access (DIAMOND OPEN ACCESS) and applies the Creative Commons Attribution (CC BY) licence on copyright. The copyright details can be found on the *Copyright notice and Self-archiving policy* page of the journal's website.

Manuscripts are submitted online, through the electronic editing system ASSISTANT, developed by the Center for Evaluation in Education and Science – CEON.

The access and the registration are through the *Military Technical Courier* site <http://www.vtg.mod.gov.rs/index-e.html>, on the page ASSISTANT or the page SCINDEKS or directly through the link (aseestant.ceon.rs/index.php/vtg).

The detailed instructions about the registration for the service are on the website <http://www.vtg.mod.gov.rs/index-e.html>, on the page *Instructions for ASSISTANT*.

All authors submitting a manuscript for publishing in the *Military Technical Courier* should register for an ORCID ID following the instructions on the web page *Registration for an ORCID identifier*.

The *Military Technical Courier* publishes articles in English, using Arial and a font size of 11pt with Single Spacing.

The procedures of article preparation, writing and editing should be in accordance with the *Publication ethics statement* (<http://www.vtg.mod.gov.rs/publication-ethics-statement.html>).

The article should contain an abstract with keywords, introduction (motivation for the work), body (adequate overview of the representative work in the field, a clear statement of the novelty in the presented research, suitable theoretical background, one or more examples to demonstrate and discuss the presented ideas), conclusion, and references (without heading and subheading enumeration). The article length should not normally exceed 16 pages of the A4 paper format with single spacing, up to a maximum of 24 pages with references and supplementary material included.

The article should be formatted following the instructions in the Article Form which can be downloaded from website page *Article form*.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable for indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle.

Letterhead title

The letterhead title is given at a top of each page for easier identification of article copies in an electronic form in particular. It contains the author's surname and first name initial (for multiple authors add "et al"), article title, journal title and collation (year, volume, issue, first and last page). The journal and article titles can be given in a shortened form.

Author's name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form (with diacritic signs if in Serbian).

Author's affiliation

The full official name and seat of the author's affiliation is given, possibly with the name of the institution where the research was carried out. For organizations with complex structures, give the whole hierarchy (for example, University of Defence in Belgrade, Military Academy, Department for Military Electronic Systems). At least one organization in the hierarchy must be a legal entity. When some of multiple authors have the same affiliation, it must be clearly stated, by special signs or in other way, which department exactly they are affiliated with. The affiliation follows the author's name. The function and title are not given.

Contact details

The postal addresses or the e-mail addresses of the authors are given in the first page.

Type of articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification.

Journal articles are classified as follows:

Scientific articles:

- Original scientific papers (giving the previously unpublished results of the author's own research based on scientific methods);
- Review papers (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution demonstrated by self-citation);
- Short communications or Preliminary communications (original scientific full papers but shorter or of a preliminary character);
- Scientific commentaries or discussions (discussions on a particular scientific topic, based exclusively on scientific argumentation) and opinion pieces.

Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Papers classified as scientific must have at least two positive reviews.

If the journal contains non-scientific contributions as well, the section with scientific papers should be clearly denoted in the first part of the Journal.

Professional articles:

- Professional papers (contributions offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
- Informative contributions (editorial, commentary, etc.);
- Reviews (of a book, software, case study, scientific event, etc.)

Short communications are usually 4-7 pages long, research articles and case studies 10-14 pages, while reviews can be longer. Page number limits are not strict and, with appropriate reasoning, submitted manuscripts can also be longer or shorter. If extended versions of previously published conference papers are submitted, Editors will check if sufficient new material has been added to meet the journal standards and to qualify such manuscripts for the review process. The added material must not have been previously published. New results are desired but not necessarily required; however, submissions should contain expansions of key ideas, examples, elaborations, etc. of conference papers.

Language

The language of the article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and summary

An abstract is a concise informative presentation of the article content for fast and accurate evaluation of its relevance. It contains the terms often used for indexing and article search. A 100- to 250-word abstract has the following parts: introduction/purpose of the research, methods, results and conclusion.

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is, the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages. For this purpose, the ASSISTANT system uses a special tool KWASS for the automatic extraction of key words from disciplinary thesauruses/dictionaries by choice and the routine for their selection, i.e. acceptance or rejection by author and/or editor.

Article acceptance date

The date of the reception of the article, the dates of submitted corrections in the manuscript (optional) and the date when the Editorial Board accepted the article for publication are all given in a chronological order at the end of the article.

Acknowledgements

The name and the number of the project or programme within which the article was realised is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programme.

Article preliminary version

If an article preliminary version has appeared previously at a meeting in a form of an oral presentation (under the same or similar title), this should be stated in a separate note at the bottom of the first page. An article published previously cannot be published in the *Military Technical Courier* even under a similar title or in a changed form.

Tables and illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and



are denoted by Arabic numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

For figures and graphs, proper data plot is recommended i.e. using a data analysis program such as Excel, Matlab, Origin, SigmaPlot, etc. It is not recommended to use a screen capture of a data acquisition program as a figure or a graph.

Citation in the text

Citation in the text must be uniform. The *Military Technical Courier* applies the Harvard Referencing System given in the Harvard Style Manual. When citing sources within your paper, i.e. for in-text references of the works listed at the end of the paper, place the year of publication of the work in parentheses and optionally the number of the page(s) after the author's name, e.g. (Petrovic, 2012, pp.10-12). A detailed guide on citing, with examples, can be found on *Military Technical Courier* website on the page *Instructions for Harvard Style Manual*. In-text citations should follow its guidelines. For checking in-text citations, the ASSISTANT system uses a special tool CiteMatcher to find out quotes left out within papers and in reference lists.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

Reference list (Literature)

The cited literature encompasses bibliographic sources such as articles and monographs and is given in a separate section in a form of a reference list. References are not translated to the language of the article.

In compiling the reference list and bibliography, the *Military Technical Courier* applies the Harvard System – Harvard Style Manual. All bibliography items should be listed alphabetically by author's name, without numeration. A detailed guide for listing references, with examples, can be found on *Military Technical Courier* website on the page *Instructions for Harvard Style Manual*. Reference lists at the end of papers should follow its guidelines. In journal evaluation systems, non-standard, insufficient or inconsequent citation is considered to be a sufficient cause for denying the scientific status to a journal.

Authorship Statement

The Authorship statement, submitted together with the paper, states authors' individual contributions to the creation of the paper. In this statement, the authors also confirm that they followed the guidelines given in *the Call for papers* and the *Publication ethics and malpractice statement of the journal*.

All articles are peer reviewed.

The list of referees of the *Military Technical Courier* can be viewed at website page *List of referees*. The article review process is described on the *Peer Review Process* page of the website.

Editorial Team

Address of the Editorial Office:
Vojnotehnički glasnik / Military Technical Courier
Veljka Lukića Kurjaka 33
11042 Belgrade, Republic of Serbia
e-mail: vojnotehnicki.glasnik@mod.gov.rs, tel.: +381 11 3603 260, +381 66 8700 123

Ликовно-графички уредник
Марија Марић, e-mail: marija.maric@mod.gov.rs

Лектор
Добрила Милетић, e-mail: miletic.dobрила@gmail.com

Превод на енглески
Јасна Вишњић, e-mail: jasnavisnjic@yahoo.com

Превод на шпански
Јована Јовановић, e-mail: jovana.jov92@gmail.com

Превод на руски
Др Карина Авагјан, e-mail: karinka2576@mail.ru

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Војнотехнички гласник (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Цена: 600,00 динара

Тираж: 100 примерака

На основу мишљења Министарства за науку, технологију и развој Републике
Србије, број 413-00-1201/2001-01 од 12. 9. 2001. године,
часопис „Војнотехнички гласник“ је публикација од посебног интереса за науку.

УДК: Народна библиотека Србије, Београд

Адреса редакције: Војнотехнички гласник,
Велка Лукића Курјака 33, 11042 Београд

<http://www.vtg.mod.gov.rs>

<http://aseestant.ceon.rs/index.php/vtg/issue/current>

<http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469>

<https://www.redalyc.org/revista.oa?id=6617>

http://elibrary.ru/title_about.asp?id=53280

<https://doaj.org/toc/2217-4753>

Војнотехнички гласник је лиценциран код EBSCO Publishing-a.

Комплетан текст Војнотехничког гласника доступан је у базама података EBSCO Publishing-a.

e-mail: vojnotehnicki.glasnik@mod.gov.rs; X: @MilTechCourier

Претплата на штампано издање: e-mail: vojnotehnicki.glasnik@mod.gov.rs; тел. 066/87-00-123.

Часопис излази тромесечно.

Први штампани број Војнотехничког гласника објављен је 1. 1. 1953. године.

Прво електронско издање Војнотехничког гласника на Интернету објављено је 1. 1. 2011. г.

Штампа: Војна штампарија – Београд, Ресавска 40б, e-mail: vojna.stamparija@mod.gov.rs

Художественный редактор
Мария Марич, e-mail: marija.maric@mod.gov.rs
Корректор
Добрила Милетич, e-mail: miletic.dobрила@gmail.com
Перевод на английский язык
Ясна Вишнич, e-mail: jasnavisnjic@yahoo.com
Перевод на испанский язык
Йована Йованович, e-mail: jovana.jov92@gmail.com
Перевод на русский язык
Д.филол.н. *Карина* Кареновна Авагян, e-mail: karinka2576@mail.ru
СIP – Каталогизация в публикации
Национальная библиотека Сербии, г. Белград

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Vojnotehnički glasnik (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Цена: 600,00 динаров

Тираж: 100 екземпляров

На основании решения Министерства науки и технологий Республики Сербия,
№ 413-00-1201/2001-01 от 12. 9. 2001 года, журнал «Военно-технический вестник»
объявлен изданием, имеющим особое значение для науки.

УДК: Национальная библиотека Сербии, г. Белград

Адрес редакции: Војнотехнички гласник,

Ул. Велька Лукича Куряка 33, 11042 Белград, Республика Сербия

<http://www.vtg.mod.gov.rs>

<http://aseestant.ceon.rs/index.php/vtg/issue/current>

<http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469>

<https://www.redalyc.org/revista.oa?id=6617>

http://elibrary.ru/title_about.asp?id=53280

<https://doaj.org/toc/2217-4753>

«Военно-технический вестник» включен в систему EBSCO. Полный текст журнала
«Военно-технический вестник» можно найти в базах данных EBSCO Publishing.

e-mail: vojnotehnicki.glasnik@mod.gov.rs, X: @MilTechCourier

Подписка на печатную версию журнала: e-mail: vojnotehnicki.glasnik@mod.gov.rs;

тел. +381 66 87 00 123.

Журнал выпускается ежеквартально.

Первый номер журнала «Военно-технический вестник» выпущен 1.1.1953 года.

Первая электронная версия журнала размещена на интернет странице 1.1.2011 года.

Типография: Војна штампарија – Белград, Ресавска 40б, e-mail: vojna.stamparija@mod.gov.rs

Graphic design editor

Marija Marić, e-mail: marija.maric@mod.gov.rs

Proofreader

Dobriša Miletić, e-mail: miletic.dobriša@gmail.com

English translation and polishing

Jasna Višnjić, e-mail: jasnavisnjic@yahoo.com

Spanish translation and polishing

Jovana Jovanović, e-mail: jovana.jov92@gmail.com

Russian translation and polishing

Dr. *Karina* Avagyan, e-mail: karinka2576@mail.ru

CIP – Catalogisation in the publication

National Library of Serbia, Belgrade

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Vojnotehnički glasnik (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Price: 600.00 RSD

Printed in 100 copies

According to the Opinion of the Ministry of Science and Technological Development
No 413-00-1201/2001-01 of 12th September 2001, the *Military Technical Courier* is a
publication of special interest for science.

UDC: National Library of Serbia, Belgrade

Address: Vojnotehnički glasnik/Military Technical Courier,
Veljka Lukića Kurjaka 33, 11042 Belgrade, Republic of Serbia

<http://www.vtg.mod.gov.rs/index-e.html>

<http://aseestant.ceon.rs/index.php/vtg/issue/current>

<http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469>

<https://www.redalyc.org/revista.oa?id=6617>

http://elibrary.ru/title_about.asp?id=53280

<https://doaj.org/toc/2217-4753>

Military Technical Courier has entered into an electronic licensing relationship with EBSCO Publishing.
The full text of *Military Technical Courier* can be found on EBSCO Publishing's databases.

e-mail: vojnotehnicki.glasnik@mod.gov.rs, X: @MilTechCourier

Subscription to print edition: e-mail: vojnotehnicki.glasnik@mod.gov.rs; Tel. +381 66 87 00 123.

The journal is published quarterly.

The first printed issue of the *Military Technical Courier* appeared on 1st January 1953.

The first electronic edition of the *Military Technical Courier* on the Internet appeared on 1st January 2011.

Printed by Voјna štampariја – Belgrade, Resavska 40b, e-mail: vojna.stampariја@mod.gov.rs

