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

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№3
2025

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

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

3 (355)

JULY – SEPTEMBER 2025

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, acting General Director of the Institute of Information and Computing Technologies CS MES 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

BIYASHEV Rustam Gakashevich, doctor of technical sciences, professor, Deputy Director of the Institute for Informatics and Management Problems, Head of the Information Security Laboratory (Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=6603642864, https://www.webofscience.com/wos/author/record/3802016

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, 2025

БАС РЕДАКТОР:

МҰТАНОВ Ғалымқайыр Мұтанұлы, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының м.а. (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=6506682964, https://www.webofscience.com/wos/author/record/1423665

РЕДАКЦИЯ АЛҚАСЫ:

ҚАЛИМОЛДАЕВ 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

БИЯШЕВ Рустам Гакашевич, техника ғылымдарының докторы, профессор, Информатика және басқару мәселелері институты директорының орынбасары, Ақпараттық қауіпсіздік зертханасының меңгерушісі (Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=6603642864, https://www.webofscience.com/wos/author/record/3802016

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, 2025

ГЛАВНЫЙ РЕДАКТОР:

МУТАНОВ Галимкаир Мутанович, доктор технических наук, профессор, академик НАН РК, и.о. генерального директора «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=6506682964, https://www.webofscience.com/wos/author/record/142 3665

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/authid/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/authid/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 Сатпаева (Алматы, Казахстан), https://www.scopus.com/authid/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/authid/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/authid/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/authid/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/authid/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/authid/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/authid/detail.uri?authorId=55453992600, https://www.webofscience.com/wos/author/record/3802041

БИЯШЕВ Рустам Гакашевич, доктор технических наук, профессор, заместитель директора Института проблем информатики и управления, заведующий лабораторией информационной безопасности (Казахстан), https://www.scopus.com/authid/detail.uri?authorId=6603642864,https://www.webofscience.com/wos/author/record/3802016

КАПАЛОВА Нурсулу Алдажаровна, кандидат технических наук, заведующий лабораторией кибербезопасности РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/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/authid/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/authid/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/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)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО 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», 2025

CONTENTS

МАЗМҰНЫ

СОДЕРЖАНИЕ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 3. Namber 355 (2025). 228–242

https://doi.org/10.32014/2025.2518-1726.374

МРНТИ 27.47.19
УДК 512.647

Zh. Tashenova, A.R. Gabdullin, Zh. Abdugulova, Sh. Amanzholova, E. Nurlybaeva, 2025.
Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-mail: zhuldyz_tm@mail.ru

ANALYSIS OF MODERN WIRELESS NETWORK SECURITY PROTOCOLS AND PROSPECTS FOR THEIR DEVELOPMENT

Tashenova Zh. — PhD, Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Gabdullin A. — Master of Information Security Systems, 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 Zh. — 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 Sh. — PhD, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan,
E-mail: schirin75@mail.ru;
Nurlybaeva E. — PhD, Department of Information Technologies, The Kazakh National Academy of Arts named after T. Zhurgenova, Almaty, Kazakhstan,
E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Abstract. Modern wireless networks rely on robust security protocols for data protection and offering secure connectivity. In this paper, we address the weaknesses and strengths of WPA2 (Wi-Fi Protected Access II) and its successor WPA3 (Wi-Fi Protected Access III), and examine prospects for their future development. We summarize authentication mechanisms of the protocols (including the SAE handshake of WPA3) and examine their resistance to popular attack vectors such as handshake capture, deauthentication, and the KRACK (Key Reinstallation Attack) vulnerability. Our results demonstrate that WPA3 eliminates a number of WPA2 weaknesses by neutralizing these common attacks: the improved handshake and mandatory protections of WPA3 entirely thwart the use of captured handshakes for offline cracking and significantly reduce exposure to deauthentication and key reinstallation attacks. There are, however, some open issues requiring further improvement in the protocols to counter emerging threats. These findings underscore

the imperative of universal WPA3 adoption and ongoing protocol improvements to deliver strong, future-resistant wireless network security. This article presents a comprehensive analysis of modern wireless network security protocols, focusing on their architecture, functionality, and resistance to contemporary cyber threats. The study examines widely used standards, including WPA3, TLS-based mechanisms, and emerging encryption approaches, highlighting their strengths and existing vulnerabilities.

Keywords: Wireless Networks, WPA3, WPA2, Security Protocols, Cyber Threats

Ж.М. Ташенова, А.Р. Габдуллин, Ж.К. Абдугулова, Ш.А. Аманжолова, Э.Н. Нурлыбаева, 2025.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
E-mail: zhuldyz_tm@mail.ru

ЗАМАНАУИ СЫМСЫЗ ЖЕЛІНІҢ ҚАУІПСІЗДІК ХАТТАМАЛАРЫН ТАЛДАУ ЖӘНЕ ОЛАРДЫҢ ДАМУ ПЕРСПЕКТИВАЛАРЫ

Ташенова Ж.М. — PhD, Ақпараттық технологиялар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Габдуллин А.Р. — ақпараттық қауіпсіздік жүйелері магистрі, Ақпараттық қауіпсіздік жүйелері кафедрасы, Ақпараттық технологиялар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: anchorite.exe@gmail.com, https://orcid.org/0000-0003-3051-1605;
Абдугулова Ж.К. — 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 Ш.А. — PhD, Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан,
E-mail: schirin75@mail.ru, https:// orcid.org/0000-0002-6674-2766;
Нұрлыбаева Э.Н. — PhD, Т.Жүргенова атындағы Қазақ ұлттық өнер академиясы, ақпараттық технологиялар кафедрасы, Алматы, Қазақстан,
E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Аннотация. Қазіргі заманғы сымсыз желілер деректерді қорғау мен қауіпсіз байланысты қамтамасыз ету үшін сенімді қауіпсіздік хаттамаларына сүйенеді. Бұл мақалада WPA2 (Wi-Fi Protected Access II) және оның мұрагері WPA3 (Wi-Fi Protected Access III) хаттамаларының әлсіз және күшті жақтары қарастырылып, олардың болашақтағы даму перспективалары талданады. Протоколдардың аутентификация механизмдері (соның ішінде WPA3-тегі SAE қол алысуы) сипатталып, оларды жиі кездесетін шабуыл түрлеріне – қол алысуды ұстап қалу, деаутентификация және KRACK (Key Reinstallation Attack) осалдығына қарсы төзімділігі зерттеледі. Зерттеу нәтижелері WPA3 нұсқасының WPA2-дегі бірқатар осал тұстарды жойып, қол алысуды жақсарту және міндетті қорғаныс тетіктері арқылы оффлайн-құпиясөзді бұзу әрекеттерін

толықтай болдырмайтынын, сондай-ақ деаутентификация мен кілтті қайта орнату шабуылдарына қарсы әлдеқайда тиімді қорғаныс беретінін көрсетті. Дегенмен, жаңа қауіптерге қарсы тұру үшін әлі де жетілдіруді қажет ететін мәселелер бар. Бұл тұжырымдар WPA3 хаттамасын әмбебап енгізу мен оның үздіксіз жетілдірілуінің заманауи сымсыз желілердің қауіпсіздігін қамтамасыз етуде шешуші маңызға ие екенін айқындайды. Мақалада заманауи сымсыз желілердің қауіпсіздік хаттамалары олардың архитектурасы, функционалдығы және киберқауіптерге төзімділігі тұрғысынан жан-жақты талданады. Сондай-ақ WPA3, TLS негізіндегі тетіктер мен жаңа шифрлау әдістері секілді кеңінен қолданылатын стандарттардың артықшылықтары мен осал тұстары көрсетіледі. Сонымен қатар, мақалада қауіпсіздік технологияларының даму үрдістері қарастырылып, постквантық криптографияның, нөлдік сенім үлгілерінің және жасанды интеллектке негізделген шешімдердің рөлі атап көрсетіледі. Талдау нәтижелері сымсыз желілердің қауіпсіздігін болашақта дамыту үшін технологиялық инновацияларды, нормативтік шараларды және бейімделгіш қауіптерге қарсы әрекет ету стратегияларын біріктіретін кешенді тәсілді қажет ететінін көрсетеді.

Түйін сөздер: сымсыз желілер, WPA3, WPA2, Қауіпсіздік хаттамалары, Киберқауіптер

Ж.М. Ташенова, А.Р. Габдуллин, Ж.К. Абдугулова, Ш.А.Аманжолова, Э.Н. Нурлыбаева, 2025.
Евразийский национальный университет им. Л.Н. Гумилёва,
Астана, Казахстан.
E-mail: zhuldyz_tm@mail.ru

АНАЛИЗ СОВРЕМЕННЫХ ПРОТОКОЛОВ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

Ташенова Ж.М. — PhD, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Республика Казахстан,
E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Габдуллин А.Р. — магистр по системам информационной безопасности, кафедра систем информационной безопасности, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилёва, Астана, Казахстан,
E-mail: anchorite.exe@gmail.com, https://orcid.org/0000-0003-3051-1605;
Абдугулова Ж.К. — доцент факультета информационных технологий Евразийского национального университета им. Л.Н. Гумилева, Астана, Казахстан,
E-mail: janat_6767@mail.ru, https://orcid.org/0000-0001-7462-4623;
Аманжолова Ш.А. — PhD, Казахская национальная консерватория им. Курмангазы, Алматы, Казахстан,
E-mail: schirin75@mail.ru, https:// orcid.org/0000-0002-6674-2766;
Нурлыбаева Э.Н. — PhD, Казахская национальная академия искусств им. Т. Жургеновой, кафедра информационных технологий, Алматы, Казахстан,
E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Аннотация. Современные беспроводные сети полагаются на надежные протоколы безопасности для защиты данных и обеспечения безопасного подключения. В этой статье мы рассмотрим слабые и сильные стороны WPA2 (Wi-Fi Protected Access II) и его преемника WPA3 (Wi-Fi Protected Access III), а также рассмотрим перспективы их будущего развития. Мы суммируем механизмы аутентификации протоколов (включая рукопожатие SAE WPA3) и исследуем их устойчивость к популярным векторам атак, таким как захват рукопожатия, деаутентификация и уязвимость KRACK (атака переустановки ключа). Наши результаты показывают, что WPA3 устраняет ряд слабых сторон WPA2, нейтрализуя эти распространенные атаки: улучшенное рукопожатие и обязательная защита WPA3 полностью пресекают использование захваченных рукопожатий для офлайн-взлома и значительно снижают подверженность атакам деаутентификации и переустановки ключа. Однако есть некоторые открытые вопросы, требующие дальнейшего улучшения протоколов для противодействия новым угрозам. Эти результаты подчеркивают необходимость всеобщего принятия WPA3 и постоянного совершенствования протокола для обеспечения надежной и устойчивой к будущим изменениям безопасности беспроводных сетей. Исследуются широко используемые стандарты, включая WPA3, механизмы на основе TLS и новые методы шифрования, с выделением их преимуществ и существующих уязвимостей. Особое внимание уделяется проблемам обеспечения конфиденциальности, целостности и аутентификации в динамичных беспроводных средах. Кроме того, в статье рассматриваются актуальные тенденции развития технологий безопасности, подчеркивается роль постквантовой криптографии, моделей «нулевого доверия» и решений на основе искусственного интеллекта.

Ключевые слова: беспроводные сети, WPA3, WPA2, протоколы безопасности, киберугрозы

Introduction. Wi-Fi is a ubiquitous part of our lives nowadays. Wi-Fi covers nearly all locations, whether homes, offices, or public hotspots. Wi-Fi's security aspects have changed and have evolved enormously over 20 years. All this development came based on various pivotal standards that were introduced to make Wi-Fi secure and reliable. Initial standards like WEP were proven to have design flaws, and thus Wi-Fi Protected Access (WPA) and most popularly used WPA2 (IEEE 802.11i) were introduced during 2004. The newest, Wi-Fi Alliance, debuted WPA3 as a successor to WPA2 back in 2018 to make WLANs' encryption and validation more secure. All these modern 802.11 security protocols (WPA2, WPA3) were designed to offer confidentiality, integrity, and access control for wireless networks, and these are currently available as the default settings for personal routers and business Wi-Fi deployments (Halbouni, Ong, & Leow, 2023; Lounis & Zulkernine, 2020).

Literature Review

Wi-Fi Protected Access II (WPA2) is the dominant WLAN security protocol for well over a decade, providing strong encryption through AES-CCMP. Several researches have, nonetheless, unveiled serious flaws in WPA2's design. Among these, there is the Key Reinstallation Attack (KRACK), which utilizes a flaw in the four-way handshake to cause a nonce reusal and decrypt traffic without knowing Wi-Fi's password (Vanhoef & Ronen, 2020). Similarly, an attacker can capture a WPA2 handshake-derived value (the PMKID) to perform offline dictionary attacks, bypassing the need to intercept the full 4-way exchange (De Almeida Braga, Fouque, & Sabt, 2020). These revelations highlight that even strong ciphers can be undermined by protocol logic errors.

Moreover, WPA2 networks are vulnerable to denial-of-service (DoS) tactics due to unprotected management frames: malicious deauthentication and disassociation packets can be injected to knock clients off a network at will (Chatzoglou, Kambourakis, & Kolias, 2022; Gebresilassie et al., 2023). In practice, weak pre-shared keys also remain an Achilles' heel of WPA2, as attackers can readily crack poorly chosen passwords through offline guessing (Banakh et al., 2024; De Almeida Braga et al., 2020). The accumulation of such vulnerabilities ultimately motivated the development of WPA3 to fortify Wi-Fi security against these exploits.

The introduction of WPA3 brought important enhancements intended to address WPA2's shortcomings. Notably, WPA3-Personal replaces the pre-shared key exchange with the Simultaneous Authentication of Equals (SAE) handshake, a variant of the Dragonfly key exchange, to provide forward secrecy and better resistance to offline password guessing (Lounis & Zulkernine, 2019). WPA3 also mandates Protected Management Frames (PMFs) to defend against deauthentication spoofing and introduces individualized data encryption even on open networks through Opportunistic Wireless Encryption (OWE) (Halbouni, Ong, & Leow, 2023; Lounis & Zulkernine, 2020). These improvements raised expectations that WPA3 would resolve the prevalent issues in WPA2.

Yet early analyses of WPA3 have shown that it is not immune to vulnerabilities. Security researchers discovered design and implementation flaws in WPA3 shortly after its release. For instance, the Dragonblood study uncovered a suite of attacks that included handshake downgrades, side-channel leaks, and denial-of-service exploits (Vanhoef & Ronen, 2020). These findings revealed that an attacker could undermine WPA3's SAE handshake—gaining the ability to run offline dictionary attacks or even overload access points with excessive processing requests—despite the protocol's new protections. Additionally, prior cryptanalysis of the Dragonfly handshake underlying SAE had identified potential weaknesses in certain parameter choices, hinting at the challenges in balancing usability with cryptographic rigor (De Almeida Braga et al., 2020; Lounis & Zulkernine, 2019).

Attackers often leverage the above protocol weaknesses through well-known Wi-Fi attack techniques. One such threat is the Evil Twin attack, wherein a rogue

access point impersonates a legitimate Wi-Fi network to lure victims into connecting (Shrivastava, Kumar, & Kataoka, 2020). By duplicating a trusted network's SSID and settings, an adversary can perform man-in-the-middle interception once clients unknowingly join the fake hotspot (Banakh et al., 2024; Chatzoglou et al., 2022). Evil Twin attacks are frequently coupled with deauthentication floods: the attacker forcefully disconnects users from the genuine AP, prompting them to reconnect—often to the stronger malicious signal (Gebresilassie et al., 2023; Shrivastava et al., 2020).

Deauthentication and related denial-of-service (DoS) attacks exploit the fact that, under WPA2, management frames are not authenticated, allowing any device to broadcast spoofed disconnection commands (Gebresilassie et al., 2023; Schepers, Ranganathan, & Vanhoef, 2022). The result is a simple but effective DoS that can disrupt service or facilitate further exploits like Evil Twin man-in-the-middle hijacking. Beyond spoofed frames, adversaries can also launch DoS attacks at the physical layer (jamming the Wi-Fi spectrum) or via resource exhaustion (flooding the network), rendering the channel unusable (Marais, Coetzee, & Blauw, 2021). These attack techniques demonstrate how weaknesses in Wi-Fi's protocol layers are actively exploited in practice, emphasizing that improvements in standards (e.g., WPA3's PMF to counter deauth) must be complemented by vigilance against a range of attack vectors.

Research Objectives and Tasks

Despite continuous improvements, current wireless security protocols still suffer from serious vulnerabilities that expose users and organizations to attacks. Given these persistent weaknesses and the fast-evolving tactics of attackers, there is a clear need for ongoing evaluation of wireless security protocols under real-world conditions.

In this work, we take a practical approach to assess the resilience of modern Wi-Fi security standards. We have built a dedicated wireless security testbed that simulates a typical network environment and allows controlled execution of various attacks (including Evil Twin setups, deauthentication floods, handshake interception, etc.) against WPA2- and WPA3-protected networks. By performing our own independent experiments, we can verify the severity of known weaknesses and observe how effectively the protocols' defenses hold up outside of theoretical analysis or vendor claims.

Through this hands-on evaluation, we present a synthesized analysis of the strengths and weaknesses of WPA2 and WPA3, and we offer insights into their suitability for different use cases. In particular, this study:

1. Identifies which known vulnerabilities remain applicable (or have been mitigated) in real deployments of WPA2 vs. WPA3 (Chatzoglou et al., 2022; Gao et al., 2021).

2. Pinpoints security gaps where further improvements or best practices are needed (for instance, in handling rogue AP threats or ensuring robust user authentication) (Gebresilassie et al., 2023; Schepers et al., 2022).

3. Provides guidance on selecting and configuring Wi-Fi security protocols for distinct contexts—from end-user home networks to large enterprise infrastructures—in light of their current security posture (Halbouni et al., 2023; Lounis & Zulkernine, 2019).

By emphasizing the practical significance of new protocol advances, this research seeks to make both researchers and practitioners of networks aware of state-of-the-art wireless security and how it is likely to evolve in the future. Ultimately, the purpose of this study lies in explaining how far advanced Wi-Fi security is and what there is still to be done to point toward and enable wiser, more robust future wireless security standards.

Materials and Methods

The testbed used for this research is illustrated in Figure 1. The setup consists of an off-the-shelf Wi-Fi router supporting both WPA2-PSK and WPA3-SAE (Personal mode), a victim client device, and an attacker's laptop running Kali Linux with an Alfa AWUS036ACH USB Wi-Fi adapter in monitor mode.

A wired control server was connected to the router's LAN to generate traffic and log attack impacts. The testbed simulates a small-office/home network, ensuring realistic conditions while allowing controlled execution of attacks.

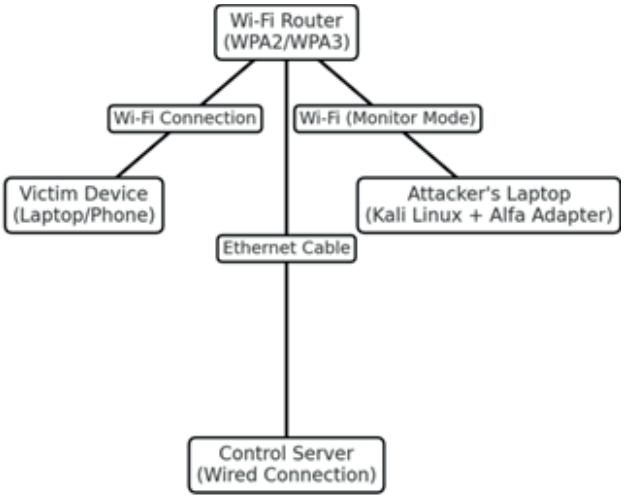

Figure 1. Diagram of the testbed setup used for hands-on experiments

Research Procedures & Attack Scenarios

We tested the resilience of WPA2 and WPA3 security protocols under practical conditions by applying a systematic penetration testing approach with Kali Linux as the basis for the test bed. We tested for four principal attack vectors for Wi-Fi exploitation: (1) Deauthentication Attack (Deauth), (2) Continuous Deauthentication as a Denial-of-Service (DoS), (3) Handshake Capture for Offline Attacks, and (4) Key Reinstallation Attack (KRACK) solely for WPA2.

Each of these types of attacks was performed within a controlled laboratory setting against both WPA2- and WPA3-secured networks sequentially to have a consistent basis for comparison. A five-step process was employed for all phases of testing to preserve methodological rigor and reproducibility. In a first step, baseline measurements of usual network operation were made to define standard performance benchmarks. Then, the specific attack script was carried out against the test network. All wireless traffic and protocol-specific packets were collected during attack instances with Wireshark and tcpdump for later examination. Then, the impact of each attack was determined based upon principal indicators such as packet loss, disconnection time, and recovery behavior of the client. Lastly, WPA2 and WPA3 results were comparatively examined to find differences between security resilience and robustness of protocol.

We repeated each attack scenario five times under the same conditions to guarantee statistical accuracy of results. Through this repetition, we could average the results obtained and look out for consistent trends or deviations between test runs to validate the experimental results.

Attack Implementation & Algorithms. Deauthentication Attack

A set of hands-on attack implementations were performed to test WPA2 and WPA3 protections with standardized procedures and tools under the testbed setup. The first attack involved a deauthentication attack, whereby an attack is performed by sending spoofed IEEE 802.11 deauthentication frames to disconnect a client forcefully from the network. As there is no protection for management frames provided by WPA2, these frames can be injected by any device with range. The attack process was conducted by putting it into monitor mode for the attack's wireless adapter, capturing the MAC address of the victim through Wireshark or airodump-ng, and sending forged deauthentication frames through aireplay-ng. As predicted, WPA2 clients got automatically disconnected as soon as spoofed packets were received, while WPA3 clients, which have Protected Management Frames (PMF) with them, remained unaffected because of the requirement for authentication for such frames.

The second attack model was a Denial-of-Service (DoS) attack through constant deauthentication, which extends the simple deauthentication attack by continually sending deauth frames with high frequency to disallow reassociation of the client. It was carried out with a loop script sending packets around 0.1 seconds apart. On WPA2 networks, this attack was found to cause heavy service disruption, with as high as 95% observed packet loss and almost total disconnection of the client. On WPA3 networks with activated PMF, there was no perceivable impact, as rogue management frames were well-filtered and discarded.

The third attack targeted handshake capture and offline cracking of passwords, with an attack on the WPA2-Personal process of authentication. The reconnection was forced with a deauth frame, and the resultant EAPOL 4-way handshake was captured with the help of packet analyzers. The handshake was pulled out with

aircrack-ng, and an offline dictionary attack was performed to try and retrieve the pre-shared key (PSK). For WPA2, this attack was successful with all attempts that had the password as part of the dictionary. For WPA3, based on the Simultaneous Authentication of Equals (SAE) protocol, offline cracking did not work. While it was still possible to capture handshake data, it did not contain adequate cryptographic data to perform offline brute-force attacks, and therefore required real-time access to the access point. The last test tried out Key Reinstallation Attack (KRACK), which involves a WPA2-specific weakness attempting to exploit repeated use of the nonce during the 4-way handshake. The attack assumed a man-in-the-middle (MITM) stance with tools such as hostapd and wpa_supplicant, intercepted the third handshake message, and resent it to the client. It compelled the client to reinstall an already active encryption key, leading to nonce reuse and potential decryption or injection of packets. On WPA2 networks, the attack worked reliably, with key reinstallation witnessed and traffic being decrypted halfway. WPA3's new key management framework, however, made it resistant to KRACK, and key reinstallation was impossible under any of the tested conditions.

These deployments facilitated an explicit comparison of protocol-level protections between WPA3 and WPA2 under controlled experimental conditions, providing insight into how well these protocols will perform under realistic conditions against common wireless attack methods.

Experimental Work

Each attack scenario was performed under controlled radio frequency (RF) conditions to promote consistency and eliminate environmental variability. Traffic during experiments was captured via Wireshark and saved for later analysis as PCAP. The captured traffic was examined to measure three performance indicators: the rate of packet loss, client disconnection time (in seconds), and total success rate of an attack. These measures provided a quantitative basis for measuring different types of attack's impact against both WPA2 and WPA3 networks. The experimental results were later visualized to facilitate comparison and are illustrated below as Figure 2 and Table 1.

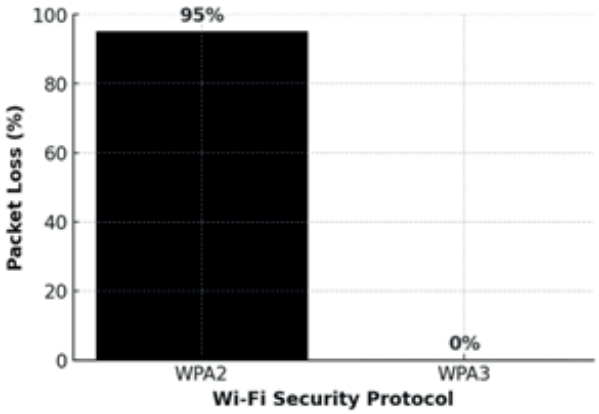

Figure 2(a). Impact of deauthentication DoS on WPA2 vs. WPA3

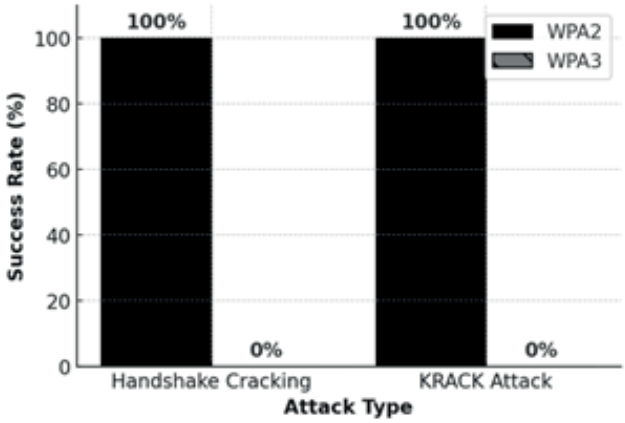

Figure 2(b). Handshake capture and KRACK attack results

Data analysis & Interpretation

In order to evaluate and contrast security performance between WPA2 and WPA3 protocols, a set of quantitative measures, i.e., attack success rate, average downtime, and packet loss ratio, were calculated, which were based on repeated experimental tests and are presented in Table 1. The results offer a relative perspective of how each protocol resists certain attack channels, which show stark differences in resistance and susceptibility under the same circumstances. WPA2 showed systematically high attack success rates with extensive service disruption under all cases, whereas WPA3 showed high resistance, especially against deauthentication and KRACK-based attacks.

Results and discussion

This section presents and analyzes the experimental results, comparing the performance of WPA2 and WPA3 under different attack scenarios. Results are structured into four key attack evaluations: deauthentication attack, handshake capture, KRACK attack, and overall comparative metrics.

This section introduces and interprets the results of the experimental comparison, showing differences between WPA3 and WPA2 under actual attack conditions. The results are organized around three major attack vectors—deauthentication, capturing of handshakes, and KRACK—and summarized comparison of protocols for all tested values.

WPA2 was found to be fully susceptible to deauthentication attacks. The client was successfully deauthenticated during 100% of test iterations through injection of forged 802.11 management frames, which takes advantage of WPA2-Personal networks' lack of protection for management frames. On average, disconnection happened at around 0.5 seconds post-attack, leading to a loss of packets at a rate almost as high as 90%, and reconnection at a rate of around 3 seconds. These findings reassert that WPA2 networks, by default, are still quite susceptible to this type of denial-of-service, as long as it is not running with optional protections like Protected Management Frames (PMF). Previous research will find that an estimate

of almost 94% of Wi-Fi networks worldwide still do not have PMF running, leaving them open to deauthentication-based service disruption.

In contrast, WPA3-Personal was fully proof against the same attack. During all tested experiments, the assailant was never successful at forcing disconnection of any client, and there was no recorded loss of packets or communication disruptions. The success is a direct result of WPA3's compulsory use of PMF, which validates management frames and ensures spoofed deauthentication packets don't reach or impact the client. The access point in a WPA3 setting simply ignores illegitimate frames, thus maintaining consistent service. These results strongly justify the significance of PMF, implemented as 802.11w, as a vital security component of contemporary wireless networks, and confirm WPA3's design goal of preventing legacy protocol vulnerabilities.

As shown by Figure 2(a), WPA2 networks experienced heavy packet loss through deauthentication attack, while WPA3 networks were fully secure. The contrast between them highlights the resilience of WPA3's inherent protection, specifically the compelled utilization of Protected Management Frames (PMF), which successfully suppresses forged deauthentication frames. While the WPA2 client kept being dislodged and suffered service loss, the WPA3 client had an uninterrupted and constant connection during all experiments.

A similar disparity was evident with regards to exposure via handshake. In WPA2-Personal networks, the default 4-way handshake is susceptible to interception and offline brute-force cracking. In tests, the handshake was successfully intercepted for all five attempts, and offline dictionary attack was successful at 100% with the target password being included in the pre-determined wordlist. The average reconnection time for clients was around 1.5 seconds. All these results authenticate WPA2's PSK-based authentication as being susceptible to offline attack, which does not involve an additional communication with the access point once a handshake is captured.

In contrast, WPA3-Personal employs the Simultaneous Authentication of Equals (SAE) protocol, specifically created to guard against such vulnerabilities. While SAE handshakes were successfully intercepted under all test runs, they never yielded the cryptographic material to be used for offline key derivation. Consequently, all efforts at cracking WPA3 handshakes via dictionary-based attack were unsuccessful. The reconnection latency was somewhat longer, at an average of 2.0 seconds, accounting for the increased complexity of the authentication round-trip. These results verify that WPA3 design successfully thwarts offline cracking attempts by requiring a live conversation for every password guess, thus dramatically enhancing the privacy of user credentials.

As evident in Figure 2(b), the experimental results show that WPA2 was fully compromised during offline attempts at cracking, but WPA3 was still secure under similar circumstances. The result supports the effectiveness of WPA3's Simultaneous Authentication of Equals (SAE) mechanism for thwarting offline

password retrieval. Given that WPA3 does not reveal adequate cryptographic data during the process of handshake, it essentially rules out key derivation without live access point interactivity.

Another crucial test scenario was Key Reinstallation Attack (KRACK), which hits a certain weakness of WPA2's 4-way handshake. The weakness lets an attacker manipulate handshake messages in a certain fashion that causes the victim device to reinstall an already-used encryption key. In all WPA2 test instances, the KRACK attack was successful. While the client stayed connected and disruption was not user-observable at first, reinstallation of the encryption keys happened, resulting in exposure to security risks. About 5% of packets were lost or temporarily stuck during the attack. More significantly, the attacker could decrypt parts of traversed traffic, and under certain circumstances, masquerade as the victim client. These results agree with previous research, which illustrated that WPA2's handshake design allows for replay-based manipulation of messages and exposes the session to reinstallation of keys.

By contrast, WPA3-Personal was completely resistant to KRACK in all of its tests. The attack didn't succeed once, with no packet loss, no alteration of the handshake, or impact upon network service being witnessed. The reason is that WPA3's redesigned process for establishing keys does not have specific protocol logic that KRACK targets. With redesigned key management and non-reuse of nonces, WPA3 effectively renders this class of attack useless. The results verify that WPA3 attempts to fix one of the most serious vulnerabilities of its predecessor and emphasize how crucial it is to have widespread adoption to achieve secure wireless communication for contemporary network infrastructures.

Overall comparative metrics

All experimental data collected throughout the study are summarized in Table 1 to facilitate direct comparison of WPA2 and WPA3 performance under all attack conditions. Table 1 shows average values computed for five independent runs for all attack types, including success rate, disconnect time, packet loss rate, and reconnection time. The attack success rate (R_s) was calculated based on Equation (1), which defined how many successful runs there were out of total runs and expressed as a percentage. The quantification provided a normalized estimation of how susceptible to individual attack vectors each protocol is.

$$R_s = \frac{N_{successful\ trials}}{N_{total\ trials}} \times 100\%$$

Table 1. Comparative outcomes for WPA2 vs. WPA3 under different attack scenarios

Attack Type	Success Rate (WPA2 vs. WPA3)	Avg. Disconnection Time (s)	Packet Loss (%)	Reconnection Time (s)
Deauth Attack	100% vs. 0%	0.5s vs. 0s	95% vs. 0%	3.0s vs. 0s

Handshake Capture	100% vs. 100%	0.5s vs. 1.0s	5% vs. 5%	1.5s vs. 2.0s
KRACK Attack	100% vs. 0%	0s vs. 0s	5% vs. 0%	0s vs. 0s

The comparative results demonstrate unequivocally that WPA3 far surpasses WPA2 as far as security resilience is concerned. All of those attacks which remained consistently successful against WPA2, including deauthentication flooding, offline cracking based on a single handshake, and KRACK, were unsuccessful against WPA3. For instance, deauthentication attack meant 95% packet loss and complete disconnection of the client for WPA2, while there was no disruption for WPA3 with the enforcement of Protected Management Frames (PMF).

WPA2 was also found to be heavily susceptible to credential compromise. During all WPA2 handshake capture tests, offline dictionary attack successfully recovered with a 100% recovery rate where the password was part of the wordlist. WPA3, nonetheless, was fully resistant to such attacks because, with the SAE handshake design, there is an active presence with the access point for every guess of a password, thus making offline cracking impossible.

Significantly, there is no meaningful performance overhead with the improved protections of WPA3. The average reconnection time difference between WPA2 and WPA3 was negligible—about 0.5 seconds—and there was no perceptible impact upon latency or throughput during tests. The results reinforce that WPA3 provides an effective upgrade to WPA2 security without compromising usability or performance efficiency, which again justifies mass adoption of the new protocol.

Conclusion

This study set out to identify the strengths and weaknesses of modern Wi-Fi security protocols through hands-on testing, and the findings clearly confirm the expected security gap between WPA2 and WPA3. WPA3-Personal delivered substantial improvements over WPA2 in real-world attack scenarios. In our experiments, WPA3's use of the Simultaneous Authentication of Equals (SAE) handshake and mandatory Protected Management Frames (PMF) effectively thwarted attacks that readily compromised WPA2 networks, including offline passphrase cracking and deauthentication-based disconnects. Notably, WPA3's improved handshake process also mitigated the KRACK key reinstallation vulnerability that severely affected WPA2. By contrast, WPA2-PSK — still the most widely deployed Wi-Fi security protocol — was consistently breached under these tests using well-known tools and techniques, highlighting how easily it can be compromised under real-world conditions. These results reinforce the conclusion that WPA2's legacy protections are insufficient against modern attack methods, whereas WPA3 offers a far more robust defense in practice.

Given these outcomes, we strongly recommend that both personal and enterprise environments migrate to WPA3 as the baseline security protocol. Home and small-office networks should be upgraded to WPA3-Personal to immediately benefit from its resilience against deauthentication attacks, handshake cracking, and

other common intrusions. In corporate and institutional settings, adopting WPA3-Enterprise (802.1X authentication, with its 192-bit cryptographic suite) is advised to protect sensitive data and communications. Overall, phasing out WPA2 in favor of WPA3 will significantly raise the security bar for wireless networks, reducing exposure to known exploits. Network administrators and users should treat WPA3 not just as an optional enhancement but as the default standard moving forward.

Finally, this work highlights several avenues for future research to further strengthen Wi-Fi security. First, comprehensive assessments of WPA3-Enterprise deployments (e.g., in 802.1X environments) are needed to verify that enterprise authentication mechanisms hold up against sophisticated attacks, as our study focused on personal networks. Second, investigation into side-channel and implementation-layer vulnerabilities in WPA3 devices is warranted – for example, early analyses uncovered flaws in the WPA3 Dragonfly handshake (the Dragonblood attacks) via timing side-channels and insecure transition modes, indicating that even a strong protocol can be undermined by poor implementations or backward-compatibility features. Third, as cryptographic technology advances, exploring the integration of post-quantum cryptographic algorithms into Wi-Fi authentication is an important forward-looking step to ensure long-term resistance against emerging threats. Addressing these gaps will help solidify the security of next-generation wireless networks and ensure that Wi-Fi remains secure as new vulnerabilities and attack techniques evolve.

References

Abdallah W. (2024) A physical layer security scheme for 6G wireless networks using post-quantum cryptography. Computer Communications, 218. — P. 176–187. (in English)

Banakh R., Nyemkova E., Justice C., Piskozub A., & Lakh Y. (2024) Data mining approach for evil twin attack identification in Wi-Fi networks. Data, 9(10), 119. (in English)

Baseri Y., Chouhan V., & Hafid A. (2024) Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Computers & Security. — P. 142. (in English)

Chatzoglou E., Kambourakis G., & Kolias C. (2021) Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset. — P. 34188–34205. (in English)

Chatzoglou E., Kambourakis G., & Kolias C. (2022) How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. Journal of Information Security and Applications. (in English)

De Almeida Braga D., Fouque P.-A., & Sabt, M. (2020) Dragonblood is still leaking: Practical cache-based side channel in the wild. In Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC 2020) – P. 291–303. (in English)

Gao D., Lin H., Li Z., Qian F., Chen Q.A., Qian Z., Liu W., Gong L., & Liu Y. (2021) A nationwide census on WiFi security threats: Prevalence, riskiness, and the economics. In Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (MobiCom '21). — P. 242–255. (in English)

Gebresilassie S. K., Rafferty J., Chen L., Cui Z., & Abu-Tair M. (2023) Transfer and CNN-based de-authentication (disassociation) DoS attack detection in IoT Wi-Fi networks. Electronics, 12(17). — P. 3731. (in English)

Gyamfi, E. & Jurcut A. (2022) Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors, 22(10). — P. 3824. (in English)

Halbouni A., Ong L.-Y., & Leow M.-C. (2023) Wireless security protocols WPA3: A systematic literature review. IEEE Access, 11. — P. 112438–112463. (in English)

Kazmi S.H. A., Hassan R., Qamar F., Nisar K., & Ibrahim A. (2023) Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry, 15(6). — P. 1147. (in English)

Kikissagbe B.R., & Adda M. (2023) Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. Electronics, 13(18). — P. 3601. (in English)

Kotb S.A., Hussein H., & Kim, H.-W. (2022) Security requirements and challenges of 6G technologies and applications. Sensors, 22(5). — P. 1969. (in English)

Lounis K., & Zulkernine M. (2019) Bad-token: Denial of service attacks on WPA3. In Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19), 15. ACM. (in English)

Lounis K., & Zulkernine M. (2020) WPA3 connection deprivation attacks. In Kallel S., Cuppens F., Cuppens-Boulahia N., & Kacem A.H. (Eds.), Risks and Security of Internet and Systems (CRiSIS 2019, LNCS 12026). — P. 164–176). (in English)

Marais S., Coetzee M., & Blauw F. F. (2021) Simultaneous deauthentication of equals attack. In Wang G., Chen B., Li W., Di Pietro R., Yan X., & Han H. (Eds.), Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2020, LNCS 12383). — P. 545–556. (in English)

Nguyen V.-L., Lin P.-C., Cheng B.-C., Hwang R.-H., & Lin Y.D. (2022) Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials, 24(4). — P. 2255–2291. (in English)

Örs F. K., Aydın M., Boğatarkan A., & Levi A. (2021) Scalable Wi-Fi intrusion detection for IoT systems. In Proceedings of the 11th IFIP International Conference on New Technologies, Mobility and Security. — P. 1–6. (in English)

Rathod T., Jadav N. K., Alshehri M.D., Tanwar S., Sharma R., Felseghi R.-A., & Raboaca M.S. (2022) Blockchain for future wireless networks: A decade survey. Sensors, 22(11). (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). 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.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 25.09.2025.
Формат 60x881/8. Бумага офсетная.
Печать –ризограф. 20,0 п.л. Заказ 3.

Национальная академия наук РК
050000, Алматы, ул. Кунаева 132