

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

**ACADEMIC SCIENTIFIC  
JOURNAL OF COMPUTER SCIENCE**

**№2**

**2026**

ISSN 2518-1726 (Online),  
ISSN 1991-346X (Print)



CENTRAL ASIAN ACADEMIC  
RESEARCH CENTER



**ACADEMIC SCIENTIFIC  
JOURNAL OF COMPUTER  
SCIENCE**

**2 (358)**

**APRIL – JUNE 2026**

**PUBLISHED SINCE JANUARY 1963  
PUBLISHED 4 TIMES A YEAR**

ALMATY, NAS RK

#### Chief Editor:

**MUTANOV Galimkair Mutanovich**, doctor of technical sciences, professor, academician of NAS RK, (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=6506682964>, <https://www.webofscience.com/wos/author/record/1423665>

#### EDITORIAL BOARD:

**KALIMOLDAYEV Maksat Nuradilovich**, (Deputy Editor-in-Chief), Doctor of Physical and Mathematical Sciences, Professor, Academician of NAS RK, Advisor to the General Director of the Institute of Information and Computing Technologies of the CS MES RK, Head of the Laboratory (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=56153126500>, <https://www.webofscience.com/wos/author/record/2428551>

**MAMYRBAEV Orken Zhumazhanovich**, (Academic Secretary), PhD in Information Systems, Deputy Director for Science of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=55967630400>, <https://www.webofscience.com/wos/author/record/1774027>

**BAIGUNCHEKOV Zhumadil Zhanabaevich**, Doctor of Technical Sciences, Professor, Academician of NAS RK, Institute of Cybernetics and Information Technologies, Department of Applied Mechanics and Engineering Graphics, Satbayev University (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=6506823633>, <https://www.webofscience.com/wos/author/record/1923423>

**WOICIK Waldemar**, Doctor of Technical Sciences (Phys.-Math.), Professor of the Lublin University of Technology (Lublin, Poland), <https://www.scopus.com/authid/detail.uri?authorId=7005121594>, <https://www.webofscience.com/wos/author/record/678586>

**SMOLARJ Andrej**, Associate Professor Faculty of Electronics, Lublin polytechnic university (Lublin, Poland), <https://www.scopus.com/authid/detail.uri?authorId=56249263000>, <https://www.webofscience.com/wos/author/record/1268523>

**KEILAN Alimkhan**, Doctor of Technical Sciences, Professor (Doctor of science (Japan)), chief researcher of Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=8701101900>, <https://www.webofscience.com/wos/author/record/1436451>

**KHAIROVA Nina**, Doctor of Technical Sciences, Professor, Chief Researcher of the Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=37461441200>, <https://www.webofscience.com/wos/author/record/1768515>

**OTMAN Mohamed**, PhD, Professor of Computer Science Department of Communication Technology and Networks, Putra University Malaysia (Selangor, Malaysia), <https://www.scopus.com/authid/detail.uri?authorId=56036884700>, <https://www.webofscience.com/wos/author/record/747649>

**NYSANBAYEVA Saule Yerkebulanovna**, Doctor of Technical Sciences, Associate Professor, Senior Researcher of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=55453992600>, <https://www.webofscience.com/wos/author/record/3802041>

**USATOVA Olga Alexandrovna**, PhD, Associate Professor, Chief Scientific Secretary of the Institute of Information and Computing Technologies of the National Academy of Sciences of the Republic of Kazakhstan (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

**KAPALOVA Nursulu Aldazharovna**, Candidate of Technical Sciences, Head of the Laboratory cybersecurity, Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=57191242124>,

**KOVALYOV Alexander Mikhailovich**, Doctor of Physical and Mathematical Sciences, Academician of the National Academy of Sciences of Ukraine, Institute of Applied Mathematics and Mechanics (Donetsk, Ukraine), <https://www.scopus.com/authid/detail.uri?authorId=7202799321>, <https://www.webofscience.com/wos/author/record/38481396>

**MIKHALEVICH Alexander Alexandrovich**, Doctor of Technical Sciences, Professor, Academician of the National Academy of Sciences of Belarus (Minsk, Belarus), <https://www.scopus.com/authid/detail.uri?authorId=7004159952>, <https://www.webofscience.com/wos/author/record/46249977>

**TIGHINEANU Ion Mihailovich**, Doctor of Physical and Mathematical Sciences, Academician, President of the Academy of Sciences of Moldova, Technical University of Moldova (Chisinau, Moldova), <https://www.scopus.com/authid/detail.uri?authorId=7006315935>, <https://www.webofscience.com/wos/author/record/524462>

---

#### Academic Scientific Journal of Computer Science

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

Owner: «Central Asian Academic Research Center» LLP (Almaty).

Certificate № **KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan

Subject area: *information and communication technologies*.

Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*

Periodicity: *4 times a year.*

<http://www.physico-mathematical.kz/index.php/en/>

© «Central Asian Academic Research Center» LLP, 2026

#### БАС РЕДАКТОР:

**МУТАНОВ Ғалымқайыр Мұтанұлы**, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=6506682964>, <https://www.webofscience.com/wos/author/record/1423665>

#### РЕДАКЦИЯ АЛҚАСЫ:

**КАЛИМОЛДАЕВ Мақсат Нұрәділұлы**, (бас редактордың орынбасары), физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының кеңесшісі, зертхана меңгерушісі (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=56153126500>, <https://www.webofscience.com/wos/author/record/2428551>

**МАМЫРБАЕВ Өркен Жұмажанұлы** (ғалым хатшы), Ақпараттық жүйелер саласындағы техника ғылымдарының (PhD) докторы, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» директорының ғылым жөніндегі орынбасары (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=55967630400>, <https://www.webofscience.com/wos/author/record/1774027>

**БАЙГУНЧЕКОВ Жұмаділ Жаңабайұлы**, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Кибернетика және ақпараттық технологиялар институты, Қолданбалы механика және инженерлік графика кафедрасы, Сәтбаев университеті (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=6506823633>, <https://www.webofscience.com/wos/author/record/1923423>

**ВОЙЧИК Вальдемар**, техника ғылымдарының докторы (физ-мат), Люблин технологиялық университетінің профессоры (Люблин, Польша), <https://www.scopus.com/authid/detail.uri?authorId=7005121594>, <https://www.webofscience.com/wos/author/record/678586>

**СМОЛАРЖ Анджей**, Люблин политехникалық университетінің электроника факультетінің доценті (Люблин, Польша), <https://www.scopus.com/authid/detail.uri?authorId=56249263000>, <https://www.webofscience.com/wos/author/record/1268523>

**КЕЙЛАН Әлімхан**, техника ғылымдарының докторы, профессор (ғылым докторы (Жапония)), ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» бас ғылыми қызметкері (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=8701101900>, <https://www.webofscience.com/wos/author/record/1436451>

**ХАЙРОВА Нина**, техника ғылымдарының докторы, профессор, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» бас ғылыми қызметкері (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=37461441200>, <https://www.webofscience.com/wos/author/record/1768515>

**ОТМАН Мохаммед**, PhD, Информатика, Коммуникациялық технологиялар және желілер кафедрасының профессоры, Путра университеті Малайзия (Селангор, Малайзия), <https://www.scopus.com/authid/detail.uri?authorId=56036884700>, <https://www.webofscience.com/wos/author/record/747649>

**НЫСАНБАЕВА Сауле Еркебұланқызы**, техника ғылымдарының докторы, доцент, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» аға ғылыми қызметкері (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=55453992600>, <https://www.webofscience.com/wos/author/record/3802041>

**УСАТОВА Ольга Александровна**, PhD, қауымдастырылған профессор, ҚР ҒЖБМ "Ақпараттық және есептеу технологиялары институтының" бас ғалым хатшысы (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

**КАПАЛОВА Нұрсұлу Алдажарқызы**, техника ғылымдарының кандидаты, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты», Киберқауіпсіздік зертханасының меңгерушісі (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=57191242124>,

**КОВАЛЕВ Александр Михайлович**, физика-математика ғылымдарының докторы, Украина Ұлттық Ғылым академиясының академигі, Қолданбалы математика және механика институты (Донецк, Украина), <https://www.scopus.com/authid/detail.uri?authorId=7202799321>, <https://www.webofscience.com/wos/author/record/38481396>

**МИХАЛЕВИЧ Александр Александрович**, техника ғылымдарының докторы, профессор, Беларусь Ұлттық Ғылым академиясының академигі (Минск, Беларусь), <https://www.scopus.com/authid/detail.uri?authorId=7004159952>, <https://www.webofscience.com/wos/author/record/46249977>

**ТИГИНЯНУ Ион Михайлович**, физика-математика ғылымдарының докторы, академик, Молдова Ғылым Академиясының президенті, Молдова техникалық университеті (Кишинев, Молдова), <https://www.scopus.com/authid/detail.uri?authorId=7006315935>, <https://www.webofscience.com/wos/author/record/524462>

---

**Academic Scientific Journal of Computer Science**

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген № **KZ77VPY00121154** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

<http://www.physico-mathematical.kz/index.php/en/>

© «Орталық Азия академиялық ғылыми орталығы» ЖШС, 2026

### Главный редактор:

**МУТАНОВ Галимканр Мутанович**, доктор технических наук, профессор, академик НАН РК, (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=6506682964>, <https://www.webofscience.com/wos/author/record/1423665>

### Редакционная коллегия:

**КАЛИМОЛДАЕВ Максат Нурадилович**, (заместитель главного редактора), доктор физико-математических наук, профессор, академик НАН РК, советник генерального директора «Института информационных и вычислительных технологий» КН МНВО РК, заведующий лабораторией (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=56153126500>, <https://www.webofscience.com/wos/author/record/2428551>

**МАМЫРБАЕВ Оркен Жумажанович**, (ученый секретарь), доктор философии (PhD) по специальности «Информационные системы», заместитель директора по науке РГП «Институт информационных и вычислительных технологий» Комитета науки МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=55967630400>, <https://www.webofscience.com/wos/author/record/1774027>

**БАЙГУНЧЕКОВ Жумадил Жанабаевич**, доктор технических наук, профессор, академик НАН РК, Институт кибернетики и информационных технологий, кафедра прикладной механики и инженерной графики, Университет Сагпаева (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=6506823633>, <https://www.webofscience.com/wos/author/record/1923423>

**ВОЙЧИК Вальдемар**, доктор технических наук (физ.-мат.), профессор Люблинского технологического университета (Люблин, Польша), <https://www.scopus.com/author/detail.uri?authorId=7005121594>, <https://www.webofscience.com/wos/author/record/678586>

**СМОЛАРЖ Анджей**, доцент факультета электроники Люблинского политехнического университета (Люблин, Польша), <https://www.scopus.com/author/detail.uri?authorId=56249263000>, <https://www.webofscience.com/wos/author/record/1268523>

**КЕЙЛАН Алимхан**, доктор технических наук, профессор (Doctor of science (Japan)), главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=8701101900>, <https://www.webofscience.com/wos/author/record/1436451>

**ХАЙРОВА Нина**, доктор технических наук, профессор, главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=37461441200>, <https://www.webofscience.com/wos/author/record/1768515>

**ОТМАН Мохамед**, доктор философии, профессор компьютерных наук, Департамент коммуникационных технологий и сетей, Университет Путра Малайзия (Селангор, Малайзия), <https://www.scopus.com/author/detail.uri?authorId=56036884700>, <https://www.webofscience.com/wos/author/record/747649>

**НЫСАНБАЕВА Сауле Еркебулановна**, доктор технических наук, доцент, старший научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=55453992600>, <https://www.webofscience.com/wos/author/record/3802041>

**УСАТОВА Ольга Александровна**, PhD, ассоциированный профессор, Главный ученый секретарь «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

**КАПАЛОВА Нурсулу Алдажаровна**, кандидат технических наук, заведующий лабораторией кибербезопасности РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/author/detail.uri?authorId=57191242124>,

**КОВАЛЕВ Александр Михайлович**, доктор физико-математических наук, академик НАН Украины, Институт прикладной математики и механики (Донецк, Украина), <https://www.scopus.com/author/detail.uri?authorId=7202799321>, <https://www.webofscience.com/wos/author/record/38481396>

**МИХАЛЕВИЧ Александр Александрович**, доктор технических наук, профессор, академик НАН Беларуси (Минск, Беларусь), <https://www.scopus.com/author/detail.uri?authorId=7004159952>, <https://www.webofscience.com/wos/author/record/46249977>

**ТИГИНЯНУ Ион Михайлович**, доктор физико-математических наук, академик, президент Академии наук Молдовы, Технический университет Молдовы (Кишинев, Молдова), <https://www.scopus.com/author/detail.uri?authorId=7006315935>, <https://www.webofscience.com/wos/author/record/524462>

---

**Academic Scientific Journal of Computer Science**

**ISSN 2518-1726 (Online),**

**ISSN 1991-346X (Print)**

Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*

Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания № **KZ77VPU00121154**. Дата выдачи **05.06.2025**

Тематическая направленность: *информационно-коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных КОКШВО МНВО РК по направлению «информационно-коммуникационные технологии».*

Периодичность: *4 раза в год.*

<http://www.physico-mathematical.kz/index.php/en/>

© ТОО «Центрально-азиатский академический научный центр», 2026

## CONTENTS

## COMPUTER SCIENCE

<b>Abduraimova B.K., Toleukhan A.B., Sapakova S.Z., Abisheva A.A.</b> Development of early cyberattack detection method using CNN-LSTM for IoT.....	11
<b>Aben A.B., Kazbekova G.N., Baimakhanova A.S., Amanzholova A.B.</b> Classification of birds and drones in the sky using MobileNetV2 model.....	30
<b>Akbarov D., Sembayev T.</b> Quality-aware pose–hand keypoint extraction pipeline for skeleton-based sign language recognition.....	44
<b>Algazy K., Alimzhan Y., Sakan K., Nyssanbayeva S.</b> Lattice-based vector commitments for Verkle trees.....	67
<b>Asylkhan N., Baidrakhmanova M.G.</b> Principles and models of spatial organization of buildings for crop production considering technological and climatic factors.....	87
<b>Basheyeva Zh., Tokesh A., Bekish U., Abdoldinova G.</b> Artificial intelligence for academic project management: a bibliometric analysis and systematic review.....	105
<b>Bekmanova G., Kantureyeva M., Omarbekova A., Zakirova A., Issainova A.</b> Integrating artificial intelligence to evaluate emotions in the learning environment.....	125
<b>Dzhusupbekova G.T., Jangassiyev R.M.</b> Gemini AI integration based on .NET MAUI for education: hybrid architecture and empirical load testing.....	146
<b>Doszhan N.S., Sultanbekova L.Ye., Zhumagali S.Zh., Konysbayev E.K.</b> Modeling and parameter calculation of an emergency response system based on LoRaWAN technology in the high-altitude conditions of the Zailiysky Alatau.....	166
<b>Zhumakhanova A., Kudabayeva R., Akanova K., Myrkanova A.</b> Entropy-normalized multidimensional model for user activity segmentation in Reddit...	180
<b>Karabaliyev Y., Kolesnikova K., Khlevnaya Y.</b> HybridKazASR: a hybrid automatic speech recognition system combining multi-model rover fusion and morpheme-aware language modeling for Kazakh.....	198
<b>Kerimkhulle S.E., Adalbek A., Baizakov N.A., Shodorova N.N.</b> Piecewise logistic and fuzzy modeling of Kazakhstan's GDP dynamics (1990–2024)....	212
<b>Kulakayeva A., Ashurov A., Aitmagambetov A., Ongenbayeva Zh.</b> Development of mathematical models and criteria for the admissibility of orbital maneuvers of spacecraft.....	228

**Kulatay A.A., Zhaisanova D.S., Daurenbayeva N.A., Mamanova S.Y., Tolegen M.**  
Machine learning for personalized learning in gamified edtech platforms:  
Aqyl Battle case.....248

**Mamyrbayev O., Kurmetkan T.**  
Enhanced sentiment analysis of e-commerce product reviews using  
Luong attention-based Bi-LSTM.....263

**Marassulov U.A., Kazbekova G.**  
TF-IDF-based fake news detection in Kazakh and Russian.....286

**Omar A.B., Mussiraliyeva Sh.Zh.**  
Federated learning: models based on transformer architecture.....302

**Rakhimova D., Duisenbekkyzy Zh., Karibayeva A., Eşref A., Ilessova B.**  
Improving the voice recognition system for children in Kazakh through additional  
training (fine-tuning).....317

**Sarsembayev M, Urmashiev B.**  
Optimization of the calculation of kinetic equations of combustion processes on GPU  
using global memory and shared memory.....335

**Symagulov A., Smurygin V., Belousov A., Karypov A., Yunicheva N.R.**  
Improving the accuracy of crop and weed detection using UAVs in soya fields  
through image segmentation.....347

**Tashenova Zh., Gabdullin A.R., Abdugulova Zh., Amanzholova Sh., Santeyeva S.**  
Security evaluation of WPA3 wireless networks under deauthentication  
attack scenarios.....368

**Tursunbayeva G.U., Satybalдина D.Zh., Tleuberdin S.T., Tashatov N.N.,  
Egamberdiyev E.E.**  
Anomaly detection in UAV telemetry systems based on simulation modeling.....391

**Tursynova N., Yerimbetova A., Amangeldy N., Zhumabayeva A., Daiyrbayeva E.**  
Comparative analysis of multilingual transformer models for Kazakh-to-gloss  
translation.....414

**Shangpeng Lei, Balakayeva G.**  
Dual-branch physical information neural networks for data center airflow velocity  
and thermal modeling.....433

**Shynzhigit B.B., Balabekova M.O., Amangeldy T.T., Malik G.J., Balgimbekova U.B.**  
Automatic brick defects detection by using a CNN-based deep learning model.....449

## МАЗМҰНЫ

### КОМПЬЮТЕРЛІК ҒЫЛЫМДАР

<b>Абдураимова Б.К., Төлеухан Ә.Б., Сапакова С.З., Абишева А.А.</b> Кибершабулдарды ерте анықтау әдісін CNN-LSTM негізінде дамыту (ИОТ үшін).....	11
<b>Абен А.Б., Қазбекова Г.Н., Баймаханова А.С., Аманжолова Ә.Б.</b> MobileNetV2 моделімен аспандағы құстар мен дрондарды классификациялау.....	30
<b>Ақбаров Д.Р., Сембаев Т.М.</b> Ым тілін тануға арналған дене қалпы мен қолдың негізгі нүктелерін сапаны бақылаумен анықтау әдісі.....	44
<b>Алғазы К.Т., Әлімжан Е.Ж., Сақан Қ.С., Нысанбаева С.Е.</b> Verkle ағаштарына арналған торлық векторлық міндеттемелер.....	67
<b>Асылхан Н., Байдрахманова М.Г.</b> Технологиялық және климаттық факторларды ескере отырып, өсімдік шаруашылығы ғимараттарының кеңістік ұйымдастыру қағидалары мен модельдері.....	87
<b>Башеева Ж., Төкеш Ә., Бекіш Ұ., Абдолдинова Г.</b> Академиялық жобаларды басқарудағы жасанды интеллект: библиометриялық талдау және жүйелі шолу.....	105
<b>Бекманова Г.Т., Кантурсева М.А., Омарбекова А.С., Закирова А.Б., Исайнова А.Н.</b> Оқу ортасындағы эмоцияларды бағалау үшін жасанды интеллектті біріктіру.....	125
<b>Джусупбекова Г.Т., Жангасиев Р.М.</b> Білім беруге арналған .NET MAUI негізіндегі Gemini AI интеграциясы: гибридігі архитектура және эмпирикалық жүктемелік тестілеу.....	146
<b>Досжан Н.С., Султанбекова Л.Е., Жумағали С.Ж., Қонысбаев Е.К.</b> Іле Алатауының биік таулы жағдайында LORAWAN технологиясы негізіндегі жедел әрекет ету жүйесінің параметрлерін модельдеу және есептеу.....	166
<b>Жумаханова А., Қудабаева Р., Ақанова К., Мырқанова А.</b> REDDIT-те пайдаланушы әрекетін сегменттеуге арналған энтропия-нормалданған көп өлшемді модель.....	180
<b>Қарабаев Е., Колесникова К., Хлевная Ю.</b> HybridKazASR: Rover көпмодельді біріктіру және морфемеге негізделген тілдік модельдеуді пайдаланатын қазақ тілін автоматты тану гибридігі жүйесі.....	198
<b>Керімқұл С.Е., Адалбек А., Байзақов Н.А., Шодорова Н.Н.</b> Қазақстан ЖІӨ динамикасын кезеңдік (Piecewise) логистикалық және бұлдыр модельдеу (1990–2024).....	212

<b>Кулакаева А.Е., Ашуров А.Е., Айтмағамбетов А.З., Онгенбаева Ж.Ж.</b> Ғарыш аппараттарының орбиталық маневрлерінің математикалық модельдері мен рұқсат критерийлерін әзірлеу.....	228
<b>Құлатай А.А., Жайсанова Д.С., Дауренбаева Н.А., Маманова С.Е., Төлеген М.</b> Геймификацияланған edtech платформаларда оқытуды жекелендіруге арналған машиналық.....	248
<b>Мамырбаев Ө.Ж., Құрметқан Т.</b> Луонг назар механизміне негізделген BI-LSTM көмегімен электрондық коммерция өнімдеріне жазылған пікірлерге жетілдірілген сентименттік талдау жасау.....	263
<b>Марасулов У.А., Казбекова Г.</b> Қазақ және орыс тілдеріндегі жалған жаңалықтарды TF-IDF арқылы анықтау.....	286
<b>Омар А.Б., Мусиралиева Ш.Ж.</b> Федеративті оқыту: трансформер архитектурасына негізделген модельдер.....	302
<b>Рахимова Д., Дүйсенбекқызы Ж., Кәрібаева А., Ешref А., Ілесова Б.</b> Қазақ тіліндегі балалар дауысын тану жүйесін қосымша оқыту (Fine-Tuning) арқылы жетілдіру.....	317
<b>Сарсембаев М., Урмашев Б.</b> Global memory және shared memory қолдану арқылы GPU-да жану процестерінің кинетикалық теңдеулерін есептеуді оңтайландыру.....	335
<b>Сымагулов А., Смурыгин В., Белоусов А., Карыпов А., Юничева Н.Р.</b> Соя алқаптарында ҰҰА көмегімен мәдени және арамшөп өсімдіктерін детекттеу сапасын кескіндерді сегменттеу арқылы арттыру.....	347
<b>Ташенова Ж.М., Габдуллин А.Р., Абдугулова Ж.К., Аманжолова Ш.А., Сантеева С.Ә.</b> Деатентификациялау шабуылы сценарийлеріндегі WPA3 сымсыз желілерінің қауіпсіздігін бағалау.....	368
<b>Турсунбаева Г., Сатыбалдина Д., Глеубердин С., Ташатов Н., Эгамбердиев Э.</b> Симуляциялық модельдеу негізінде ұшқышсыз ұшу аппараттарының телеметриялық жүйелеріндегі аномалияларды анықтау.....	391
<b>Турсынова Н., Еримбетова А., Амангелді Н., Жумабаева А., Дайырбаева Э.</b> Қазақ тілінен глосска аудару үшін көптілді трансформерлік модельдердің салыстырмалы талдауы.....	414
<b>Шанпэн Лей, Балакаева Г.</b> Деректер орталығының ауа ағынының жылдамдығына және термиялық модельдеуге арналған екі тармақты физикалық ақпараттық нейрондық желілер.....	433
<b>Шынжігіт Ш.Б., Балабекова М.О., Амангелді Т.Т., Мәлік Г.Ж., Балгимбекова У.Б.</b> Кіріш ақауларын автоматты анықтауда snn негізіндегі терең оқыту моделін пайдалану.....	449

## СОДЕРЖАНИЕ

## КОМПЬЮТЕРНЫЕ НАУКИ

<b>Абдураимова Б.К., Толеухан А.Б., Сапакова С.З., Абишева А.А.</b> Разработка метода раннего обнаружения кибератак на основе CNN-LSTM для IoT.....	11
<b>Абен А.Б., Казбекова Г.Н., Баймаханова А.С., Аманжолова А.Б.</b> Классификация птиц и дронов в небе с использованием модели MobileNetV2.....	30
<b>Акбаров Д.Р., Сембаев Т.М.</b> Метод получения ключевых точек позы и кистей с контролем качества для распознавания жестового языка.....	44
<b>Алгазы К.Т., Алимжан Е.Ж., Сакан К.С., Нысанбаева С.Е.</b> Решеточные векторные обязательства для Verkle-деревьев.....	67
<b>Асылхан Н., Байдрахманова М.Г.</b> Принципы и модели пространственной организации зданий для растениеводства с учетом технологических и климатических факторов.....	87
<b>Башеева Ж., Токеш А., Бекиш У., Абдолдинова Г.</b> Искусственный интеллект в управлении академическими проектами: библиометрический анализ и систематический обзор.....	105
<b>Бекманова Г.Т., Кантуреева М.А., Омарбекова А.С., Закирова А.Б., Исайнова А.Н.</b> Интеграция искусственного интеллекта для оценки эмоций в учебной среде.....	125
<b>Джусупбекова Г.Т., Джангасиев Р.М.</b> Интеграция Gemini AI на базе .NET MAUI для образования: гибридная архитектура и эмпирическое нагрузочное тестирование.....	146
<b>Досжан Н.С., Султанбекова Л.Е., Жумагали С.Ж., Коньсбаев Е.К.</b> Моделирование и расчет параметров системы экстренного реагирования на базе технологии LoRaWAN в условиях высокогорья Заилийского Алатау.....	166
<b>Жумаханова А., Кудабаева Р., Аканова К., Мырканова А.</b> Энтропийно-нормализованная многомерная модель для сегментации активности пользователей в Reddit.....	180
<b>Карабалиев Е., Колесникова К., Хлевна Ю.</b> HybridKazASR: гибридная система автоматического распознавания казахской речи на основе многомодельного объединения ROVER и морфемно-ориентированного языкового моделирования.....	198
<b>Керимкулов С.Е., Адалбек А., Байзаков Н.А., Шодорова Н.Н.</b> Кусочно-логистическое и нечеткое моделирование динамики ВВП Казахстана (1990–2024).....	212
<b>Кулакаева А.Е., Ашуров А.Е., Айтмагамбетов А.З., Онгенбаева Ж.Ж.</b> Разработка математических моделей и критериев допустимости орбитальных маневров космических аппаратов.....	228

<b>Кулатай А.А., Жайсанова Д.С., Дауренбаева Н.А., Маманова С.Е., Толеген М.</b> Машинное обучение для персонализации обучения на геймифицированных EdTech-платформах: кейс Aqyl Battle.....	248
<b>Мамырбаев О., Курметкан Т.</b> Усовершенствованный анализ тональности отзывов о товарах электронной коммерции с использованием Bi-LSTM на основе механизма внимания Луонга.....	263
<b>Марасулов У.А., Казбекова Г.</b> Выявление ложных новостей на казахском и русском языках TF-IDF-моделями.....	286
<b>Омар А.Б., Мусиралиева Ш.Ж.</b> Федеративное обучение: модели на основе архитектуры трансформеров.....	302
<b>Рахимова Д., Дуйсенбеккызы Ж., Карибаева А., Еҫref А., Илесова Б.</b> Совершенствование системы распознавания голоса детей на казахском языке путем дополнительного обучения (fine-tuning).....	317
<b>Сарсембаев М., Урмашев Б.</b> Оптимизация расчета кинетических уравнений процессов горения на GPU с использованием global memory и shared memory.....	335
<b>Сымагулов А., Смургин В., Белоусов А., Карыпов А., Юничева Н.Р.</b> Улучшение качества детектирования культурных и сорных растений с помощью БПЛА на полях сои с применением сегментации изображений.....	347
<b>Ташенова Ж.М., Габдуллин А.Р., Абдугулова Ж.К., Аманжолова Ш.А., Сантеева С.А.</b> Оценка безопасности беспроводных сетей WPA3 в условиях атаки с деаутентификацией.....	368
<b>Турсунбаева Г., Сатыбалдина Д., Тлеубердин С., Ташатов Н., Эгамбердиев Э.</b> Обнаружение аномалий в телеметрических системах БПЛА на основе симуляционного моделирования.....	391
<b>Турсынова Н., Еримбетова А., Амангелді Н., Жумабаева А., Дайырбаева Э.</b> Сравнительный анализ многоязычных трансформерных моделей для перевода с казахского языка на глоссированное представление.....	414
<b>Шанпэн Лэй, Балакаева Г.</b> Двухветвевые физически информированные нейронные сети для моделирования воздушных потоков и тепловых условий в центрах обработки данных.....	433
<b>Шынжыгит Ш.Б., Балабекова М.О., Амангелды Т.Т., Малик Г.Ж., Балгимбекова У.Б.</b> Использование модели глубокого обучения на основе CNN для автоматического обнаружения дефектов кирпичной кладки.....	449

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE  
ISSN 1991-346X  
Volume 2.  
Number 358 (2026). 368–390

<https://doi.org/10.32014/2026.2518-1726.444>

IRSTI 27.47.19  
UDC 512.647

© **Tashenova Zh.<sup>\*</sup>, Gabdullin A.R.<sup>1</sup>, Abdugulova Zh.<sup>1</sup>, Amanzholova Sh.<sup>2</sup>,  
Santeyeva S.<sup>1</sup>, 2026.**

Department of Information Security, L.N. Gumilyov Eurasian National  
University, Astana, Kazakhstan.  
E-mail: zhuldyz\_tm@mail.ru

### **SECURITY EVALUATION OF WPA3 WIRELESS NETWORKS UNDER DEAUTHENTICATION ATTACK SCENARIOS**

**Tashenova Zhuldyz** — PhD, Department of Information Security, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Gabdullin Abzal** — Department of Information Security System, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: anchorite.exe@gmail.com, <https://orcid.org/0000-0003-3051-1605>;

**Abdugulova Zhanat** — Associated Professor, Department of Information Technologies, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: janat\_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

**Amanzholova Shirin** — PhD, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan,

E-mail: schirin75@mail.ru; <https://orcid.org/0000-0002-6674-2766>;

**Santeyeva Saya** — PhD, Department of Information Security, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: saya\_santeyeva@mail.ru, <https://orcid.org/0000-0001-9426-6704>.

**Abstract.** Wireless networks are now ubiquitous as part of the global digital infrastructure, providing communications in residential, commercial and public contexts. The advent of the Wi-Fi Protected Access III (WPA3) protocol has represented a major advance in wireless network security through improved authentication and better cryptographic protections. Nevertheless, despite the advances provided by WPA3, there continue to be vulnerabilities in wireless network availability that attackers can leverage. Specifically, de-authentication attacks exploit vulnerabilities in IEEE 802.11 management frames that do not compromise the integrity of encryption, but can disrupt client access to the network. This study aims at assessing the resistance of WPA3 wireless networks against de-authentication attacks, as well as analyzing the effects of these attacks on the availability of the network. The study employed an experimental approach

based on a controlled wireless testbed where both WPA2 and WPA3 network configurations were created and tested with simulated de-authentication attacks. The results demonstrated that while WPA3 provides significant improvements in authentication and encryption, it is possible to negatively impact its availability through de-authentication attacks under specific circumstances. The study identifies potential avenues to improve the protection of wireless networks against availability attacks, including enhancing the protection of IEEE 802.11 management frames and developing more sophisticated intrusion detection systems. The purpose of this study is to evaluate the behavior of modern wireless networks under deauthentication attacks and to assess the impact of these attacks on wireless network availability in a network infrastructure that utilizes modern security standards. The experiments demonstrate that deauthentication attacks can seriously impact wireless network stability, disrupting communications between wireless devices and access points.

**Keywords:** Wireless network security, WPA3, Deauthentication attack, Wi-Fi security, Wireless intrusion detection

*For citations: Tashenova Zh., Gabdullin A.R., Abdugulova Zh., Amanzholova Sh., Santeyeva S. Security evaluation of WPA3 wireless networks under deauthentication attack scenarios. Academic Scientific Journal of Computer Science, 2026. — No.2. — P. 368–390. DOI <https://doi.org/10.32014/2026.2518-1726.444>*

© Ташенова Ж.М.\*, Габдуллин А.Р.<sup>1</sup>, Абдугулова Ж.К.<sup>1</sup>,  
Аманжолова Ш.А.<sup>2</sup>, Сантеева С.Ә.<sup>1</sup>, 2026.

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.  
E-mail: zhuldyz\_tm@mail.ru

### ДЕАТЕНТИФИКАЦИЯЛАУ ШАБУЫЛЫ СЦЕНАРИЙЛЕРІНДЕГІ WPA3 СЫМСЫЗ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН БАҒАЛАУ

**Ташенова Жұлдыз** — PhD, Ақпараттық қауіпсіздік кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,  
E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Габдуллин Абзал** — Ақпараттық қауіпсіздік кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,  
E-mail: anchorite.exe@gmail.com, <https://orcid.org/0000-0003-3051-1605>;

**Абдугулова Жанат** — экономика ғылымдарының кандидаты, қауымдастырылған профессор, Л.Н. Гумилев Атындағы Еуразия Ұлттық университеті, ақпараттық технологиялар факультеті, Астана, Қазақстан,  
E-mail: janat\_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

**Аманжолова Ширин** — PhD, Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан,  
E-mail: schirin75@mail.ru, [https:// orcid.org/0000-0002-6674-2766](https://orcid.org/0000-0002-6674-2766);

**Сантеева Сая** — PhD, Ақпараттық қауіпсіздік кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,  
E-mail:: saya\_santeeva@mail.ru, <https://orcid.org/0000-0001-9426-6704>.

**Аннотация.** Сымсыз желілер қазіргі уақытта тұрғын үй, коммерциялық және қоғамдық контексте байланысты қамтамасыз ететін жаһандық цифрлық инфрақұрылымның бөлігі ретінде кең таралған. Wi-Fi Protected Access III (WPA3) протоколының пайда болуы аутентификацияны жақсарту және криптографиялық қорғауды жақсарту арқылы сымсыз желі қауіпсіздігінің айтарлықтай ілгерілеуін көрсетті. Дегенмен, WPA3 ұсынған жетістіктерге қарамастан, сымсыз желінің қолжетімділігінде шабуылдаушылар пайдалана алатын осалдықтар әлі де бар. Нақтырақ айтсақ, аутентификациядан бас тарту шабуылдары IEEE 802.11 басқару шеңберіндегі осалдықтарды пайдаланады, олар шифрлаудың тұтастығына нұқсан келтірмейді, бірақ клиенттің желіге кіруіне кедергі келтіруі мүмкін. Бұл зерттеу wpa3 сымсыз желілерінің аутентификация шабуылдарына төзімділігін бағалауға, сондай-ақ осы шабуылдардың желінің қолжетімділігіне әсерін талдауға бағытталған. Зерттеу барысында wpa2 және WPA3 желілік конфигурациялары жасалған және имитацияланған аутентификация шабуылдары арқылы сыналған басқарылатын сымсыз сынақ алаңына негізделген эксперименттік тәсіл қолданылды. Нәтижелер WPA3 аутентификация мен шифрлауда айтарлықтай жақсартуларды қамтамасыз еткенімен, белгілі бір жағдайларда аутентификациядан бас тарту шабуылдары арқылы оның қолжетімділігіне теріс әсер етуі мүмкін екенін көрсетті. Зерттеу сымсыз желілерді қолжетімділік шабуылдарынан қорғауды жақсартудың ықтимал жолдарын, соның ішінде IEEE 802.11 басқару жүйелерін қорғауды күшейтуді және интрузияны анықтаудың жетілдірілген жүйелерін әзірлеуді анықтайды. Бұл зерттеудің мақсаты - аутентификациясыз шабуылдар кезіндегі заманауи сымсыз желілердің әрекетін бағалау және осы шабуылдардың заманауи қауіпсіздік стандарттарын пайдаланатын желілік инфрақұрылымдағы сымсыз желінің қолжетімділігіне әсерін бағалау. Тәжірибелер аутентификациясыз шабуылдар сымсыз желінің тұрақтылығына айтарлықтай әсер етуі мүмкін екенін, сымсыз құрылғылар мен кіру нүктелері арасындағы байланысты бұзуы мүмкін екенін көрсетеді.

**Түйін сөздер:** Сымсыз желі қауіпсіздігі, WPA3, Деаутентификация шабуылы, Wi-Fi қауіпсіздігі, Сымсыз желілерде интрузияны анықтау

© Ташенова Ж.М.<sup>\*</sup>, Габдуллин А.Р.<sup>1</sup>, Абдугулова Ж.К.<sup>1</sup>,  
Аманжолова Ш.А.<sup>2</sup>, Сантеева С.Ә.<sup>1</sup>, 2026.

<sup>1</sup> Евразийский национальный университет имени Л.Н. Гумилева,  
Астана, Казахстан;

<sup>2</sup> Казахская национальная консерватория имени Курмангазы,  
Алматы, Казахстан.

E-mail: zhuldyz\_tm@mail.ru

## ОЦЕНКА БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ WPA3 В УСЛОВИЯХ АТАКИ С ДЕАВТЕНТИКАЦИЕЙ

**Ташенова Жулдыз** — PhD, кафедра информационной безопасности, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,  
E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Габдуллин Абзал** — кафедра информационной безопасности, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,  
E-mail: anchorite.exe@gmail.com, <https://orcid.org/0000-0003-3051-1605>;

**Абдугулова Жанат** — доцент факультета информационных технологий, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,  
E-mail: janat\_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

**Аманжолова Ширин** — PhD, Казахская национальная консерватория имени Курмангазы, Алматы, Казахстан,  
E-mail: schirin75@mail.ru, [https:// orcid.org/0000-0002-6674-2766](https://orcid.org/0000-0002-6674-2766);

**Сантеева Сая** — PhD, кафедра информационной безопасности, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,  
E-mail: saya\_santeeva@mail.ru, <https://orcid.org/0000-0001-9426-6704>.

**Аннотация.** *Актуальность.* Беспроводные сети являются важной частью современной цифровой инфраструктуры и обеспечивают связь в жилых, коммерческих, образовательных и общественных пространствах. Появление протокола Wi-Fi Protected Access III (WPA3) стало значимым этапом в развитии безопасности беспроводных сетей благодаря усовершенствованной аутентификации и криптографической защите. Вместе с тем даже при использовании WPA3 сохраняются риски, связанные с доступностью сети. В частности, атаки деаутентификации используют особенности кадров управления IEEE 802.11 и могут нарушать подключение клиентов к сети, не затрагивая напрямую криптографическую целостность передаваемых данных. *Цель.* Оценить устойчивость беспроводных сетей WPA3 к атакам деаутентификации и определить влияние таких атак на доступность беспроводной сети в условиях современной сетевой инфраструктуры. *Методы.* Исследование основано на экспериментальном подходе с использованием контролируемого беспроводного испытательного стенда. В рамках эксперимента были созданы и протестированы конфигурации сетей WPA2 и WPA3, после чего проведена имитация атак деаутентификации для оценки влияния на стабильность соединения, доступность сети и взаимодействие клиентских устройств с точкой доступа. Особое внимание

уделено анализу поведения сети при воздействии на кадры управления IEEE 802.11 и сравнению устойчивости различных конфигураций безопасности. *Результаты и выводы.* Результаты показали, что WPA3 обеспечивает существенные улучшения в части аутентификации и шифрования по сравнению с предыдущими стандартами, однако при определенных условиях атаки деаутентификации могут негативно влиять на доступность беспроводной сети. Проведенные эксперименты подтвердили, что такие атаки способны нарушать стабильность беспроводной связи, препятствовать корректному взаимодействию клиентских устройств с точками доступа и снижать надежность сетевой инфраструктуры. В исследовании определены потенциальные направления повышения защищенности беспроводных сетей от атак на доступность, включая усиление защиты кадров управления IEEE 802.11, применение механизмов мониторинга сетевых аномалий и разработку более эффективных систем обнаружения вторжений в беспроводных сетях. Практическая значимость исследования заключается в возможности использования полученных результатов при проектировании и оценке безопасности Wi-Fi-инфраструктуры в организациях, образовательных учреждениях и общественных сетях.

**Ключевые слова:** безопасность беспроводных сетей, WPA3, атака деаутентификации, безопасность Wi-Fi, IEEE 802.11, кадры управления, доступность сети, обнаружение вторжений в беспроводные сети

**Introduction.** Wireless Networks are now a central element in contemporary communication infrastructures, enabling both residential and enterprise users to transmit data via Wi-Fi. With the ever-increasing number of devices being added to wireless networks, and their increasing role as a means to provide internet access and support digital services, the security of wireless networks has emerged as a very important topic of research in modern network engineering and cybersecurity studies (Stallings et al., 2018).

The mechanism for communication in Wi-Fi networks, defined by the IEEE 802.11 standard, provides for communication between wireless clients and access points. Due to the open nature of radio transmission, wireless communication is inherently more susceptible to threats than wired networks. A threat actor who is within range of a wireless network's radio coverage can attempt to intercept data being transmitted, impersonate legitimate network devices, or disrupt communication between wireless clients and access points. This makes wireless networks particularly appealing to various types of cyberattacks, including eavesdropping, unauthorized access, and denial-of-service attacks (Mishra et al.).

There have been many different methods developed over the years to secure wireless communications. Security enhancements began with the Wired Equivalent Privacy (WEP) protocol, then evolved to Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2), which included stronger encryption and authentication mechanisms. Although there have been significant enhancements

to the WPA2 protocol family, numerous researchers have found that WPA2 networks remain vulnerable to several security attacks. One example is the Key Reinstallation Attack (KRACK) that was discovered due to vulnerabilities in the WPA2 four-way handshake, allowing an attacker to manipulate encrypted traffic under specific circumstances (Vanhoef et al., 2017).

As a response to the KRACK vulnerability, the Wi-Fi Alliance released the new WPA3 protocol, which includes better authentication mechanisms and improved cryptographic protections compared to its predecessor WPA2. Specifically, WPA3 replaces the Pre-Shared Key authentication method with the Simultaneous Authentication of Equals (SAE) protocol, designed to prevent offline dictionary attacks and improve password-based authentication. Unfortunately, subsequent research demonstrated that WPA3 is not invulnerable to all security vulnerabilities. Research published in “Dragonblood” demonstrated that weaknesses in the SAE handshake can be exploited using downgrade attacks and side-channel attacks (Vanhoef et al., 2020).

In addition to authentication vulnerabilities, researchers have also identified vulnerabilities in the IEEE 802.11 standard itself. Design flaws in frame aggregation and fragmentation mechanisms allow an attacker to manipulate encrypted frames and inject malicious traffic into wireless networks, potentially impacting multiple generations of Wi-Fi security protocols, including WPA3 (Vanhoef et al., 2021). These findings demonstrate that the security of wireless networks depends not only on the strength of encryption algorithms but also on the strength of the communication protocols.

Another type of attack that continues to exist in modern wireless networks are availability attacks. Deauthentication attacks utilize vulnerabilities in management frames to communicate between clients and access points. An attacker can cause clients to be disconnected from a wireless network by sending forged deauthentication frames. Because management frames have historically been transmitted without authentication, deauthentication attacks can continue to negatively impact modern wireless networks under certain configurations (Gonçalves et al., 2018).

Although WPA3 includes new features such as Protected Management Frames (PMF), research has indicated that availability attacks can continue to negatively impact wireless networks depending on how the network is configured and implemented. Therefore, evaluating the resiliency of WPA3 networks to deauthentication attack scenarios remains an important problem in wireless network security research.

This project evaluates the resiliency of WPA3 wireless networks to deauthentication attack scenarios and evaluates the effects of such attacks on network availability. Additionally, this project identifies limitations in modern wireless security mechanisms and outlines potential avenues for enhancing wireless network protection mechanisms in future wireless network architectures.

### **Literary review**

### ***Background of Wireless Network Security***

Wireless networks have become an essential element of contemporary digital infrastructure; they provide flexibility and scalability for end-users, businesses and public services to communicate using internet connections, mobile communications, and to transfer data. Many Wi-Fi technologies (IEEE 802.11 standards) support this process. With the rapid proliferation of wireless communication technologies comes an increased number of connected devices including mobile phones, laptops, smart home systems and IoT devices. Thus, the security of wireless networks has emerged as a significant area of study in today's network engineering and cybersecurity fields (Stallings et al., 2018).

Wireless communication systems differ from wired counterparts since they use radio signals to transmit information, thus making them susceptible to potential security threats due to being physically exposed and accessible to anyone who falls within the wireless network's signal footprint. Those individuals can intercept wireless network transmissions, impersonate legitimate network devices, or prevent communication between clients and access points. As a result, wireless networks face many different types of security threats such as unauthorized access, interception of traffic, spoofing of devices, and DoS attacks (Bianchi et al., 2018).

In order to minimize these security risks, Wi-Fi networks implement security protocols to ensure that three fundamental security characteristics are met: confidentiality, integrity, and availability. Confidentiality ensures that data transmitted via the wireless network is encrypted. Integrity ensures that transmitted data cannot be altered or tampered with. Availability provides assurance to legitimate users that access will not be interrupted. Together, these security attributes represent the basis of wireless communication protection frameworks (Stallings et al., 2018).

### ***Evolution of Wi-Fi Security Protocols***

The advancements made in Wireless Communication Technologies have been matched by the continual enhancement of Security Mechanisms aimed at securing Wireless Networks. The First Wide-Scale Deployed Wireless Security Solution was Wired Equivalent Privacy (WEP), which was included in the Original IEEE 802.11 Standards. WEP was intended to provide confidentiality via the utilization of the RC4 Stream Cipher and Shared Encryption Keys. However, subsequent research revealed multiple flaws in WEP, including weaknesses in Key Management and the Reuse of Initialization Vectors; these flaws enabled an attacker to recover encryption keys by analyzing captured traffic, ultimately rendering WEP insecure and unsuitable for modern wireless networks (Mishra et al., 2018).

As an interim wireless security solution, Wi-Fi Protected Access (WPA) was developed to mitigate the limitations of WEP. WPA incorporated the Temporal Key Integrity Protocol (TKIP), improved key management and introduced message integrity protection solutions. Although WPA significantly enhanced wireless security compared to WEP, it was designed as a transitional protocol and retained many architectural limitations.

A significant improvement in wireless network protection was provided with the development of Wi-Fi Protected Access II (WPA2). WPA2 implemented the Advanced Encryption Standard (AES) using the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), providing stronger protection for the confidentiality and integrity of wireless communications. WPA2 became the dominant security standard for wireless networks for many years. However, further research demonstrated that WPA2 was not immune to security vulnerabilities, as demonstrated by the KRACK attack (Vanhoef et al., 2017).

In response to these security challenges, the Wi-Fi Alliance developed Wi-Fi Protected Access III (WPA3), which incorporates improvements in authentication and encryption mechanisms. One of the main innovations of WPA3 is the Simultaneous Authentication of Equals (SAE) protocol, which replaces the traditional Pre-Shared Key authentication mechanism and provides stronger resistance against offline dictionary attacks. WPA3 also introduces enhanced encryption mechanisms and improved protection for management frames (Vanhoef et al., 2020).

Although improvements have been made, recent studies indicate that modern wireless security protocols still contain potential vulnerabilities. The “DragonBlood” study demonstrated that weaknesses in the SAE authentication mechanism could be exploited through downgrade attacks and side-channel attacks, highlighting limitations in the current design of WPA3 authentication procedures. In addition, further research has identified structural weaknesses in IEEE 802.11 mechanisms such as frame aggregation and fragmentation (Hamad et al., 2021).

### ***Existing Research on Wi-Fi Security***

Wi-Fi Network Security has been a subject of study for over two decades, with extensive study regarding vulnerabilities in wireless protocols, authentication methods, and network architecture. Studies on Wi-Fi Security in the past analyzed vulnerabilities in the IEEE 802.11 protocol and reviewed the efficacy of current protective mechanisms. The discovery of the KRACK vulnerability is one of the greatest contributions to Wi-Fi Security Research, demonstrating that weaknesses in the WPA2 four-way handshake could allow an attacker to manipulate cryptographic keys (Ali et al., 2022).

After the release of WPA3, researchers started studying the security aspects of the new authentication methods. The Dragonblood research found that the SAE handshake in WPA3 was susceptible to downgrade and side-channel attacks when specific conditions existed (Vanhoef et al., 2020). Further studies investigated the security features of the Dragonfly Handshake and demonstrated that both implementation details and the configuration of the protocol can greatly impact the overall security of a WPA3 network (Vanhoef et al., 2020).

Another area of research is focused on attacks that target the availability of wireless networks. Deauthentication attacks use weaknesses in management frames utilized by wireless clients and access points to maintain communication.

An attacker can send forged deauthentication frames to cause the forced disconnection of wireless devices from their networks. Recently, researchers have been exploring more sophisticated methods for detecting and preventing wireless attacks, including machine learning-based intrusion detection systems (Hamad S. et al.).

### ***Research Problem***

Despite progress in development of Wi-Fi security protocols, modern Wi-Fi networks continue to experience a number of security challenges. The transition from earlier Wi-Fi protocols including WEP and WPA, to more advanced mechanisms including WPA2 and WPA3 has greatly enhanced confidentiality and authentication features of wireless communication. However, numerous studies have demonstrated that even the latest Wi-Fi security protocols may still contain weaknesses that can be exploited by attackers.

In addition to authentication related vulnerabilities, wireless networks are vulnerable to attacks targeting the operational features of wireless communication. One of the most well-known examples is the deauthentication attack which exploits weakness in management frames used in the IEEE 802.11 protocol (Wang et al., 2023). By transmitting forged deauthentication frames, an attacker can forcefully disconnect wireless clients from access points without directly breaking the encryption mechanisms of the security protocol (Carbajal et al., 2023).

Several studies have analyzed effectiveness of existing protection mechanisms against management frame-based attacks and found that deauthentication countermeasures may still be bypassed under certain conditions (Scheppers et al., 2022). Though WPA3 introduces protection mechanisms such as Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), the practical resilience of modern Wi-Fi networks against availability-based attacks remains an important research challenge.

### ***Research Objective***

The main objective of this research is to evaluate how well modern wireless networks can recover from disruptions by means of a deauthentication attack, specifically for wireless networks secured using WPA3. The primary purpose was to test and assess the effect of a deauthentication attack on the ability of a wireless network to provide continuous connections and stable communications in both WPA2 and WPA3 environments. Furthermore, this research determines if current security protections are sufficient, and provides researchers and industry professionals with information that can be used to develop more secure wireless networks (Chatzoglou et al., 2022).

### ***Scientific Novelty***

The innovative aspect of this study are the results from the first overall assessment of resilience of current wireless networks against deauthentication attacks; particularly, it evaluated the performance of wireless networks using WPA3 security protocols. In contrast to many past studies based upon protocol design defects or theoretical models, this study conducted an experimentally-

based assessment of the impacts of deauthentication attacks in real-world wireless networks, allowing for a better understanding of how resilient today's wireless security mechanisms are.

A second novel contribution is the combination of experimental assessments with an evaluation of the prior literature on wireless security vulnerabilities and attack detection methods. The research contributes to the ongoing debate on the effectiveness of current Wi-Fi security protocols by showing that improved authentication and encryption protocols alone do not preclude all types of wireless attacks.

### **Materials and Methods**

The current section explains the experimental method used to measure the resistance of modern wireless networks under deauthentication attacks. In particular, it describes the study of the behaviors of wireless networks working under WPA2 and WPA3 security protocols which are submitted to management-frame-based attacks that target their availability (Chatzoglou et al., 2021).

The experimental study was carried out in a controlled laboratory setting so as to reproduce the results of the tests and accurately monitor wireless traffic. The research method included the establishment of a wireless testbed, the implementation of deauthentication attacks and the collection and analysis of network traffic through packet inspections (Natkaniec et al., 2022).

### **Research Methodology**

The research methodology employed within this study is based upon an experimental approach aimed at studying the effect of deauthentication attacks on modern wireless networks. The experimental methodology consists of multiple phases. At first, a controlled wireless network setting was established in order to simulate normal wireless communications settings. The experimental setup consisted of a wireless access point that worked under both WPA2 and WPA3 security protocols; a wireless client device connected to the wireless network and a monitoring device used to capture and analyze wireless traffic.

Then deauthentication attacks were implemented in order to study the responses of the wireless network to the malicious management frames. The deauthentication attacks were implemented by sending fake deauthentication frames to disrupt the communication between the wireless client and the access point. During the experiment, wireless traffic was recorded in monitoring mode so as to be able to record all the frames exchanged in the wireless network (Suryadi et al., 2021).

All the captures have been analyzed using packet inspection tools in order to identify authentication frames, management frames and deauthentication events that occurred during the attack. The results of the experiments have been used to study the resistance of wireless networks under different security configurations (Carbajal et al., 2021).

### **Experimental Testbed**

The experimental laboratory setting simulated a typical wireless communication setting and was developed to provide an experimental testbed that could replicate

the wireless network operations found in typical networks but allow for close examination and monitoring of wireless network traffic during an active attack.

There were three primary elements to the experimental setup: (1) A Wireless Access Point (WAP), which was configured to operate with current Wi-Fi security protocols; (2) A Client Device that was attached to the wireless network via a wireless interface on the WAP; (3) A Monitoring Device, which was placed into “monitoring mode” so that the wireless traffic could be captured.

The wireless infrastructure in this experimental environment was provided by a wireless access point utilizing the OpenWrt firmware. OpenWrt is an open source operating system for network devices, such as wireless routers, that provides users with flexibility in configuring their wireless devices and also provides options for configuring their wireless security settings and protocols. The wireless access point utilized in this experimental testbed is shown in Figure 1.

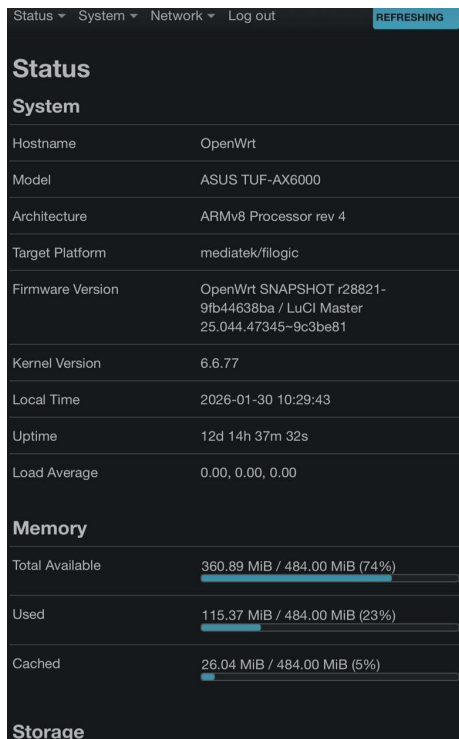


Figure 1- OpenWrt-based wireless access point used in the experimental environment.

During the normal operational phase, as well as during the Deauthentication Attack phases, the monitoring device was able to capture the wireless traffic being transmitted through the wireless network. All of the captured packets were then saved in PCAP format and were analyzed using various packet inspection tools to determine the behavior of the authentication exchanges and the behavior of the management frames and deauthentication events.

### Network Configuration

Two configurations were set up in the experimental testing environment, each based on different security protocols: a network secured by the WPA2 protocol, and a network operating under the WPA3 security protocol. The network configurations were set up to allow researchers to analyze how the current generation of wireless security mechanisms respond to de-authentication attacks.

The WPA2 network was configured to operate under the pre-shared key (PSK) method of authentication using Advanced Encryption Standard (AES) for data encryption. To verify the WPA2 network configuration parameters, the authors analyzed beacon frames and RSN Information Elements captured in the wireless traffic. The decoded RSN parameters indicated that the PSK authentication suite was used. An example of RSN parameter decoding for the WPA2 network is illustrated in Figure 2.

```

abzalqabdellin: ~$pcaps 2025$ cd ~/pcaps 2025
PCAP=wpa2_psk_12345678_2025-10.pcapng

tshark -r "$PCAP" -Y "wlan.fc.type_subtype==0x08 && wlan.rsn.akms" \
-V | egrep -n "SSID:RSN capabilities|AKM Suites|Authentication Key Management|Suite|WPA version" | head -n 80
154:      SSID: "test-wm-rsn"
198:      Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
199:      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
200:      Group Cipher Suite type: AES (CCM) (4)
201:      Pairwise Cipher Suite Count: 1
202:      Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
203:      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
204:      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
205:      Pairwise Cipher Suite type: AES (CCM) (4)
206:      Auth Key Management (AKM) Suite Count: 1
208:      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
367:      .0. .... = Multiple BSSID: Not supported
395:      ....0 = UTF-8 SSID: Not supported
634:      SSID: "test-wm-rsn"
678:      Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
679:      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
680:      Group Cipher Suite type: AES (CCM) (4)
681:      Pairwise Cipher Suite Count: 1
682:      Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
683:      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
684:      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
685:      Pairwise Cipher Suite type: AES (CCM) (4)
686:      Auth Key Management (AKM) Suite Count: 1
688:      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
847:      .0. .... = Multiple BSSID: Not supported
875:      ....0 = UTF-8 SSID: Not supported
1114:     SSID: "test-wm-rsn"
1158:     Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1159:     Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
1160:     Group Cipher Suite type: AES (CCM) (4)
1161:     Pairwise Cipher Suite Count: 1
1162:     Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
1163:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1164:     Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
1165:     Pairwise Cipher Suite type: AES (CCM) (4)
1166:     Auth Key Management (AKM) Suite Count: 1
1168:     Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
1327:     .0. .... = Multiple BSSID: Not supported
1355:     ....0 = UTF-8 SSID: Not supported

```

Figure 2- RSN information elements of the WPA2 network indicating the use of the PSK authentication suite.

A second wireless network was established using the WPA3 protocol, which builds upon prior wireless security technologies with additional enhancements including the Simultaneous Authentication of Equals (SAE) protocol (Vanhoef et al., 2017). In the experimental environment, the WPA3 network configuration was set-up using SAE authentication with Protected Management Frames enabled. The authors verified the RSN parameters of the WPA3 network by analyzing beacon frames captured during operation. An example of RSN parameter decoding for the WPA3 configuration is illustrated in Figure 3.

```
abzal@gabdullin: ~$ sudo tcpdump -i wlan0 -s 0 -w pcap.pcapng
PCAP="wpa3_2025-10.pcapng"
tshark -r "PCAP" -Y "wlan.fc.type_subtype==0x08 66 wlan.rsn.akms" \
-V | egrep -n "SSID:[Auth Key Management]AKM[SAE]Suite: 00:0f:ac" | head -n 120
153:   SSID: "WPA3-Network"
197:   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
202:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
205:   Auth Key Management (AKM) Suite Count: 1
206:   Auth Key Management (AKM) List: 00:0f:ac (Ieee 802.11) SAE (SHA256)
207:   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
208:   Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
209:   Auth Key Management (AKM) type: SAE (SHA256) (8)
233:   .1. .... = Multiple BSSID: Supported
281:   ....0 = UTF-8 SSID: Not supported
305:   SSID: "WPA3-Network"
349:   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
354:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
357:   Auth Key Management (AKM) Suite Count: 1
358:   Auth Key Management (AKM) List: 00:0f:ac (Ieee 802.11) SAE (SHA256)
359:   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
360:   Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
361:   Auth Key Management (AKM) type: SAE (SHA256) (8)
365:   .1. .... = Multiple BSSID: Supported
387:   ....0 = UTF-8 SSID: Not supported
391:   SSID: "WPA3-Network"
396:   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
397:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
399:   Auth Key Management (AKM) Suite Count: 1
400:   Auth Key Management (AKM) List: 00:0f:ac (Ieee 802.11) SAE (SHA256)
411:   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
412:   Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
413:   Auth Key Management (AKM) type: SAE (SHA256) (8)
457:   .1. .... = Multiple BSSID: Supported
485:   ....0 = UTF-8 SSID: Not supported
1209:   SSID: "WPA3-Network"
1253:   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1258:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1261:   Auth Key Management (AKM) Suite Count: 1
1262:   Auth Key Management (AKM) List: 00:0f:ac (Ieee 802.11) SAE (SHA256)
1263:   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
1264:   Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
1265:   Auth Key Management (AKM) type: SAE (SHA256) (8)
1309:   .1. .... = Multiple BSSID: Supported
1337:   ....0 = UTF-8 SSID: Not supported
1561:   SSID: "WPA3-Network"
1605:   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1610:     Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
1613:   Auth Key Management (AKM) Suite Count: 1
1614:   Auth Key Management (AKM) List: 00:0f:ac (Ieee 802.11) SAE (SHA256)
1615:   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
1616:   Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
1617:   Auth Key Management (AKM) type: SAE (SHA256) (8)
1661:   .1. .... = Multiple BSSID: Supported
1689:   ....0 = UTF-8 SSID: Not supported
```

Figure 3- RSN information elements of the WPA3 network showing the SAE authentication suite.

The wireless network configurations were set up and managed through the OpenWrt administration interface, where it is possible to have complete control of all wireless parameters including security mode, channel configuration, and authentication settings. The OpenWrt administration interface for setting up the wireless experimental network configuration is shown in Figure 4.

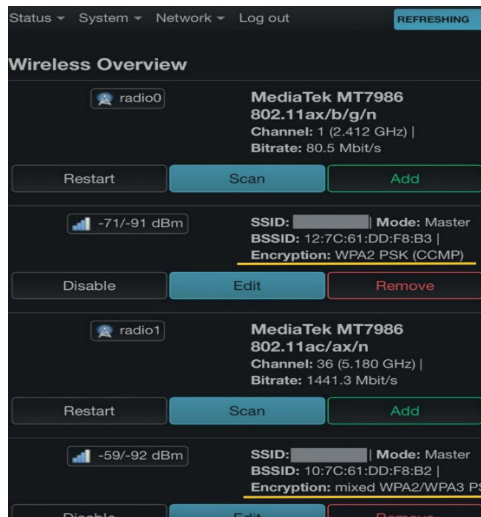


Figure 4- Wireless configuration interface of the OpenWrt-based access point used in the experimental testbed.

### Attack Modeling

This study's attack focus area is a deauthentication attack focused on disrupting the availability of wireless communication. Deauthentication attacks take advantage of the characteristics of IEEE 802.11 Management Frames, which handle the association between wireless clients and access points and are unencrypted.

Wireless clients periodically exchange management frames with their associated access point to maintain their active association. When a wireless client intentionally disconnects from a network, it sends a deauthentication frame. Due to the nature of IEEE 802.11 protocols, however, an attacker may create a deauthentication frame using forged management frames that represents itself as either the client or the access point. The target device will then see the forged frame as a valid request and subsequently disconnect from the network.

To model the attack scenario, the study employed a wireless network consisting of a single access point and one wireless client device. The attack was simulated by transmitting forged deauthentication management frames toward the target wireless client device. The attack was performed using a wireless adapter designed for packet injection. During the transmission of the deauthentication frames, a monitoring device captured all of the wireless traffic that occurred between devices on the network.

### Data Collection and Traffic Analysis

The collection and analysis of Wi-Fi traffic were an important component of the methodology. To assess the effect of death-attacks on the performance of a Wi-Fi network, all of the 802.11 wireless frames sent or received within the scope of the experiments were captured and analyzed through packet inspection techniques. Wi-Fi traffic was captured via a monitor station containing a wireless NIC functioning in "monitor" mode, which allows a device to capture all of the IEEE 802.11 frames including Management Frames, Control Frames and Data Frames.

Frames that were captured were saved as PCAP or PCAPNG files, which preserve detailed metadata for each frame, including timestamps, frame type information, and protocol hierarchy information. A depiction of metadata collected during a capture of traffic is illustrated in Figure 5.

```

ahza@gabdullin:~$ pcaps_2025$ cd ~/pcaps_2025
for f in wpa2_psk_12345678_2025-10.pcapng wpa3_2025-10.pcapng krack_example_ft_2025-10.pcapng pmf_deauth_example_2025-10.pcapng; do
  echo "---- $f ----"
  capinfos "$f" | egrep -i "File name|Number of packets|Capture duration|Earliest packet time|Latest packet time"
  echo
done
---- wpa2_psk_12345678_2025-10.pcapng ----
File name:      wpa2_psk_12345678_2025-10.pcapng
Number of packets: 39
Capture duration: 0.275304454 seconds
Earliest packet time: 2025-10-15 12:00:00.000000072
Latest packet time: 2025-10-15 12:00:00.275304526
Number of packets = 39
---- wpa3_2025-10.pcapng ----
File name:      wpa3_2025-10.pcapng
Number of packets: 167
Capture duration: 13.414401502 seconds
Earliest packet time: 2025-10-15 12:00:00.000000057
Latest packet time: 2025-10-15 12:00:13.414401639
Number of packets = 167
---- krack_example_ft_2025-10.pcapng ----
File name:      krack_example_ft_2025-10.pcapng
Number of packets: 1378
Capture duration: 48.459441261 seconds
Earliest packet time: 2025-10-15 12:00:00.000000001
Latest packet time: 2025-10-15 12:00:48.459441262
Number of packets = 1378
---- pmf_deauth_example_2025-10.pcapng ----
File name:      pmf_deauth_example_2025-10.pcapng
Number of packets: 37
Capture duration: 6.778807177 seconds
Earliest packet time: 2025-10-15 12:00:00.000000070
Latest packet time: 2025-10-15 12:00:06.778807247
Number of packets = 37
ahza@gabdullin:~$ pcaps_2025$

```

Figure 5- PCAP/PCAPNG capture metadata and timestamp parameters.

When analyzing the WPA3 network configuration, the presence of EAPOL (Extensible Authentication Protocol Over LAN) frames served as indicators that authentication was active on the wireless network. These frames represent the key exchange procedures and authentication processes that take place between the client device and the Access Point (AP). A representation of the EAPOL frames captured in the WPA3 network traffic is depicted in Figure 6.

```

abzal@gabdullin:~/pcaps_2025$ cd ~/pcaps_2025
PCAP="wpa3_2025-10.pcapng"

echo -n "EAPOL frames count (WPA3): "
tshark -r "$PCAP" -Y "eapol" | wc -l

tshark -r "$PCAP" -Y "eapol" \
  -T fields -E header=y -E separator='\t' \
  -e frame.number -e frame.time -e wlan.sa -e wlan.da -e eapol.type | head -n 25
EAPOL frames count (WPA3): 4
frame.number      frame.time          wlan.sa wlan.da eapol.type
92      Oct 15, 2025 12:00:06.711381602 +05      e2:20:ae:cb:03:04      d2:c6:b4:ab:58:88      3
94      Oct 15, 2025 12:00:06.715514396 +05      d2:c6:b4:ab:58:88      e2:20:ae:cb:03:04      3
96      Oct 15, 2025 12:00:06.715832796 +05      e2:20:ae:cb:03:04      d2:c6:b4:ab:58:88      3
98      Oct 15, 2025 12:00:06.716112352 +05      d2:c6:b4:ab:58:88      e2:20:ae:cb:03:04      3
    
```

Figure 6- Captured EAPOL frames in the WPA3 traffic record that indicate the presence of handshake artifacts during authentication.

**Results**

This section presents the traffic captured from the wireless network while the deauthentication attack was being conducted. The traffic was analyzed for its effects upon the operation of the network. Specifically, this work analyzes traffic traces collected by the monitoring system during the execution of the deauthentication attack for the presence of deauthentication frames and assesses the effectiveness of these frames in interrupting or disrupting the wireless connection established by the client.

**Execution of Deauthentication Attack**

The deauthentication attack simulated in this study consisted of transmitting forged IEEE 802.11 management frames toward a wireless client that had previously been authenticated to the experimental access point. The objective of the attack was to provide a realistic model of an availability-based attack and to determine how a wireless network would respond to malicious management frames.

Deauthentication frames were transmitted toward the client device utilizing a wireless adapter configured to perform packet injection. These frames were forged to appear as if they were legitimate communication between the access point and the client device and caused the client device to interpret them as a valid request to terminate the wireless association.

Examples of the captured deauthentication management frames are illustrated in Figures 7 and 8. These figures represent the decoding of the IEEE 802.11 frame fields observed in the captured wireless traffic trace.

```
abzalagabdullin:~pcap$ cd ~/pcaps_2025
PCAP="pmf_deauth_example_2025-10.pcapng"
tshark -r "SPCAP" -Y "frame.number==38" -V | head -n 140
Frame 36: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface hwsim0, id 0
Section number: 1
Interface id: 0 (hwsim0)
Interface name: hwsim0
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
Arrival Time: Oct 15, 2025 12:00:06.778804566 +05
UTC Arrival Time: Oct 15, 2025 07:00:06.778804566 UTC
Epoch Arrival Time: 176011696.778804566
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.002377856 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 6.778804496 seconds]
Frame Number: 36
Frame Length: 64 bytes (512 bits)
Capture Length: 64 bytes (512 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan:data]
Radiotap Header v0, Length 22
Header revision: 0
Header pad: 0
Header length: 22
Present flags:
Present flags word: 0x0000000f
.....01 = TSFT: Present
.....01 = Flags: Present
.....01 = Rate: Present
.....01 = Channel: Present
.....00 = FHSS: Absent
.....00 = dBm Antenna Signal: Absent
.....00 = dBm Antenna Noise: Absent
.....00 = Lock Quality: Absent
.....00 = TX Attenuation: Absent
.....00 = dB TX Attenuation: Absent
.....00 = dBm TX Power: Absent
.....00 = Antenna: Absent
.....00 = dB Antenna Signal: Absent
.....00 = dB Antenna Noise: Absent
.....00 = RX flags: Absent
.....00 = TX flags: Absent
.....00 = data retries: Absent
.....00 = Channels: Absent
.....00 = MCS information: Absent
.....00 = A-MPDU Status: Absent
.....00 = VHT information: Absent
.....00 = Frame timestamp: Absent
.....00 = HE information: Absent
.....00 = HE MU information: Absent
.....00 = 0 Length PSDU: Absent
.....00 = L-SIG: Absent
.....00 = Reserved: 0xd0
.....00 = TLS: Absent
.....00 = Radiotap NS next: False
.....00 = Vendor NS next: False
.....00 = Ext: Absent
MAC timestamp: 1681570102201666
Flags: 0x00
.....00 = CFP: False
.....00 = Preamble: Long
.....00 = WEP: False
.....00 = Fragmentation: False
.....00 = FCS at end: False
.....00 = Data Pad: False
.....00 = Bad FCS: False
.....00 = Short GI: False
```

Figure 7- Detailed decoding of deauthentication management frame (part 1).

```
Data Rate: 3.0 Mb/s
Channel Frequency: 2412 [2.4 GHz 1]
Channel flags: 0x0000, Complementary Code Keying (CCK), 2 GHz spectrum
.....00 = 700 MHz spectrum: False
.....00 = 800 MHz spectrum: False
.....00 = 900 MHz spectrum: False
.....00 = Turbo: False
.....01 = Complementary Code Keying (CCK): True
.....00 = Orthogonal Frequency-Division Multiplexing (OFDM): False
.....01 = 2 GHz spectrum: True
.....00 = 5 GHz spectrum: False
.....00 = Passive: False
.....00 = Dynamic CCK-OFDM: False
.....00 = Gaussian Frequency Shift Keying (GFSK): False
.....00 = GFSK (20MHz): False
.....00 = Static Turbo: False
.....00 = Half rate Channel (20MHz Channel Width): False
.....00 = Quarter Rate Channel (5MHz Channel Width): False
802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)
Short preamble: False
Data rate: 3.0 Mb/s
Channel: 1
Frequency: 2412MHz
TSF timestamp: 1681570102201666
[Duration: 529us]
[Preamble: 192us]
[IFS: 1681570102201138us]
[Start: 1681570102201138us]
[End: 1681570102201666us]
IEEE 802.11 deauthentication, Flags: p.....
Type/Subtype: Deauthentication (ex000c)
Frame Control fields: 0x0000
.....00 = Version: 0
.....00 = Type: Management frame (0)
.....1100 = Subtype: 12
Flags: 0x00
.....00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.....00 = More Fragments: This is the last fragment
.....00 = Retry: Frame is not being retransmitted
.....00 = PMF MFG STA wait stay up
.....00 = More Data: No data buffered
.....01 = Protected flag: Data is protected
.....00 = HT/Order flag: Not strictly ordered
.....0000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: 02:00:00:00:00:00 (02:00:00:00:00:00)
.....01 = IG bit: Locally administered address (this is NOT the factory default)
.....00 = IG bit: Individual address (unicast)
Destination address: 02:00:00:00:00:00 (02:00:00:00:00:00)
.....01 = IG bit: Locally administered address (this is NOT the factory default)
.....00 = IG bit: Individual address (unicast)
Transmitter address: 02:00:00:00:01:00 (02:00:00:00:01:00)
.....01 = IG bit: Locally administered address (this is NOT the factory default)
.....00 = IG bit: Individual address (unicast)
Source address: 02:00:00:00:01:00 (02:00:00:00:01:00)
.....01 = IG bit: Locally administered address (this is NOT the factory default)
.....00 = IG bit: Individual address (unicast)
BSS Id: 02:00:00:00:00:00 (02:00:00:00:00:00)
.....01 = IG bit: Locally administered address (this is NOT the factory default)
.....00 = IG bit: Individual address (unicast)
.....0000 = Fragment number: 0
.....0000 0101 0011 = Sequence number: 0
[WLAN Flags: p.....]
COP parameters
COP Ext. Initialization Vector: 0x000000000001
Key Index: 0
Data (10 bytes)
0000 28 95 09 0d 76 a1 ed 6b 3f 00 (.....k.)
Data: 2895090d76a1ed6b3f00
[Length: 10]
```

Figure 8- Detailed decoding of deauthentication management frame (part 2).

The decoded frame fields verify that the transmitted frames are IEEE 802.11 deauthentication management frames that include frame control fields, transmitter and receiver MAC addresses, and reason codes that indicate the termination of a wireless association. Analysis of the captured wireless traffic indicated that the injected deauthentication frames successfully terminated communication between the wireless client and the access point.

### ***Results for WPA2 Network***

The initial test case used a wireless network operating under the WPA2 security standard. In normal network operation, the wireless client remained associated to the access point, and the captured trace indicated typical IEEE 802.11 network communications, including beacon frames, authentication dialogues and encrypted data transfer.

During the de-authentication attack, forged de-authentication management frames were sent towards the wireless client device, which was currently connected to the access point. The received frames led to the client device losing its association with the network, and attempting to re-associate again. An examination of the captured trace demonstrated that the WPA2 network was susceptible to the described de-authentication attack.

The numerous de-authentication frames captured during the attack could be easily identified through the analysis of the IEEE 802.11 management frame fields and reason codes present within each packet. Therefore, the results obtained from this study demonstrate that the WPA2 network is still vulnerable to de-authentication attacks on network availability, but unlike traditional man-in-the-middle (MitM) attacks, no encryption keys nor authentication credentials were compromised.

### ***Results for WPA3 Network***

The second set of experiments used a network configured with the WPA3 security protocol. During normal operation the network demonstrated stable connectivity between the wireless client and access point. Analysis of captured traffic traces from the PCAP file showed standard IEEE 802.11 communication patterns including beacon frames, authentication exchanges and encrypted data transmissions.

The WPA3 protocol has several advantages over earlier wireless security methods, notably in the area of authentication. The SAE protocol was designed to improve password-based authentication by providing better protection against offline dictionary attacks (Vanhoef M. et al., 2020). Despite these improvements, the experimental results show that attacks targeting management frame behavior may still affect the availability of Wi-Fi networks.

During the execution of the deauthentication attack, forged IEEE 802.11 deauthentication frames were sent towards the Wi-Fi client device connected to the access point. Analysis of the captured traffic traces confirmed that the deauthentication frames caused the connection termination events on the client device. The Wi-Fi client interpreted the forged management frames as legitimate

requests to terminate the connection and subsequently attempted to reconnect to the access point.

**Impact on Network Availability**

Experimental results from deauthentication attack simulations show significant disruption in availability of wireless network communications. Analysis of captured traffic showed that injecting forged deauthentication management frames caused the wireless client to be disconnected from the access point multiple times and attempt to reconnect. During the simulation, the client continuously lost and then tried to regain connection to the AP through WPA2 and WPA3 network configurations.

Although the WPA3 protocol includes enhanced authentication mechanisms compared to past wireless security protocols, the experimental results indicated that it does not provide complete protection against availability-based attacks. The results confirmed that management-frame based attacks can disrupt wireless connectivity even when using current generation wireless security.

```

abzal@gabdullin: ~/pcaps_2025$ cd ~/pcaps_2025
PCAP="pmf_deauth_example_2025-10.pcapng"
echo -n "Deauth frames: "
tshark -r "$PCAP" -Y "wlan.fc.type_subtype==0x0c" | wc -l
Deauth frames: 1
abzal@gabdullin: ~/pcaps_2025$
    
```

Figure 9- Deauthentication frame activity observed in captured wireless traffic during attack execution.

Table 1 – Impact of deauthentication attack on wireless network availability

Parameter	WPA2 Network	WPA3 Network
Successful client disconnection	Yes	Yes
Reconnection attempts observed	Yes	Yes
Presence of deauthentication frames in traffic	High	High
Impact on network availability	Significant	Significant
Authentication mechanism affected	No	No
Encryption compromised	No	No

Table 1 shows the results of the experiment clearly indicating that the main effect of the deauthentication attack is to interfere with the operation of the wireless network, rather than to break either the authentication mechanism or the encryption mechanism. Thus, the deauthentication attack targeted the availability of the network rather than the confidentiality or integrity of the transmitted data.

```

abzal@gabdullin: ~/pcaps_2025$ set -euo pipefail
cd ~/pcaps_2025
mkdir -p ~/pcaps_out

OUT=~/pcaps_out/results_table.txt

{
  printf "%-34s %8s %12s %10s %8s %8s %8s %8s\n" \
    "FILE" "PKTS" "DUR(s)" "PPS" "MGMT" "DATA" "EAPOL" "DEAUTH"

  for f in \
    wpa2_psk_12345678_2025-10.pcapng \
    wpa3_2025-10.pcapng \
    pmf_deauth_example_2025-10.pcapng \
    krack_example_ft_2025-10.pcapng
  do
    # PKTS with commas/spaces removed (e.g., "1,378" -> "1378")
    pkts=$(capinfos "$f" | awk -F: '/Number of packets/ {gsub(/[, ], "", $2); print $2}')
    # duration seconds
    dur=$(capinfos "$f" | awk -F: '/Capture duration/ {gsub(/ seconds/, "", $2); gsub(/ ^/, "", $2); print $2}')
    # PPS (safe if dur=0)
    pps=$(python3 - <<PY
pkts=float("$pkts")
dur=float("$dur") if float("$dur")>0 else 1.0
print(f"{pkts/dur:.2f}")
PY
)

    # Counts from tshark (never crash on parse errors)
    mgmt=$(tshark -r "$f" -Y "wlan.fc.type==0" 2>/dev/null | wc -l | tr -d ' ')
    data=$(tshark -r "$f" -Y "wlan.fc.type==2" 2>/dev/null | wc -l | tr -d ' ')
    eapol=$(tshark -r "$f" -Y "eapol" 2>/dev/null | wc -l | tr -d ' ')
    deauth=$(tshark -r "$f" -Y "wlan.fc.type_subtype==0x0c" 2>/dev/null | wc -l | tr -d ' ')

    printf "%-34s %8s %12s %10s %8s %8s %8s %8s\n" \
      "$f" "$pkts" "$dur" "$pps" "$mgmt" "$data" "$eapol" "$deauth"
  done
} | tee "$OUT"

echo
echo "Saved: $OUT"
FILE PKTS DUR(s) PPS MGMT DATA EAPOL DEAUTH
wpa2_psk_12345678_2025-10.pcapng 39 0.275304454 141.66 16 6 4 2
wpa3_2025-10.pcapng 167 13.414401582 12.45 151 4 4 1
pmf_deauth_example_2025-10.pcapng 37 6.778807177 5.46 19 5 5 1
krack_example_ft_2025-10.pcapng 1378 48.459441261 28.44 1089 141 4 1
Saved: /home/abzal/pcaps_out/results_table.txt

```

Figure 10 – Comparative packet statistics observed during normal operation and deauthentication attack scenarios.

These results identify an important aspect of contemporary wireless security mechanisms: that although recent generations of Wi-Fi standards have greatly improved the level of authentication and encryption security, management-frame based attacks could potentially affect the stability of wireless networks.

**Discussion**

In order to better understand the behaviors of wireless communications in response to an attack on the deauthentications, the researchers analyzed the captured packets from their experiment and identified how much of an impact an attack that uses forged deauthenticating frames can cause to the availability of wireless communications. The forged deauthenticating frames resulted in the access point repeatedly disconnecting from the client device, which resulted in a disruption in the network’s availability until the access point was able to reconnect back to the client device.

Additionally, according to the researcher’s findings, most of the improvements in the WPA3 protocol were focused on the authentication and cryptographic aspects. The Simultaneous Authentication of Equals (SAE) protocol is designed to improve the security of the authentication mechanism and prevent a user’s password from being guessed (Vanhoef et al., 2020). However, the results found in this study demonstrate that even though the SAE protocol provides improved security against authentication-related attacks, there are still ways to disrupt the

normal operation of a wireless network through the use of a deauthenticating frame.

### ***Interpretation of Experimental Results***

The experimental results clearly demonstrate that deauthentication attacks can disrupt wireless network availability regardless of the Wi-Fi security protocol in use. This behavior is in-line with the way the IEEE 802.11 protocol works; the 802.11 standard states that management frames are used by network devices to determine if they are associated with each other (Dalal et al., 2023).

Previous studies have shown that similar types of attacks, including deauthenticating frames, are still possible and can disrupt the normal functioning of a wireless network, due to the fact that these attacks target the control mechanisms of the wireless protocol and not the encryption methods (Chadee et al., 2022). Therefore, even if a wireless network has implemented strong authentication mechanisms, a deauthenticating frame attack can potentially disrupt its operation.

Furthermore, the researchers identified that the deauthenticating frames produced visible anomalies in the normal patterns of wireless traffic. The anomalies that occur as a result of deauthenticating frames may be useful for developing intrusion detection mechanisms and wireless monitoring systems that can detect these types of attacks (Moharam et al., 2024).

### ***Limitations of WPA3 Security Mechanisms***

WPA3 introduces significant improvements to wireless network security; however, it does not fully eliminate all potential vulnerabilities. The protocol primarily focuses on strengthening authentication mechanisms and improving protection against password-based attacks. These improvements represent an important advancement compared to previous wireless security standards, but they do not address all possible attack vectors within wireless communication systems.

The experimental results indicate that attackers may still influence wireless network connectivity by targeting management frame exchanges, particularly through deauthentication attacks. These attacks exploit the control mechanisms responsible for maintaining associations between wireless clients and access points. Because these mechanisms operate independently from the main encryption process, they may still be used to disrupt the availability of wireless communication.

Beyond authentication-related limitations, potential vulnerabilities may also arise from other aspects of the IEEE 802.11 protocol design. Previous studies have identified weaknesses related to frame aggregation and fragmentation mechanisms, which were originally introduced to improve network performance but may introduce additional security risks. These observations suggest that improving wireless network security requires a broader approach that extends beyond authentication improvements alone.

### ***Comparison with Previous Research***

The results obtained in this study are consistent with findings reported in previous research examining how wireless networks behave under attack conditions. Earlier

studies have shown that attackers frequently use deauthentication techniques to disrupt wireless communication by exploiting weaknesses in the way wireless networks manage device connections and exchange management frames (Wang et al., 2022). These attacks remain one of the most common methods used to interfere with wireless network availability.

Large-scale traffic analysis studies, such as the AWID3 dataset, verify that management frame-based attacks still exist in modern wireless environments. The research methodology adopted in this study is similar to those presently being adopted in wireless network security research, using a testbed environment to study how wireless networks behave under attack (Carbajal et al., 2022). The findings of this study provide additional evidence of how availability-based attacks can impact the stability of wireless networks even when security protocols like WPA3 are being adopted.

### ***Future Directions for Wireless Network Security***

The results obtained from the study demonstrate that the development of the resilience of wireless communication systems against availability-based attacks is an important area for further research. One promising area is the development of sophisticated wireless monitoring systems able to identify abnormal management frame traffic in real-time. The application of traffic analysis for detecting abnormal wireless traffic that could indicate attack activities has already been identified as having considerable potential (Suryadi et al., 2024).

Another important area for further research is the development of wireless intrusion detection systems that take into account the application of modern security protocols such as WPA3. The application of machine learning could provide the solution for the accurate identification of complex attack patterns in wireless network environments (Wang et al., 2023).

Moreover, the development of wireless resilience against other sophisticated attack mechanisms that compromise wireless communication protocols, such as side-channel attacks and packet-level manipulation attacks, has been identified in emerging wireless security research (Wang et al., 2022). Therefore, the development of wireless security mechanisms in the future must consider the integration of stronger authentication protocols, sophisticated monitoring mechanisms, and advanced detection mechanisms.

### **Conclusion**

This study aimed to evaluate the behavior of modern wireless networks under deauthentication attack scenarios and evaluate the impacts of these attacks on the availability of wireless networks within a network infrastructure that uses modern security standards. The experiments conducted have shown that deauthentication attacks can severely affect the stability of wireless communication by disrupting the association between wireless devices and wireless access points.

Although the WPA3 security protocol has shown significant improvements in wireless network authentication security using Simultaneous Authentication of Equals (SAE), the experiments have shown that these improvements do not entirely

remove the impacts of attacks on the behavior of wireless network management frames. This shows a severe limitation of modern wireless security standards, which mostly attempt to strengthen wireless network authentication security.

The contribution of this work to the scientific community lies in the experimental assessment of the resilience of the wireless network under deauthentication attack scenarios, conducted in controlled environments using traffic analysis. This work adds further weight to the fact that attacks involving the use of management frames still need to be considered in modern wireless networks.

This work further stresses the need to ensure that future wireless security protocols not only focus on improving existing authentication protocols but also include effective detection mechanisms. Improving the security of management frames, improving the capabilities of existing wireless intrusion detection systems, and improving traffic analysis techniques can greatly improve the resilience of modern wireless networks against availability attacks.

Future research will thus be focused on the development of stronger wireless monitoring systems that can effectively identify any abnormalities in the management frames in real time, as well as the improvement of the design of wireless security protocols to effectively combat threats to network availability. Continued investigation of wireless attack scenarios in controlled experimental environments is necessary to evaluate the effectiveness of newly developed wireless security mechanisms.

Generally, the current research seeks to provide a deeper understanding of the behavior of modern wireless networks when subjected to deauthentication attack scenarios, as well as the challenges that must be overcome to effectively advance the security of future wireless communication systems.

### References

W. Stallings (2018) *Wireless Communications and Networks*. Upper Saddle River, NJ, USA: Pearson Education. (in English)

A. Mishra and W.A. Arbaugh (2002) "An Initial Security Analysis of the IEEE 802.11 Wireless Network Protocol," Univ. Maryland, College Park, MD, USA, Tech. Rep. (in English)

M. Vanhoef and F. Piessens (2017) "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS). — P. 1313–1328, doi: 10.1145/3133956.3134027. (in English)

M. Vanhoef and E. Ronen (2020) "Dragonblood: A Security Analysis of WPA3's SAE Handshake," in Proc. IEEE Symp. Security and Privacy. — P. 517–533, doi: 10.1109/SP40000.2020.00037 (in English)

M. Vanhoef (2021) "Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation," in Proc. USENIX Security Symp. — P. 183–199. (in English)

R. Gonçalves, M. E. Correia, and P. Brandão (2018) "A Flexible Framework for Rogue Access Point Detection," in Proc. Int. Conf. Security and Cryptography (SECRYPT). — P. 1–8. (in English)

G. Bianchi (2000) "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3. — P. 535–547, Mar. doi: 10.1109/49.840210. (in English)

S. Hamad et al. (2021) "Machine Learning-Based Intrusion Detection for Wireless Networks," *IEEE Access*, vol. 9. — P. 123456–123468. (in English)

M. Vanhoef and C. Matte (2020) “Dragonblood: Analyzing the Dragonfly Handshake of WPA3,” *IEEE Security Privacy*, vol. 18, no. 3. — P. 51–57, May/Jun. doi: 10.1109/MSEC.2020.2979196. (in English)

A. Ali, S. Khan, and I. Ahmad (2022) “Security Analysis of Modern Wi-Fi Networks: Attacks and Countermeasures,” *IEEE Access*, vol. 10. — P. 65432–65450. doi: 10.1109/ACCESS.2022.3176543. (in English)

Z. Wang, X. Feng, Q. Li, K. Sun, and Y. Yang (2023) “Real-Time Detection of Wi-Fi Attacks Using Hybrid Deep Learning Models,” *IEEE Access*, vol. 11. — P. 11234–11248. (in English)

A. Carbajal and A. Akbarfam (2023) “Evaluating the Effectiveness of WPA3 Protocol Against Advanced Hacking Attacks,” in *Proc. Int. Conf. Cyber Security*. — P. 45–52. (in English)

D. Schepers, A. Ranganathan, and M. Vanhoef (2021) “On the Robustness of Wi-Fi Deauthentication Countermeasures,” in *Proc. ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec)*. — P. 101–112, doi: 10.1145/3507657.3528540. (in English)

E. Chatzoglou, G. Kambourakis, and C. Koliass (2021) “How Is Your Wi-Fi Connection Today? DoS Attacks on WPA3-SAE,” *J. Inf. Security Appl.*, vol. 63, Art. no. 103020. doi: 10.1016/j.jisa.2021.103020. (in English)

E. Chatzoglou, G. Kambourakis, and C. Koliass (2021) “Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset,” *IEEE Access*, vol. 9. — P. 34188–34205. doi: 10.1109/ACCESS.2021.3061211. (in English)

M. Natkaniec and M. Bednarz (2023) “Wireless Local Area Networks Threat Detection Using 1D-CNN,” *Sensors*, vol. 23, no. 4, Art. no. 2145. doi: 10.3390/s23042145. (in English)

M.T. Suryadi et al. (2024) “Machine Learning-Based Policing Models for Cyber-Attack Detection in Wi-Fi Networks,” *Electronics*, vol. 13, no. 2, Art. no. 415. doi: 10.3390/electronics13020415. (in English)

A. Carbajal and A. Akbarfam (2023) “A Software-Defined Testbed for Quantifying Deauthentication Resilience in Modern Wi-Fi Networks,” in *Proc. IEEE Int. Conf. Commun. (ICC)*. — P. 1–6. (in English)

N. Dalal et al. (2023) “A Wireless Intrusion Detection System for 802.11 WPA3 Networks,” in *Proc. IEEE Int. Conf. Cyber Security and Resilience*. — P. 78–85. (in English)

K. Chadee, W. Goodridge, and K. Khan (2022) “Recovering WPA3 Network Password by Bypassing the Simultaneous Authentication of Equals Handshake Using a Social Engineering Captive Portal,” in *Proc. Int. Conf. Cyber Warfare Security*. — P. 55–63. (in English)

M.H. Moharam et al. (2024) “Real-Time Detection of Wi-Fi Attacks Using Hybrid Deep Learning Models on NodeMCU,” *Sensors*, vol. 24, no. 1, Art. no. 145. doi: 10.3390/s24010145. (in English)

Z. Wang et al. (2022) “Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side-Channel Attack,” in *Proc. USENIX Security Symp.* — P. 987–1004. (in English)

## **Publication Ethics and Publication Malpractice in the journals of the Central Asian Academic Research Center LLP**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct ([http://publicationethics.org/files/u2/New\\_Code.pdf](http://publicationethics.org/files/u2/New_Code.pdf)). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Requirements for articles design for publication in the journal are available on the websites:

**[www.nauka-nanrk.kz](http://www.nauka-nanrk.kz)  
<http://physics-mathematics.kz/index.php/en/archive>  
ISSN2518-1726 (Online),  
ISSN 1991-346X (Print)**

Managing Editor: *A. Shormakova*  
Editors: *D.S. Alenov, T. Apendiev*  
Computer layout: *G.D. Zhadyranova*

Signed for print: June 15, 2026  
Format: 70×90 1/16. 26.5 printed sheets. Order No. 2.