ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Базарбаев Ахмет Русланұлы

«Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру»

ДИПЛОМДЫҚ ЖҰМЫС

6B06201 – «Телекоммуникация» білім беру бағдарламасы

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
ЭТжҒТ кафедра меңгерушісі
техн.ғыл.канд.
_____Е.Таштай
«30» 05 2025 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру»

6В06201 – Телекоммуникация

Орындаған: Базарбаев А.Р

Пікір беруші
Алматы энергетика және
байланыс университеты
профессоры. т.ғ.к.,
Чежимбаева К.С_____
«30» 05 2025 ж.

Ғылыми жетекші
ҚазҰТЗУ, Доктор PhD,
ЭТжҒТ кафедрасының
қауымдастырылған профессор
_____ Хабай А
«26» 05 2025 ж.

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыш технологиялар кафедрасы

6В06201 –Телекоммуникация

БЕКІТЕМІН
ЭТжҒТ Кафедра меңгерушісі
_____Е.Таштай
«_03_» _02_____ 2024ж

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы Базарбаев Ахмет Русланұлы

Тақырыбы «Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру»

Университет ректорының «29» қаңтар 2025 ж. №26 бұйрығымен бекітілген.

Аяқталған жұмысты тапсыру мерзімі «30» сәуір 2025 ж.

Дипломдық жұмысқа арналған бастапқы деректер: 1) O-RAN (Open Radio Access Network) архитектурасының ерекшеліктері мен қауіпсіздік мәселелері; 2) жасанды интеллект (AI) және машиналық оқыту (ML) әдістерін қолдану арқылы желі қауіпсіздігін қамтамасыз ету тәсілдері; 3) O-RAN желісінің осалдықтарына шолу және кибершабуыл түрлерін классификациялау;

Дипломдық жұмыста қарастырылатын мәселелер тізімі: 1) Жасанды интеллект негізінде шабуылдарды анықтау және алдын алу механизмдерінің алгоритмін әзірлеу; 2) AI және ML құралдарын пайдаланып O-RAN желісінің қауіпсіздік көрсеткіштерін бағалау; 3) Әзірленген әдістерді симуляциялау және нәтижелерді талдау; 4) Жасанды интеллект шешімдерін O-RAN желісіне интеграциялау кезінде туындайтын қиындықтар мен қол жеткізген нәтижелерді ұсыну.

Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):

Ұсынылатын негізгі әдебиеттер: 1) O-RAN Alliance. "O-RAN Architecture and Specification Documents." – 2023. 2) Bangerter B., Talwar S., Arefi R., et al. "Networks 5G and beyond: Security challenges and solutions" //IEEE Communications Magazine. – 2023. 3) Zhao H., Wu H., Li Y. "AI-powered cybersecurity for O-RAN networks" //Sensors and Communications. – 2022. 4) Zhang Y., Liu J., Zhang X. "Deep learning applications in secure open RAN networks" //Springer, 2024.

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
O-RAN желісінің осалдықтарына шолу және кибершабуыл түрлерін классификациялау, жасанды интеллект және машиналық оқыту әдістерін қолдану арқылы желі қауіпсіздігін қамтамасыз ету тәсілдеріне шолу	04.01.2025-01.02.2025	Орындалды
AI және ML құралдарын пайдаланып O-RAN желісінің қауіпсіздік көрсеткіштерін бағалау	01.02.2025 - 01.03.2025	Орындалды
Әзірленген әдістерді симуляциялау және нәтижелерді талдау	01.03.2025-30.05.2025	Орындалды

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған **қолтаңбалары**

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылымидәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Хабай А, PhD., ЭТжҒТ қауымдастырылған профессор	26.05.25	
Теориялық ақпарат	Хабай А., PhD., ЭТжҒТ қауымдастырылған профессор	26.05.25	
Норма бақылау	Досбаев Ж.М. ЭТжҒТ, PhD., аға оқытушысы	20.05.25	

Ғылыми жетекшісі Хабай А

Тапсырманы орындауға алған білім алушы Базарбаев А.

«30» 05 2025 ж.

АҢДАТПА

Бұл дипломдық жұмыс O-RAN желісінің қауіпсіздігін арттыру мақсатында жасанды интеллектке негізделген қорғаныс жүйесін құруға бағытталған. Зерттеу барысында желілік шабуылдардың түрлері (DDoS, SSH Brute Force) және оларды анықтау әдістері талданды. Wireshark арқылы 2024 жылғы трафик үлгісі зерттеліп, Firebase платформасында нақты уақыт режимінде визуализация жасалды. Жасалған ORAN Defender жүйесі шабуылдарды анықтап, автоматты түрде әкімшіге хабар жіберді. ЖИ модельдері жүйенің тиімділігін арттыруда маңызды рөл атқарды. Жүйе болашақта Zero-Day шабуылдарын тануға және шынайы желілерге енгізуге бейімделе алады.

АННОТАЦИЯ

В выпускной работе реализована система защиты сети O-RAN с использованием искусственного интеллекта. Цель – выявление киберугроз (DDoS, SSH Brute Force) в реальном времени. Анализ трафика осуществлялся с помощью Wireshark на основе данных 2024 года, визуализация – через Firebase. Разработанная система ORAN Defender успешно обнаруживала аномалии и уведомляла администратора. Алгоритмы ИИ повысили точность детектирования. Решение перспективно для внедрения в реальные телеком-сети и дальнейшего улучшения.

ANNOTATION

This thesis presents an AI-based security system for O-RAN networks. The goal is real-time detection of cyberattacks such as DDoS and SSH Brute Force. Using Wireshark and Firebase, 2024 traffic data was analyzed and visualized. The developed ORAN Defender system detected anomalies and notified the admin automatically. AI models improved detection accuracy. The system shows potential for future deployment and expansion to detect Zero-Day threats

МАЗМҰНЫ

КІРІСПЕ

Қазіргі әлем экономиканың, әлеуметтік инфрақұрылымның және адамдардың күнделікті өмірінің дамуына негіз болатын цифрлық технологиялардың белсенді енгізілуін бастан кешуде. Деректер көлемінің қарқынды өсуі және қосылған құрылғылар санының артуы жағдайында телекоммуникациялық желілер ақпараттың үздіксіз алмасуын қамтамасыз етуде шешуші рөл атқарады. Бесінші буын желілеріне (5G) және олардың эволюциясына, соның ішінде ашық радио қол жетімділік архитектурасына көшуге баса назар аударылады. АРАЖ - бұл операторларға ашық интерфейстерді, бағдарламалық жасақтамамен анықталған компоненттерді және бұлтты технологияларды қолдану арқылы икемді, масштабталатын және үнемді желілерді құруға мүмкіндік беретін инновациялық тұжырымдама.

Алайда, АРАЖ - ның таратылған табиғаты және оның ашық стандарттарға тәуелділігі киберқауіпсіздікке жаңа қиындықтар туғызады. Қорғалмаған интерфейстер, үлестірілген компоненттерді басқарудың қиындығы және бағдарламалық жасақтамаға шабуыл жасаудың жоғары ықтималдығы сияқты осалдықтар АРАЖ желілерін зиянкестер үшін тартымды нысанаға айналдырады. Check Point Research (2023) мәліметтері бойынша, өткен жылы телекоммуникациялық желілердегі кибершабуылдар саны 38%-ға өсті, бұл АРАЖ - дағы қауіпсіздік мәселесінің өзектілігін көрсетеді. Деректерді шифрлау, IDS/IPS жүйелері (Жүйеге қол салу/Болдырмау жүйелері) және құрылғылардың аутентификациясы сияқты дәстүрлі қорғаныс әдістері әрдайым заманауи қауіптерге тиімді қарсы тұра бермейді, әсіресе DDoS, "ортадағы адам" және RIC (Ақылды радиобасқару контроллері) компасы сияқты күрделі шабуылдардың көбеюі жағдайында.

Бұл мәселені шешудің перспективалық тәсілдерінің бірі-жасанды интеллект технологияларын қолдану. ЖИ нақты уақыттағы деректердің үлкен көлемін талдауға, ауытқуларды анықтауға, шабуылдарды болжауға және қорғаныс процестерін автоматтандыруға мүмкіндік береді. Мысалы, IBM Security (2023) зерттеуі ЖИ қолдану шабуылдарды анықтау уақытын 25% - ға қысқартуға және оқиғалардың зақымдануын 30% - ға азайтуға мүмкіндік беретінін көрсетті. Бұл ЖИ-ді АРАЖ желілеріндегі қауіпсіздікті жақсартудың қуатты құралына айналдырады.

Бұл жұмыстың мақсаты жасанды интеллектті пайдалана отырып, O-RAN желілері үшін қауіпсіздік тетіктерін әзірлеу және енгізу болып табылады. Мақсатқа жету үшін келесі міндеттерді шешу қажет:

1) АРАЖ желілеріндегі ағымдағы қауіптер мен қорғаныс әдістерін талдау.

2) Кибершабуылдарды анықтау және алдын алу үшін жасанды интеллектті қолдану мүмкіндіктерін зерттеу.

3) АРАЖ желілерінің қауіпсіздігін жақсарту үшін ЖИ негізіндегі модель немесе алгоритм жасау.

4) Эксперименттік мәліметтер негізінде ұсынылған шешімнің тиімділігін бағалау.

Зерттеу нысаны – АРАЖ архитектурасындағы қауіпсіздік механизмдері және оларды жасанды интеллект арқылы жетілдіру.

Жұмыстың әдіснамалық негізі:

АРАЖ желілерінің қауіпсіздігі бойынша ғылыми әдебиеттер мен нормативтік құжаттарды талдау.

Машиналық оқыту және деректерді талдау әдістерін қолдана отырып модельдеу және эксперименттік зерттеулер.

Шешімдерді әзірлеу және сынау үшін заманауи құралдар мен платформаларды қолдану.

Жұмыстың ғылыми жаңалығы-жасанды интеллект технологияларын қолдана отырып, АРАЖ желілерін қорғаудың жаңа тәсілдерін ұсыну. Ұсынылған модель шабуылдарды анықтау және алдын алу процестерін автоматтандыру, сондай - ақ жаңа қауіптерге бейімделу арқылы қауіпсіздік деңгейін арттыруға мүмкіндік береді.

Зерттеудің практикалық маңыздылығы - олардың кибершабуылдарға төзімділігін арттыру үшін нақты АРАЖ желілерінде әзірленген шешімдерді қолдану мүмкіндігі. Жұмыс нәтижелерін байланыс операторлары мен телекоммуникациялық жабдықты әзірлеушілер пайдалана алады.

Жұмыс құрылымы үш тараудан тұрады:

1. АРАЖ желілерінің қауіпсіздігінің теориялық негіздері: архитектураны, қауіптерді және қолданыстағы қорғаныс әдістерін талдау.

2. Жасанды интеллект негізінде қауіпсіздік тетіктерін әзірлеу: модельді жобалау, алгоритмдер мен құралдарды таңдау.

3. Эксперименттік бөлім: әзірленген шешімді сынау және оның тиімділігін бағалау.

Осылайша, бұл жұмыс озық жасанды интеллект технологияларын пайдалана отырып, АРАЖ желілерінің қауіпсіздігін қамтамасыз етудің өзекті мәселесін шешуге бағытталған.

1 АРАЖ желілерінің қауіпсіздігінің теориялық негіздері

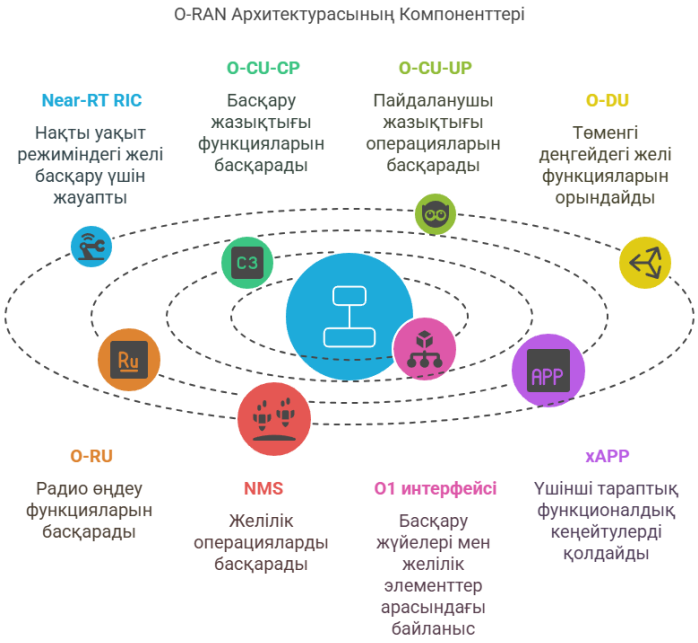
1.1 АРАЖ технологиясына шолу

Ашық Радио Ақпарат Желісі (АРАЖ) технологиясы радио қол жеткізу желілерін ұйымдастырудың заманауи тәсілі болып табылады. Дәстүрлі жүйелерден айырмашылығы, онда барлық жабдықтар мен бағдарламалық жасақтаманы бір сатушы ұсынса, АРАЖ ашық интерфейстерге, стандартталған хаттамаларға және бағдарламалық жасақтамамен анықталған компоненттерге негізделеді. Осылайша, тасымалдаушылар әртүрлі өндірушілерден құрылғылар мен бағдарламаларды таңдауға мүмкіндік алады, нәтижесінде, нақты жеткізушілерге тәуелділік айтарлықтай төмендейді.

Сонымен қатар, АРАЖ идеясының негізінде бәсекеге қабілетті және инновациялық орта құруға деген ұмтылыс жатыр. Бұл ғана емес, мұндай тәсіл желілерді орналастыру шығындарын азайтуға көмектеседі және, сонымен бірге, жаңа технологияларды енгізу процесін жеделдетеді. Одан бөлек, операторлар байланыс сапасын жақсарту және ресурстарды тиімдірек бөлу арқылы өзгеретін талаптарға тез бейімделу мүмкіндігіне ие болады.

1.1.1 АРАЖ жұмысының архитектурасы мен принциптері

Суретте АРАЖ архитектурасына жалпы шолу, оның ішінде радио мен басқарудың функционалды аймақтарына бөлінген негізгі компоненттер мен интерфейстер бар.



1.1-сурет – АРАЖ архитектурасына шолу

АРАЖ архитектурасы компоненттер арасындағы икемділік пен өзара әрекеттесуді қамтамасыз ететін ашық интерфейстер мен стандартталған протоколдарды қолдануға негізделген. Жүйеде орталық орынды радиобайланыс модульдері алады: Near-RT RIC (нақты уақыттағы радио барлау контроллері), ол қысқа мерзімді оңтайландыруға, ресурстарды динамикалық бөлуге және шешім қабылдауға жауап береді; O-CU-CP (басқару жазықтығының орталық блогы), радиоресурстар мен ұтқырлықты басқару функцияларын орындайды; o-cu-up (пайдаланушы деңгейіндегі орталық блок), желі мен пайдаланушы жабдықтары арасында деректерді беруді қамтамасыз етеді; сигналдар мен радиоресурстарды физикалық өңдеу функцияларын орындайтын O-DU (үлестірілген модуль); және O-Радиожиілік сигналдарын өңдеуге және оларды түрлендіруге жауап беретін RU (радиоқұрылғы). Бүкіл жүйені басқару жеке элементтер арқылы жүзеге асырылады: желіні жалпы орнатуға, өмірлік циклды басқаруға және оркестрлеуге жауап беретін Қызметтерді басқару және оркестр платформасы және ұзақ мерзімді оңтайландыру мен саясатты басқаруды қамтамасыз ететін RT RIC (нақты уақыттағы радио барлау контроллері) емес. Компоненттер басқару платформасы мен желілік компоненттер арасындағы байланыс үшін O1 сияқты интерфейстер, сондай-ақ қосымша функцияларды қамтамасыз ететін кеңейтілген O1* интерфейсі арқылы біріктірілген. Осы элементтердің барлығының өзара әрекеттесуі АРАЖ жүйесінің жоғары бейімделгіш және тиімді болуына мүмкіндік береді.

1.1.2 Дәстүрлі Радио ақпараттық желілерімен салыстырғанда артықшылықтары мен ерекшеліктері

АРАЖ архитектурасы – дәстүрлі жабық РАЖ - дан ерекшеленетін мобильді желілерді ұйымдастырудың заманауи тәсілі.

1.2-сурет - АРАЖ артықшылықтары

Оның басты артықшылығы – ашықтық, яғни дәстүрлі шешімдердегі (Ericsson, Nokia, Huawei) бір өндірушіге тәуелділіктен арылып, ашық интерфейстер мен стандарттар (E2, F1) арқылы әртүрлі жеткізушілердің құрылғыларын біріктіруге мүмкіндік береді. Сонымен қатар, АРАЖ модульдік құрылымға негізделген, онда негізгі компоненттер – Near-RT RIC (нақты уақыттағы басқару және оңтайландыру), O-CU (орталық басқару блогы), O-DU (үлестірілген модуль) және O-RU (радио құрылғы) өзара байланысып, бүкіл жүйені толық жаңартпай-ақ жеке бөліктерді ауыстыруға немесе жаңартуға жағдай жасайды. Бұдан бөлек, АРАЖ жасанды интеллект пен машиналық оқытуды (Near-RT RIC және Non-RT RIC арқылы) қолдану арқылы ресурстарды басқаруды автоматтандырып, желінің жүктемесін болжауға және нақты уақыттағы өзгерістерге икемделуге мүмкіндік береді. Сондай-ақ, коммерциялық "ақ" жабдықты (Дайын коммерциялық өнімдер) және ашық бастапқы бағдарламалық жасақтаманы пайдалану құрылыс және пайдалану шығындарын (Капиталдық шығындар/Операциялық шығындар) айтарлықтай төмендетеді, ал виртуализация мен бұлттық технологияларды қолдауы ЖФР (Желілік функцияларды виртуализациялау) негізінде желіні икемді орналастыруға және масштабтауға жағдай жасайды. Бұған қоса, АРАЖ архитектурасы төмен кідірісті, кеңейтілген қамтуды және жоғары өнімділікті қамтамасыз етіп, 5G мен болашақ технологияларға бейімделген. Сонымен қатар, АРАЖ экожүйесі операторларға xAPPs және rAPPs қолданбалары арқылы IoT, жеке желілер сияқты бірегей қызметтерді әзірлеуге мүмкіндік беріп, жаңа бизнес үлгілерін дамытуға ықпал етеді. Ақырында, ашық стандарттардың қолданылуы мен орталықтандырылған басқарудың болуы желінің қауіпсіздігін күшейтіп, инфрақұрылымға деген сенімділікті арттырады. Осылайша, АРАЖ технологиясы үнемді, инновациялық және икемді жаңа буын желілерін дамытуды қалайтын операторлар үшін оңтайлы шешім болып табылады.

1.1.3 O-CU, O-DU, O-RU негізгі компоненттері

O-CU (Ашық орталық бірлік) PDCP (Деректер пакеттерін біріктіру хаттамасы) сияқты байланыс протоколдарының жоғарғы деңгейлерін өңдеуге жауапты және пакет деңгейіндегі деректерді өңдеу, қосылымдар мен деректерді басқаруды ұйымдастыру, сондай-ақ handover сияқты ұтқырлық функцияларын қолдау секілді негізгі міндеттерді атқарады. Бұл модуль әдетте бұлттық инфрақұрылымда немесе деректер орталығында орналастырылып, басқарудың икемділігін және желінің жұмысын оңтайландыруды қамтамасыз етеді. Сонымен қатар, ол стандартты серверлерде (Дайын коммерциялық өнімдер) жүзеге асырылып, F1 интерфейсі арқылы Ашық таралған бірлікпен, ал Ng интерфейсі арқылы желі ядросымен өзара әрекеттеседі, бұл ресурстарды басқаруды жақсартып, Бағдарламалық жасақтамамен анықталған желі және желі функцияларын виртуалдау сияқты бағдарламалық жасақтамамен анықталған шешімдерді біріктіруге мүмкіндік береді.

O-DU (Ашық таралған бірлік) байланыс протоколының орташа деңгейлерін өңдеу функцияларын орындай отырып, RLC (Радио байланыс басқаруы), MAC (Ортаға қатынау басқаруы) және белгілі бір физикалық деңгей (ФД) тапсырмаларын басқарады. Ол радиоресурстарды реттеп, дабылды өңдейді және Ашық радио блогымен физикалық деңгейде тапсырмаларды орындау үшін өзара әрекеттеседі. Базалық станцияларға (Шеткі есептеу) немесе орталық түйіндерге жақын орналасқан бұл компонент жоғары өнімді аппараттық платформаларда жүзеге асырылып, Ашық орталық блокпен F1 интерфейсі, ал Ашық радио блогымен ECPRI (жақсартылған ортақ радиоинтерфейс) немесе ROE (Ethernet арқылы радио) интерфейстері арқылы байланысады, осылайша операторларға жабдықты таңдауда және жүктемені бөлуде икемділік береді.

O-RU (Ашық радио блогы) байланыс хаттамаларының төменгі деңгейлерін өңдеуге жауапты болып, оның функционалдығы сандық сигналдарды аналогтық және кері түрлендіру, радио сигналдарды модуляциялау және демодуляциялау, сондай-ақ антеннаны басқару (мысалы, Көп кірісті-көп шығысты технология және Сәулелерді бағыттау) секілді міндеттерді қамтиды. Бұл модуль базалық станцияларға немесе мұнараларға жақын орналастырылып, радио жабдықтарына тікелей қосылу арқылы ең аз кідірісті қамтамасыз етеді. Ашық радио блогы ашық таратылған блокқа жақсартылған ортақ радиоинтерфейс немесе ROE интерфейсі, ал антенналарға радио жиілігі интерфейстері арқылы қосылып, жоғары өнімділік пен әртүрлі жиілік диапазондарында тиімді жұмыс істеу қабілетін қамтамасыз етеді.

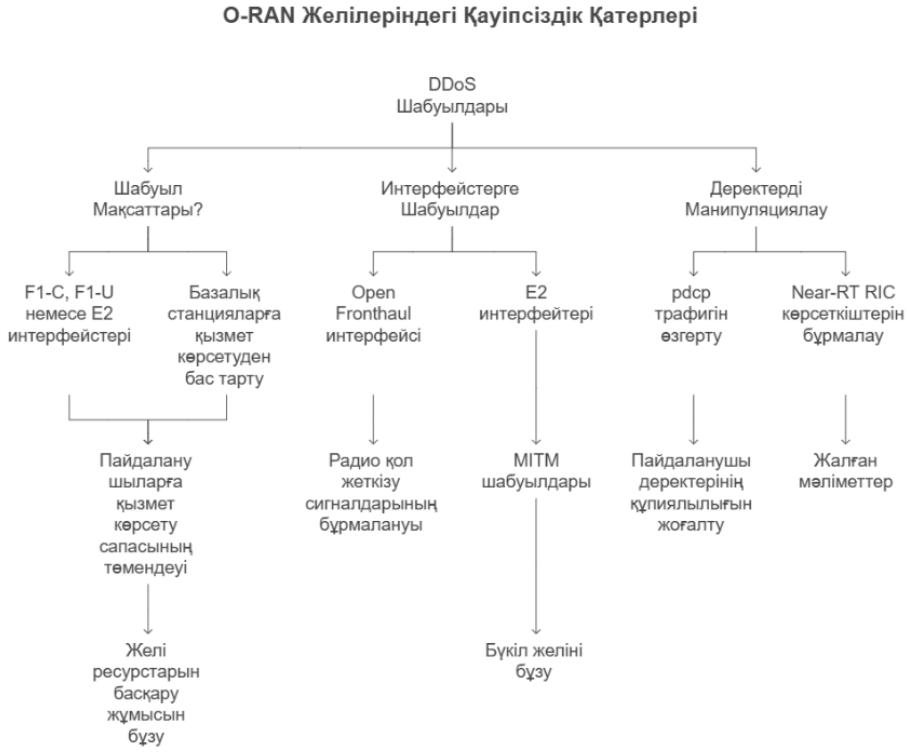
1.3-сурет – АРАЖ архитектурасының негізгі компоненттері

1.2 АРАЖ желілеріндегі қауіпсіздік қатерлерін талдау

АРАЖ — әртүрлі өндірушілердің аппараттық және бағдарламалық жасақтамасының үйлесімділігін қамтамасыз ететін ашық мобильді желі архитектурасы. Мұндай икемділік пен орталықтандырылмаған құрылым бірқатар артықшылықтармен қатар, жаңа қауіп-қатерлерді де тудырады, әсіресе қауіпсіздікке қатысты. Негізгі мәселелердің қатарында интерфейстер мен протоколдардағы осалдықтар, ашық интеграция нүктелері арқылы рұқсатсыз кіру мүмкіндігі, таратылған архитектураны басқарудың күрделілігі және оның тұтастығын қамтамасыз ету қажеттілігі бар. Сонымен қатар, жүйенің қауіпсіздігі әртүрлі сатушылардан қолданылатын компоненттердің әркелкілігімен қиындайды, бұл әлсіз жерлерді анықтау мен жою үшін үйлестірілген күш-жігерді талап етеді.

1.2.1 DDOS (Таралған сервер тоқтату шабуылы) шабуылдары, интерфейс шабуылдары, деректерді манипуляциялау

ТСТШ желі ресурстарын немесе оның компоненттерін шамадан тыс жүктеуге бағытталған, бұл қызмет көрсетуден бас тартуға әкеледі. Бұл шабуылдар АРАЖ архитектурасына үлкен қауіп төндіреді, мұнда таратылған құрылым мен көптеген қосылған құрылғылар қосымша осалдықтар тудырады.



1.4-сурет – АРАЖ Желілеріндегі қауіпсіздік қатерлері

Мұндай шабуылдардың негізгі мақсаттарына F1-C, F1-U және E2 сияқты желілік компоненттер арасындағы интерфейстердің шамадан тыс жүктелуі, сондай-ақ базалық станциялардың (Ашық радио блогы және ашық таратылған блок) және тірек желісінің элементтерінің істен шығуы жатады. Мұның салдары пайдаланушыларға қызмет көрсету сапасының төмендеуінен, базалық станциялармен байланыстың жоғалуынан және желі ресурстарын басқарудың бұзылуынан көрінуі мүмкін. АРАЖ контекстінде мұндай шабуылдар әсіресе қауіпті, өйткені орталықтандырылмаған жүйе қауіптерді уақтылы анықтау мен бейтараптандыруды қиындатады. ТСТШ шабуылдары интерфейстер мен протоколдар деңгейіндегі қауіпсіздікті әлсірету арқылы көптеген компоненттер арасындағы өзара әрекеттесуді қиындатуы мүмкін, бұл аппараттық және бағдарламалық жасақтама өндірушілері арасында күшейтілген қорғаныс пен үйлестіру шараларын қажет етеді.

АРАЖ архитектурасындағы интерфейстерге жасалған шабуылдар желінің қауіпсіздігіне үлкен қауіп төндіреді, өйткені Open Fronthaul(Ашық алдыңғы байланыс), E2, F1-C және F1-U сияқты нүктелер осалдықтың маңызды аймақтары болып табылады. Шабуылдардың кең таралған әдістерінің ішінде радио қол жеткізу сигналдарының бұрмалануына әкелетін Open Fronthaul (Басқару блогы - пайдаланушы жазықтығы) интерфейсіндегі деректердің өзгеруін атап өтуге болады; шабуылдаушылар деректерді ұстап, өзгертетін E2 интерфейстеріндегі MITM шабуылдары (Аралықтағы шабуылшы); және басқару интерфейстеріне шабуылдар (Басқару жазықтығы), бұл желіні басқаруға рұқсатсыз қол жеткізуге мүмкіндік береді. Мұндай шабуылдардың салдары радио қол жеткізу құрылғылары арасындағы синхрондаудың бұзылуын, басқару деректерін ұстап қалуды және өзгертуді, сондай-ақ интерфейстердің бірінің осалдығына байланысты бүкіл желіні бұзуды қамтуы мүмкін, бұл АРАЖ дамуы контекстінде осы компоненттерді қорғауды басымдыққа айналдырады.

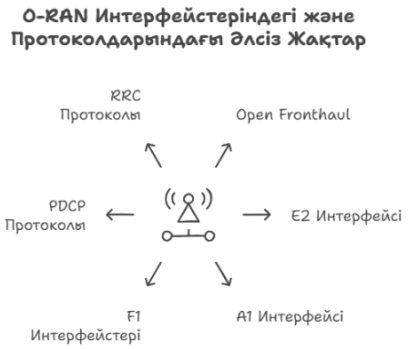
Деректерді манипуляциялау пайдаланушы деректеріне және басқару деректеріне әсер ететін қауіп болып табылады. Мұндай манипуляциялардың мысалдарына деректер тұтастығын бұзатын ПДБП (Пакеттік деректерді біріктіру протоколы) трафигінің өзгеруі жатады; желіні оңтайландыру туралы дұрыс емес шешімдерге әкелетін Near-RT RIC-ге(Жақын реалды уақыттағы радио интеллектуалды контроллер) жіберілген көрсеткіштерді бұрмалау; және құпия Пайдаланушы ақпаратының немесе желі конфигурациясының ағып кетуіне ықпал ететін қорғалмаған интерфейстер арқылы деректерді ұрлау. Мұндай әрекеттердің салдары пайдаланушы деректерінің құпиялылығын жоғалтуды, жалған деректерге байланысты желінің бұзылуын және тасымалдаушылардың қаржылық және беделдік шығындарын қамтиды. Мысалы, 2021 жылғы Нақты жағдай F1-C қорғалмаған интерфейсі арқылы шабуылдаушылар 100 000-нан астам пайдаланушының деректеріне, соның ішінде олардың орналасқан жері мен қоңырау тарихына қалай қол жеткізе алатынын көрсетті, бұл АРАЖ архитектурасында деректер мен интерфейстерді қорғауды күшейту қажеттілігін көрсетеді.

1.2.2 АРАЖ архитектурасының ерекшеліктері және оның қауіпсіздікке әсері

Таратылған АРАЖ архитектурасы желі қауіпсіздігіне айтарлықтай әсер ететін бірқатар ерекше мүмкіндіктерге ие, өйткені көптеген компоненттер (O-RU, O-DU, O-CU, near-RT RIC, non-RT RIC) және ашық интерфейстер (Open Fronthaul, E2, F1-C, F1-U) арқылы кіру нүктелерінің көбеюі желіні осал етеді, бір элементтегі осалдық каскадты әсерлерді тудыруы мүмкін, ал әртүрлі өндірушілер қолданатын жабдықтар мен бағдарламалық жасақтаманың үйлесімсіздігі қауіпсіздікті стандарттауды қиындатып, осалдық қаупін арттырады, сонымен қатар Near-RT RIC және non-RT RIC сияқты компоненттерді орналастыруға арналған бұлттық технологияларға тәуелділік инфрақұрылымға шабуылдар мен рұқсат етілмеген қол жетімділікке байланысты қауіптерді арттырады, таратылған желіні бақылау мен басқарудың қиындығы аномалияларды уақтылы анықтауды қиындатып, шабуылдарды дер кезінде анықтамау қаупін арттырады, интерфейстердің ашықтығы MITM (Аралықтағы шабуылшы) типті шабуылдар мен деректерді ауыстыруды жеңілдетіп, ал әртүрлі деңгейлерде таратылған деректерді өңдеу ақпараттың бұзылу ықтималдығын арттырады, сонымен қатар O-RU сияқты қашықтан орналастырылған жабдыққа физикалық қол жетімділік желіні бақылауды жоғалтуға, зиянды бағдарламалық жасақтаманың енгізілуіне және жалпы қауіпсіздіктің әлсіреуіне әкелуі мүмкін, сондықтан АРАЖ архитектурасындағы қауіпсіздік қатерлерін азайту үшін қорғаныс шараларын мұқият қарастыру қажет.

1.2.3 Интерфейстер мен протоколдардағы әлсіз жақтар

Интерфейстердің әлсіз тұстарының ішінде құрылғылардың синхрондауын бұзу және деректердің бұрмалануы ерекшеленеді: Open Fronthaul MITM (Аралықтағы шабуылшы) шабуылдарына және API(Қолданбалық программалау интерфейсі) арқылы манипуляцияларға осал, E2 құпия деректердің ағып кетуіне және зиянды кодтың енгізілуіне мүмкіндік береді.



1.5-сурет – АРАЖ интерфейстеріндегі және протоколдарындағы әлсіз жақтар

A1 зиянды әсерлерге ұшырайды, ал F1-C және F1-U интерфейстері пайдаланушылардың деректерін ұстап қалу қаупіне ұшырайды, бұл IPSec (Интернет протоколін қауіпсіздікке алу) конфигурациясына байланысты болуы мүмкін, сонымен қатар PDCP (Пакеттік деректерді біріктіру протоколы) деректердің тұтастығы мен құпиялылығын қорғаудың жеткіліксіздігінен зардап шегуі мүмкін, ал RRC (Радиоресурстарды басқару) жүйелік ақпаратты ұстап қалуға және қызмет көрсетуден бас тарту шабуылдарына осал, IPSec қорғауда маңызды рөл атқарғанымен, кілттермен алмасу шабуылдарына ұшырауы мүмкін, жалпы осалдықтар қашықтағы жабдыққа физикалық қол жетімділікті қамтиды, бұл зиянды бағдарламаларды енгізу қаупін арттырады, әр түрлі өндірушілердің шешімдерінің үйлесімсіздігі "нөлдік күн" осалдығының ықтималдығын жоғарылатады, ал бұлтқа тәуелділік виртуалды машиналар мен гипервизорларға шабуыл жасау қаупін тудырады, сондықтан АРАЖ желілеріндегі интерфейстер мен протоколдарды қорғау үшін қауіпсіздік шараларын күшейту міндетті.

1.3 АРАЖ-да қауіпсіздікті қамтамасыз етудің заманауи әдістері

Деректерді шифрлау — бұл АРАЖ ішіндегі ақпаратты қорғаудың негізгі әдістерінің бірі. Ол желінің әртүрлі деңгейлерінде деректердің ұсталуына, өзгертілуіне немесе рұқсатсыз кіруіне жол бермейді. Сонымен қатар, пайдаланушы деректерін шифрлау және RRC хабарламаларының тұтастығын қорғау үшін PDCP, F1-C және F1-U интерфейстеріндегі трафиктің құпиялылығы мен тұтастығын қамтамасыз ету үшін IPSec сияқты протоколдар қолданылады. Бұған қоса, пайдаланушы жазықтығы (U-plane), сигнал жазықтығы (C-plane) және басқару деңгейі (M-plane) қамтылады. Әрі қарай, басқару деңгейінде әкімшілік трафикті қорғау үшін TLS (Тасымалдау қабатының қорғанысы)/SSH (Қауіпсіз қабықша) пайдаланылады. Жалпы, шифрлаудың негізгі мақсаттарына құпиялылықты сақтау, деректердің тұтастығын қамтамасыз ету және ойнату шабуылдарынан қорғау кіреді.

Шифрлау көптеген артықшылықтарға ие. Біріншіден, ол деректердің ұстап қалудан қорғалуын қамтамасыз етеді. Екіншіден, ақпараттың тұтастығын сақтауға көмектеседі. Үшіншіден, сәтті шабуылдардың қаупін азайтады. Дегенмен, бұл әдістің кейбір шектеулері бар. Атап айтқанда, ол айтарлықтай есептеу ресурстарын қажет етеді. Сонымен қатар, оны іске асыру барысында кателіктер орын алуы мүмкін, бұл жүйенің осалдығын арттырады. Бұдан бөлек, АРАЖ архитектурасындағы кілттерді басқару күрделі тапсырмалардың бірі болып табылады.

Сондай-ақ, АРАЖ желілеріндегі қауіпсіздікті қамтамасыз етудің тағы бір маңызды аспектісі — аутентификация және авторизация. Бұл механизмдер пайдаланушылардың, құрылғылардың және қолданбалардың түпнұсқалығын тексеруді, сондай-ақ желі ресурстарына қол жеткізуді басқаруды қамтамасыз етеді. Мысалы, аутентификация SIM (Тіркелушіні анықтайтын модуль) және

eSIM (Енгізілген тіркелушіні анықтайтын модуль) карталарын, X.509 (Сертификаттардың стандарттық форматы) сандық сертификаттарын, 5G-AKA (5G аутентификациясы мен кілт келісімі) протоколын және API (Қолданбалық программалау интерфейсі) кілттерін қолданады. Сонымен қатар, авторизация рөлдерді бөлу үшін Рөлге негізделген қатынауды басқару (RBAC), Қолданбалық программалау интерфейсін қорғау үшін Ашық авторизациялау протоколы 2.0 және сезімтал ақпарат пен компоненттерге қол жеткізуді шектеу үшін қауіпсіздік саясатын қамтиды. Осылайша, аутентификация және авторизация рұқсатсыз кіруден қорғауды қамтамасыз етіп, жалған құрылғыларды енгізу сияқты шабуыл қаупін азайтады.

Дегенмен, бұл әдістерді енгізу барысында белгілі бір қиындықтар туындайды. Біріншіден, әртүрлі жабдық өндірушілері арасындағы үйлестіру мәселелері кездесуі мүмкін. Екіншіден, кілт алмасу механизмдері осалдықтарға ұшырауы ықтимал. Үшіншіден, бұлттық инфрақұрылымға байланысты қауіптер бар. Сол себепті, бұл механизмдерді үнемі жетілдіру және жаңарту қажет.

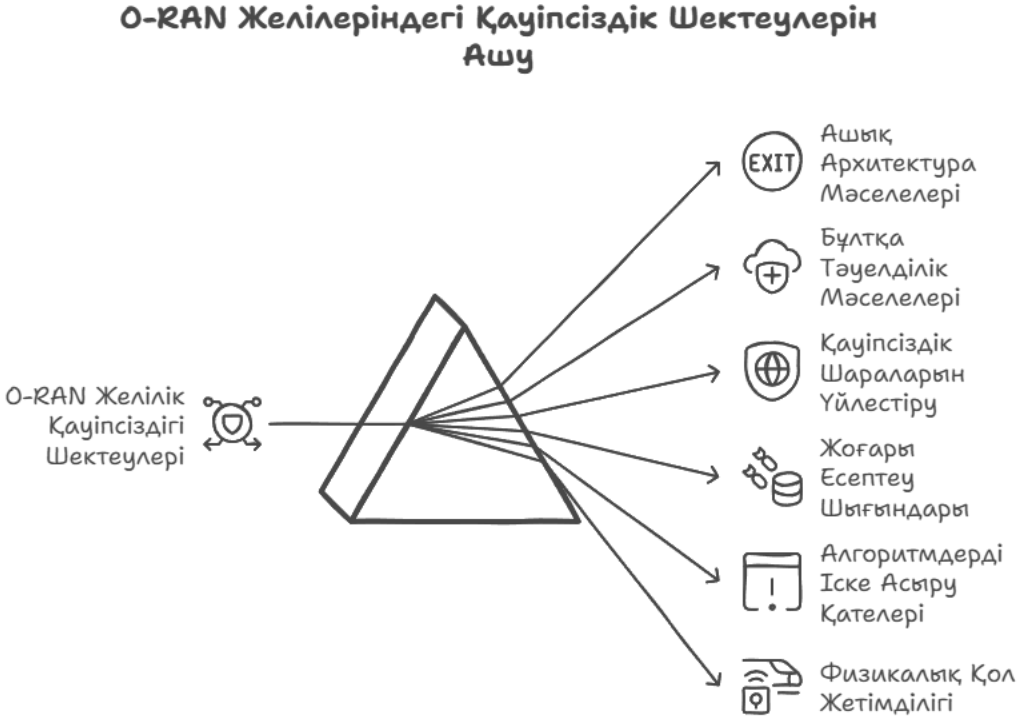
Бұдан бөлек, АРАЖ желілеріндегі қауіпсіздікті қамтамасыз етудің маңызды компоненттерінің бірі — трафикті бақылау және талдау. Бұл әдістер желідегі ауытқуларды анықтау, ықтимал қауіптерді табу және нақты уақыттағы оқиғаларға жауап беру үшін қолданылады. Атап айтқанда, бақылау жүйелері ТСТШ немесе MITM сияқты шабуылдарды тез анықтауға, желіні оңтайландыруға және сәйкестікті қамтамасыз етуге бағытталған. Сонымен бірге, интрузияны анықтау жүйелері (IDS), нақты уақыттағы деректерді талдау үшін Near-RT RIC, зиянды деректерді сүзу үшін трафикті тазарту орталықтары және Жасанды интеллект / Машиналық үйрену технологиялары қолданылады.

Бұл әдістердің де өз артықшылықтары мен шектеулері бар. Бір жағынан, олар қауіп-қатерлерге жылдам әрекет етуге, процестерді автоматтандыруға және желінің сенімділігін арттыруға көмектеседі. Екінші жағынан, бақылау жүйелері жоғары қаржылық шығындарды талап етуі мүмкін, жалған позитивтерге бейім болуы ықтимал және әртүрлі жабдықтармен біріктіру қиындықтарын тудыруы мүмкін. Сондықтан, бұл әдістерді жетілдіру тұрақты түрде жүзеге асырылуы қажет.

Жалпы алғанда, АРАЖ желілеріндегі қолданыстағы қауіпсіздік тәсілдерінің белгілі бір шектеулері бар. Біріншіден, Open Fronthaul және E2 сияқты көптеген интерфейстердің ашықтығы шабуылдарға кіру нүктелерінің санын көбейтеді. Екіншіден, әртүрлі өндірушілердің әртүрлі жабдықтары осалдықтардың ықтималдығын арттырады. Сонымен қатар, Near-RT RIC сияқты компоненттердің бұлтты инфрақұрылымда орналасуы виртуалды машиналардың немесе MEC (Көп қатынаулы жиегіндегі есептеу) сегменттерінің бұзылуына әкелуі мүмкін.

Сонымен бірге, қауіпсіздікті орталықтандырылған басқарудың болмауы қорғаныс шараларын үйлестіруде қиындықтар тудырады. Бұған қоса, IPSec және PDCP сияқты шифрлау әдістерін енгізу жоғары есептеу шығындарын талап етеді, бұл желінің өнімділігіне әсер етуі мүмкін. Оған қоса, хаттамалар мен қауіпсіздік

алгоритмдерін іске асыру кезіндегі қателіктер, сондай-ақ O-RU сияқты жабдықтардың физикалық қолжетімділігі желінің осалдығын арттырады. Осы мәселелердің барлығы бірыңғай қауіпсіздік стандарттарын енгізуді, хаттамаларды жетілдіруді және O-RAN инфрақұрылымының барлық деңгейлерін қорғауды күшейтуді талап етеді.



1.6-сурет - АРАЖ желілеріндегі қауіпсіздік шектеулері

1.4 Қауіпсіздікті қамтамасыз етудегі жасанды интеллекттің рөлі

Жасанды интеллект (ЖИ) қазіргі заманғы қауіпсіздік жүйелерінде, әсіресе нөлдік күн осалдықтары мен мақсатты шабуылдар сияқты күрделі киберқауіптер жағдайында таптырмас құралға айналуда. Бұл технология дәстүрлі әдістерден, соның ішінде антивирустар мен брандмауэрлерден әлдеқайда тиімді болып келеді. Сондықтан, қазіргі заманғы киберқауіптерге қарсы күресте AI негізіндегі шешімдер кеңінен қолданыла бастады.

AI-дың қауіпсіздік саласындағы негізгі артықшылықтарының бірі – нақты уақыт режимінде үлкен көлемдегі ақпаратты өңдеу мүмкіндігі. Сонымен қатар, жасанды интеллект машиналық оқыту алгоритмдерін қолдану арқылы жасырын қауіптерді анықтап, жүйеде болатын ауытқуларды бақылауға көмектеседі. Бұдан бөлек, тарихи деректерді талдау негізінде шабуылдарды болжау қабілеті де ерекше маңызды.

Оның үстіне, ЖИ қауіпсіздік қызметтерінің жұмысын жақсартуға ықпал етіп, жалған позитивтердің санын азайтады. Яғни, жүйе зиянды әрекеттерді дәл анықтап, қажетсіз ескертулердің алдын алады. Сонымен қатар, бейімделгіш жүйелердің арқасында жасанды интеллект қауіптің жаңа түрлерін тез үйреніп, оларға жылдам бейімделе алады.

1.4.1 Желілік трафикті талдау үшін ЖИ қолдану

Жасанды интеллект көмегімен желілік трафикті талдау – киберқауіптердің үнемі өсіп келе жатқан жағдайында қауіпсіздікті қамтамасыз етудің тиімді әдістерінің бірі. Бұл тәсіл трафиктегі күдікті заңдылықтарды анықтауға бағытталған. Мысалы, желі трафигінің кенеттен ұлғаюы деректердің бұзылуына немесе ТСТШ шабуылының басталуына әкелуі мүмкін. Осыған байланысты, ЖИ стандартты мінез-құлық үлгілерінен ауытқуларды дәл анықтап, қауіптерді ерте кезеңде бейтараптандыруға көмектеседі.

Бұл мүмкіндіктерді жүзеге асыру үшін жасанды интеллект нейрондық желілер мен кластерлеуді қоса алғанда, машиналық оқыту алгоритмдерін қолданады. Сонымен қатар, интеллектуалды интрузияны анықтау жүйелері (IDS) желідегі зиянды әрекеттерді тиімді түрде жіктеп, олардың алдын алуға мүмкіндік береді. Пайдаланушылардың мінез-құлқын бақылау арқылы ЖИ есептік жазбалардың бұзылуын немесе рұқсатсыз кіру әрекеттерін де анықтай алады.

Тағы бір маңызды артықшылығы – жасанды интеллекттің ТСТШ шабуылдарынан қорғау қабілеті. Ол қалыптан тыс желілік үлгілерді тез таниды, күдікті әрекеттерді блоктайды және қауіптерді анықтау үшін метадеректерді пайдалана отырып, тіпті шифрланған трафикті де талдай алады. Сонымен қатар, ЖИ желі трафигін заңды, күдікті және зиянды деп санаттарға жіктеп, әрбіріне тиісті қауіпсіздік саясатын қолдануға мүмкіндік береді.

Осы технологияның тиімділігін арттыру үшін терең оқыту әдістері, қайталанатын нейрондық желілер (RNN), конволюциялық нейрондық желілер (CNN), үлкен деректерді талдау және гибридті тәсілдер кеңінен қолданылады. Бұл ЖИ-дің өңдеу жылдамдығын арттырып, киберқауіптерді жоғары дәлдікпен анықтауға, ауқымды желілерге бейімделуге және киберқауіпсіздік мамандарына түсетін жүктемені азайтуға мүмкіндік береді.

Қолдану мысалдарына Darktrace және Vectra AI сияқты компаниялардың әзірлемелері, сондай-ақ энергетикалық инфрақұрылымдар мен банк жүйелері сияқты маңызды салаларды қорғау жатады. Осылайша, ЖИ желілік қауіпсіздікті қамтамасыз етуде таптырмас құралға айналып отыр.

1.4.2 Аномалияларды анықтау және шабуылдарды болжау

Аномалияларды анықтау және жасанды интеллект (ЖИ) көмегімен шабуылдарды болжау – желілер мен жүйелердің қауіпсіздігін қамтамасыз етудің маңызды құралы. Желілік трафиктегі немесе жүйелік процестердегі ауытқулар

кибершабуылдарды, конфигурация қателерін немесе күдікті әрекеттерді көрсетуі мүмкін. Дәстүрлі әдістер, мысалы, қолтаңбаларға немесе ережелерге негізделген шешімдер мұндай ауытқуларды әрдайым анықтай алмайды. Ал ЖИ деректерді терең талдау, күрделі үлгілерді тану және машиналық оқыту әдістерін қолдану арқылы күдікті әрекеттерді тиімді түрде анықтайды.

Жасанды интеллект трафикті жіктеу және пайдаланушылар мен құрылғылардың стандартты емес мінез-құлқын анықтау үшін бақылаулы, бақылаусыз және жартылай бақылаусыз оқыту әдістерін пайдаланады. Сонымен қатар, терең оқыту, автоэнкодерлер және уақыттық қатарларды талдау стандартты мінез-құлықтан ауытқуларды анықтауға мүмкіндік береді. Мысалы, пайдаланушының мінез-құлқын бақылау (UEBA) жүйесі сыртқы ресурстарға рұқсатсыз кіру әрекеттерін немесе қалыптан тыс белсенділікті тіркеп, осындай қауіптерге жылдам жауап бере алады.

Бұдан бөлек, ЖИ тарихи деректерді талдау арқылы ықтимал шабуыл сценарийлерін модельдейді және сыртқы қауіптерді бағалайды. Бұл жүйе, мысалы, хакерлік форумдарда осалдықтар туралы талқылауларды зерттеп, жаңа қауіптерді алдын ала болжауға қабілетті. Сондай-ақ ЖИ сұраныстардың экспоненциалды өсуін анықтау арқылы DDoS шабуылдарының басталуын алдын ала білуге және жүйе компоненттері үшін тәуекел деңгейін бағалауға мүмкіндік береді.

Осы технологияның негізгі артықшылықтарына процестерді автоматтандыру, нақты уақыт режимінде жұмыс істеу, жалған дабылдарды азайту және қауіптерді жоғары дәлдікпен анықтау жатады. Сонымен қатар, AI жаңа қауіптерге тез бейімделе отырып, деректерді талдаудың тиімділігін арттырады. Осылайша, жасанды интеллект желілер мен жүйелерді күрделі киберқауіптерден қорғаудың таптырмас шешіміне айналып отыр.

1.4.3 Қорғаныс процестерін автоматтандыру

Жасанды интеллект көмегімен қорғаныс процестерін автоматтандыру – ұйымдарға киберқауіптерге тиімді қарсы тұруға көмектесетін заманауи киберқауіпсіздіктің маңызды бағыты. Бұл технология қауіпсіздік процестерін жетілдіруде шешуші рөл атқарады және бірнеше негізгі аспектілерді қамтиды.

Біріншіден, ЖИ автоматтандырылған бақылауды жүзеге асырады, бұл оқиғалар журналдарын, желілік трафикті және құрылғылардың әрекеттерін үнемі талдауға мүмкіндік береді. Сонымен қатар, жасанды интеллект қауіптерді автоматты түрде анықтау жүйелерінде қолданылады, осылайша шабуылдардың белгілі және жаңа түрлерін ажыратуға қабілетті. Бұдан бөлек, ЖИ оқиғаларға автоматты түрде жауап береді, бұл күдікті трафикті бұғаттау, вирус жұққан құрылғыларды оқшаулау және зиянды бағдарламаларды жою секілді әрекеттерді жылдам орындауға мүмкіндік береді.

Екіншіден, ЖИ осалдықтарды басқаруды жақсартады, яғни жүйелерді сканерлеу, тәуекелдерді бағалау, осалдықтарды жоюға басымдық беру және тіпті

патчтарды автоматты түрде қолдану арқылы қауіпсіздікті күшейтеді. Сонымен қатар, стандарттарға сәйкестікті тексеру процесін автоматтандыру аудит пен сәйкестік шараларын жеңілдетеді.

Үшіншіден, жасанды интеллект шабуылдарды болжау және алдын алу процестерін жетілдіреді. ЖИ үлкен деректермен жұмыс істей отырып, нақты уақыттағы ақпаратты сүзуге, талдауға және ықтимал қауіптерді жіктеуге мүмкіндік береді. Бұл ұйымдарға кибершабуылдарға алдын ала дайындалуға және оларға жылдам жауап беруге жол ашады.

Автоматтандырудың негізгі артықшылықтарына уақытты үнемдеу, қауіптерді анықтау дәлдігін арттыру, нақты уақыт режимінде жұмыс істеу, жүйелерді кең ауқымда масштабтау және шығындарды азайту жатады. Сонымен қатар, ЖИ қауіпсіздік мамандарына стратегиялық мәселелерге көбірек көңіл бөлуге мүмкіндік береді, осылайша күнделікті тапсырмаларды жеңілдетіп, киберқауіптермен күресудің тиімділігін арттырады.

2 Жасанды интеллект негізінде қауіпсіздік тетіктерін әзірлеу

АРАЖ сияқты заманауи телекоммуникациялық желілер қауіпсіздікті қамтамасыз ету үшін инновациялық тәсілдерді қажет етеді, себебі олар үнемі дамып келе жатқан күрделі киберқауіптерге тап болуда. Дәстүрлі қорғаныс әдістері, мысалы, шабуыл қолтаңбаларына немесе статикалық ережелерге негізделген жүйелер, заманауи қауіп-қатерлерге төтеп бере алмайды. Сондықтан адаптивті, проактивті және автоматтандырылған қорғауды қамтамасыз ететін жасанды интеллект (ЖИ) және машиналық оқыту (МО) технологиялары барған сайын маңызды бола түсуде.

Жасанды интеллект қолдану бірнеше артықшылық береді. Біріншіден, ЖИ нақты уақыт режимінде үлкен көлемдегі деректерді өңдеуге қабілетті, бұл күдікті мінез-құлықты талдауға және қауіпті ауытқуларды жылдам анықтауға мүмкіндік береді. Екіншіден, шабуылдарды алдын ала болжау және оларға автоматты түрде әрекет ету мүмкіндігі желіні белсенді қорғауға ықпал етеді. Үшіншіден, ЖИ адамның араласуынсыз оқиғаларға жауап бере алады, бұл қауіп-қатерлерге жедел әрі тиімді қарсы тұруды қамтамасыз етеді. Сонымен қатар, талдау мен шешім қабылдау процестерін автоматтандыру АРАЖ желілерінің жалпы тиімділігін арттырады.

2.1 АРАЖ желілеріндегі ТСТШ шабуылдары: қауіптер мен өзектіліктер

АРАЖ желілері таратылған құрылымына байланысты бірқатар киберқауіптерге, соның ішінде ТСТШ шабуылдарына осал келеді. Атап айтқанда, o-CU және O-DU секілді негізгі компоненттер осындай шабуылдардың негізгі нысандарына айналуы мүмкін. Мұндай шабуылдар бұзылған пайдаланушы құрылғылары арқылы жаппай сұраныстар жіберу арқылы басқару элементтерін шамадан тыс жүктеп, сигналдық дауылдарды туындатады. Бұл, өз кезегінде, пайдаланушылардың тіркелуі мен аутентификациясының бұзылуына әкеліп соғады.

Сонымен қатар, шабуылдар O-CU және O-DU компоненттерінің есептеу ресурстарын сарқып, деректерді жеткізудегі кідірісті арттырады, бейне және дауыстық қызметтердің сапасын төмендетеді және жаңа қосылуларды бұғаттауға әкеледі. Бұдан бөлек, F1 және E1 интерфейстерін мақсатты түрде зақымдау арқылы шабуылдаушылар желі ішіндегі компоненттер арасындағы байланысты үзіп, АРАЖ инфрақұрылымының тұрақтылығына қатер төндіреді.

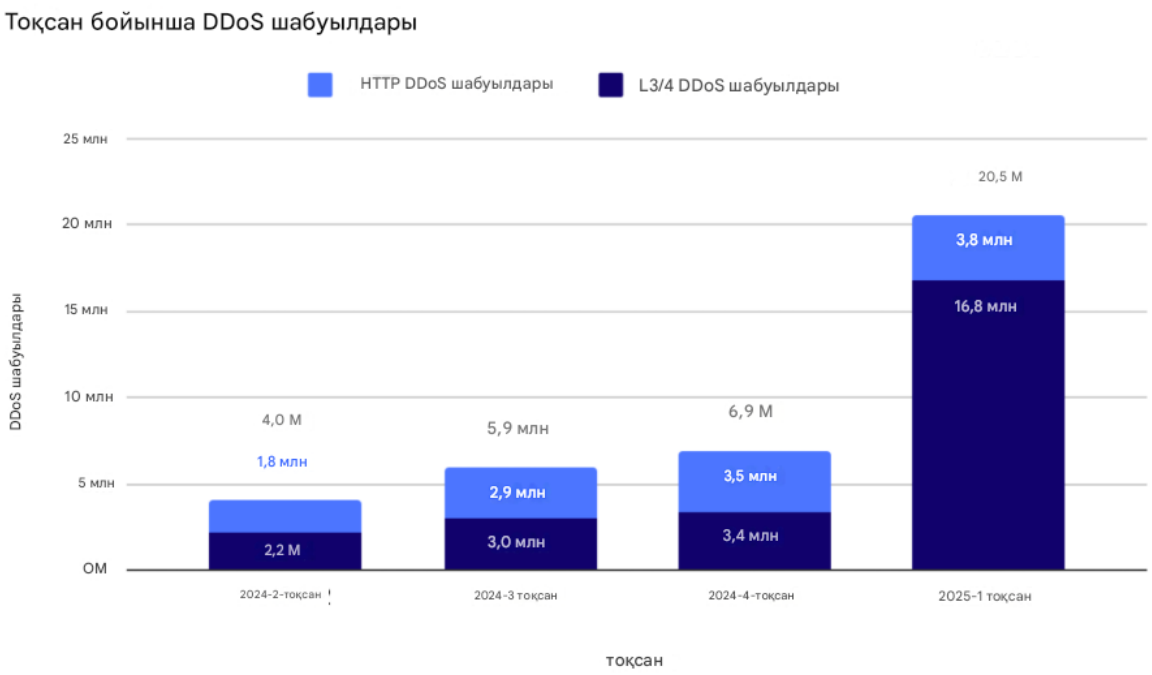
Бұл шабуылдардың салдары ауқымды болуы мүмкін: қызмет көрсету сапасының (QoS) айтарлықтай төмендеуі, операторлар үшін бір сағат ішінде жүздеген мың доллар көлемінде қаржылық шығын, сондай-ақ желі қолжетімділігінің жоғалуы нәтижесінде байланыс операторларының беделіне нұқсан келуі ықтимал. Мұндай қауіптердің өзектілігі соңғы жылдары айқын

байқалып отыр: мысалы, 2023 жылы ТСТШ шабуылдарының саны 200%-ға өскені тіркелген. Сарапшылардың болжауынша, ТСТШ-дан қорғанысқа бағытталған шешімдер нарығы 2030 жылға қарай 7,45 миллиард АҚШ долларына жетуі мүмкін.

АРАЖ архитектурасының таратылған табиғаты бұл осалдықтарды одан әрі күшейтеді. Себебі желідегі трафик ондаған түйіндер арқылы өтеді, бұл шабуылдарды анықтауды күрделендіреді. Сонымен қатар, желінің төмен кідірісі (<10 мс) қолтаңбаға негізделген классикалық қорғаныс әдістерінің тиімділігін шектейді. Қазіргі кезде байқалып отырған қауіптер қатарына Zero-Day шабуылдары, АРАЖ-ның E2 секілді протоколдық интерфейстеріндегі осалдықтарды пайдалану, сондай-ақ IoT құрылғылары негізінде құрылған ботнеттер арқылы іске асырылатын жаппай шабуылдар жатады.

Дәстүрлі қауіпсіздік тетіктері желіде деректердің жоғары жылдамдықпен генерациялануына және F1 мен E1 сияқты интерфейстерде жаңа шабуыл түрлерін уақытылы танудағы қиындықтарға байланысты өз тиімділігін жоғалта бастады. Осыған байланысты, жасанды интеллект және машиналық оқыту технологияларын қолдану АРАЖ қауіпсіздігін қамтамасыз етуде негізгі бағыттардың біріне айналуда.

ЖИ негізіндегі шешімдер нақты уақыт режимінде трафик үлгілерін терең талдауға, құрылғылардың мінез-құлқындағы ауытқуларды логистикалық регрессия немесе нейрондық желілер көмегімен анықтауға мүмкіндік береді. Сонымен бірге, LSTM (Long Short-Term Memory) үлгілері арқылы желілік шамадан тыс жүктемелерді алдын ала болжауға болады. Бұдан бөлек, сыртқы динамикалық тізімдер негізінде күмәнді IP немесе IMEI идентификаторларын автоматты түрде бұғаттау мүмкіндігі бар, бұл желіні зиянды трафиктен жедел қорғайтын тиімді механизм ретінде қолданылады.



2.1-сурет – Тоқсан бойынша ТСТШ шабуылдары

Диаграммада 2024 жылдың 2-тоқсанынан бастап 2025 жылдың 1-тоқсанына дейінгі кезеңде тіркелген ТСТШ шабуылдарының сандық өсімі бейнеленген. Бұл мәліметтер HTTP деңгейіндегі (қабат 7) және желілік/транспорттық деңгейдегі (қабат 3/4) шабуылдарды жеке-жеке қарастыра отырып, олардың жалпы динамикасын салыстыруға мүмкіндік береді.

2024 жылдың 2-тоқсанында жалпы ТСТШ шабуылдарының саны 4,0 миллионды құраған. Оның ішінде 2,2 миллионы — L3/4 деңгейіндегі шабуылдар болса, 1,8 миллионы — HTTP деңгейіндегі шабуылдар. Келесі тоқсанда, яғни 2024 жылдың 3-тоқсанында бұл көрсеткіш 5,9 миллионға жетіп, тиісінше 3,0 млн (L3/4) және 2,9 млн (HTTP) шабуылдар тіркелген. Бұл кезеңде HTTP шабуылдарының L3/4 шабуылдарына жақындай түскені байқалады.

2024 жылдың 4-тоқсанында шабуыл саны 6,9 миллионға дейін өскен. Бұл көрсеткіштің ішінде 3,4 миллионы – L3/4, ал 3,5 миллионы – HTTP шабуылдары, яғни осы тоқсанда HTTP шабуылдары алғаш рет L3/4 шабуылдарының санынан асып түскен. Бұл өзгеріс, шабуыл түрлерінің динамикасындағы маңызды бетбұрыс ретінде бағалануы мүмкін.

2025 жылдың 1-тоқсанында ТСТШ шабуылдарының жалпы саны күрт артып, 20,5 миллионға жеткен. Оның ішінде 16,8 миллионы – L3/4 деңгейіндегі шабуылдар болса, 3,8 миллионы – HTTP шабуылдары. Бұл кезеңде L3/4 шабуылдарының саны айтарлықтай артқан, ал HTTP шабуылдары салыстырмалы түрде біршама баяу өскен.

2.2 АРАЖ желілеріндегі ТСТШ шабуылдарына қарсы жасанды интеллекттің рөлі

Жасанды интеллект АРАЖ архитектурасында ТСТШ шабуылдарынан қорғауда маңызды рөл атқарады. Себебі қолтаңбаны талдау, статикалық брандмауэр ережелері секілді дәстүрлі әдістер деректер ағынының жоғары жылдамдығына, қауіптерді анықтаудың кешенділігіне және жедел жауап берудің қажеттілігіне бейімделуде шектеулі. Бұл жағдайда машиналық оқыту алгоритмдері тиімді балама ретінде ұсынылады.

Атап айтқанда, логистикалық регрессия және шешім ағашы сияқты әдістер нақты уақыттағы трафикті талдау және ауытқуларды жіктеу үшін қолданылады. Сонымен қатар, кластерлеу алгоритмдері мен терең оқыту тәсілдері (LSTM, Autoencoder) пайдаланушы құрылғыларының күрделі мінез-құлық үлгілерін анықтауға мүмкіндік береді. Бұл модельдер шабуыл түрлерін нақты айқындап, шабуылдың алдын алуға бағытталған шешімдерді уақтылы қабылдауға жол ашады.

Қорғанысты көпдеңгейлі ұйымдастыру аясында бірнеше ЖИ-негізделген қызметтер енгізіледі. Атап айтқанда, РАЖ деңгейіндегі dApp шешімі сыртқы динамикалық тізім негізінде зиянды құрылғыларды дереу бұғаттауға мүмкіндік береді. Сонымен қатар, near-RT RIC құрамындағы xApp-U модулі күдікті құрылғыларды терең талдайды, ал xApp-S модулі түрлі қызметтердің корреляциясын жүзеге асырады. Бұл кешенді тәсіл жалған оң нәтижелердің үлесін 30–50% аралығында төмендетуге мүмкіндік береді.

Айта кету керек, EDL механизмін пайдалану арқылы жауап беруді автоматтандыру — шабуылдаушы IP немесе IMEI мекенжайларының тізімдерін жедел жаңартуға жол ашады. Бұл қорғаныс шараларының жылдамдығын едәуір арттырып, дәстүрлі YANG моделдеріне қарағанда жоғары масштабталуды қамтамасыз етеді.

2.3 ЖИ негізіндегі ТСТШ анықтау алгоритмдері

АРАЖ желілерінде ТСТШ шабуылдарын анықтауда жасанды интеллект алгоритмдерінің үш негізгі санаты — мұғаліммен оқыту, мұғалімсіз оқыту және терең оқыту әдістері қолданылады. Бұл тәсілдердің әрқайсысы шабуылдарды тиімді талдау мен болжауға бағытталған түрлі модельдерді қамтиды.

Мұғаліммен оқыту әдістері алдын ала таңбаланған деректерге негізделеді. Бұл бағытта SVM, Random Forest, XGBoost секілді классикалық алгоритмдермен қатар, көп қабатты нейрондық желілер (MLP) кеңінен қолданылады. Аталған модельдер трафиктегі ауытқуларды дәл жіктеуге мүмкіндік береді, алайда сынып теңгерімсіздігі мәселесі оларды қолдануда қосымша шешімдерді талап етеді.

Ал мұғалімсіз оқыту әдістері алдын ала таңбаланбаған деректерді талдау арқылы аномалияларды анықтауға бағытталған. K-means, DBSCAN, One-Class

SVM және автоэнкодерлер секілді алгоритмдер белгісіз сипаттағы шабуылдарды анықтауда маңызды рөл атқарады. Бұл әдістер, әсіресе жаңа немесе белгісіз қауіп-қатерлерді тануда тиімділігімен ерекшеленеді.

Терең оқыту әдістері күрделі трафик үлгілерін зерттеуде кеңінен пайдаланылады. Уақыттық деректерді талдауда RNN және LSTM модельдері қолданылады, ал кеңістіктік сипаттамаларды өңдеуде CNN тиімді болып саналады. Сонымен қатар, CNN мен LSTM-нің біріктірілген гибридті модельдері желілік ағындарды кешенді сараптау үшін қолданылады. Бұған қоса, XGBoost немесе графтық нейрондық желілермен (GNN) біріктірілген автоэнкодерлер ботнеттер сияқты күрделі шабуыл үлгілерін дәлірек модельдеуге мүмкіндік береді.

ЖИ модельдері негізінде талданатын негізгі сипаттамаларға трафик көлемі, сұраныс көздері, хаттама түрлері мен пайдаланушылардың мінез-құлық ерекшеліктері жатады. Ал модельдердің шешімдерін түсіндіру үшін LIME және SHAP сияқты интерпретация әдістері қолданылады, бұл өз кезегінде қауіптің қай көзден туындағанын нақты анықтауға жағдай жасайды.

Жасанды интеллектке негізделген шешімдерді табысты енгізу мысалдарына Cloudflare, Darktrace және AWS Shield қызметтері жатады. Бұл платформалар зиянды трафикті нақты уақыт режимінде анықтап, оны бұғаттауда машиналық оқытуды белсенді қолданады. Модельдердің тиімділігін бағалау үшін дәстүрлі метрикалар — Precision, Recall, ROC-AUC және F1-score — пайдаланылады. Бұл өлшемдер жалған оң нәтижелер мен шабуылдарды өткізіп жіберу ықтималдығын төмендетуге мүмкіндік береді, осылайша жүйенің сенімділігі мен қауіпсіздігін арттырады.

2.4 Қорғаныс механизмдерінің тиімділігін бағалау

АРАЖ инфрақұрылымында қорғаныс тетіктерінің тиімділігін бағалау мақсатында желілік трафикті талдау негізінде түрлі машиналық оқыту алгоритмдері қолданылды. Бұл бағалау процесі ауытқуларды дер кезінде анықтау және ықтимал ТСТШ шабуылдарының алдын алу үшін жүргізілді.

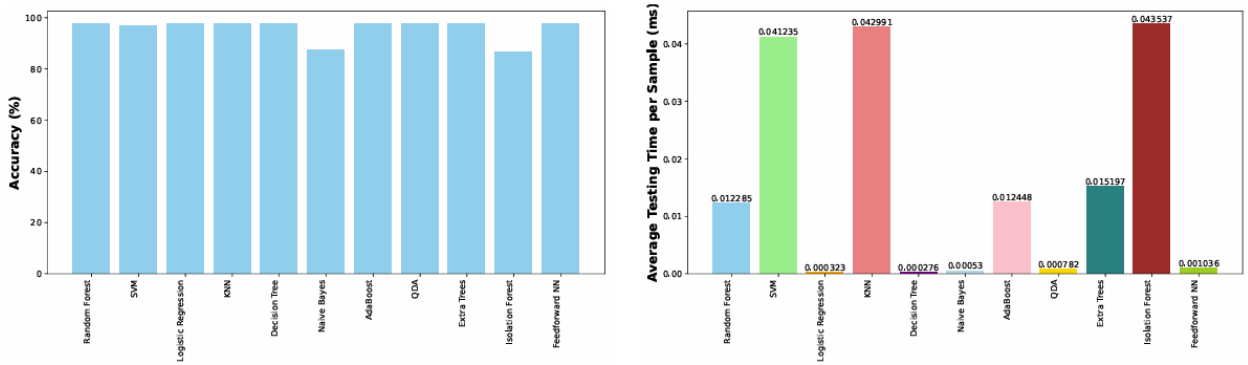
Әрбір қолданылған алгоритм үшін бірнеше негізгі метрикалар есептелді. Accuracy (дәлдік) — барлық дұрыс жіктелген оқиғалардың жалпы үлесін сипаттайды, ал Precision (нақтылық) — шабуыл ретінде белгіленген оқиғалардың ішінен шын мәнінде зиянды әрекеттердің қаншалықты дұрыс анықталғанын көрсетеді. Сонымен қатар, Recall (толықтық) — модельдің нақты шабуылдардың қаншасын анықтай алғанын өлшейді, ал FPR (жалған оң нәтиже деңгейі) — зиянсыз трафиктің шабуыл ретінде қате танылу ықтималдығын көрсетеді.

Бұдан бөлек, оқыту және тестілеу уақыты модельдің нақты уақыттағы оқиғаларға жауап беру қабілетіне тікелей әсер етеді. Тиімді қорғаныс жүйесін құру барысында алгоритм таңдау деректердің өңдеу жылдамдығы мен жүйеге қойылатын дәлдік талаптарына байланысты жүзеге асырылады. Ал модельдерді

оңтайландыру барысында дәлдік пен есептеу өнімділігі арасындағы теңгерімді сақтау қажеттілігі туындайды.

TABLE II
PERFORMANCE COMPARISON OF VARIOUS ML ALGORITHMS.

Methods	Accuracy (%)	Precision (%)	Recall (%)	FPR (%)	Avg. Training Time (ms)	Avg. Testing Time (ms)
Random Forest	97.60	97.11	93.85	1.03	1455.36	24.57
SVM	96.85	98.57	89.57	0.48	1650.37	82.47
Logistic Regression	97.55	98.03	92.73	0.68	94.5400	0.650
KNN	97.50	95.86	94.79	1.50	1.31000	85.98
Decision Tree	97.65	97.30	93.85	0.96	64.2500	0.550
Naive Bayes	87.55	100.00	53.63	0.00	5.13000	1.060
AdaBoost	97.60	96.39	94.60	1.30	1137.02	24.90
QDA	97.65	92.39	99.44	3.01	10.6800	1.560
Extra Trees	97.60	97.11	93.85	1.03	434.270	30.39
Isolation Forest	86.50	78.22	68.90	7.04	1299.59	87.07
Feedforward NN	97.55	98.22	92.55	0.62	5823.98	2.070



2.2-сурет - Әр түрлі МО алгоритмдерінің өнімділігін салыстыру.

2.2-сурет бойынша АРАЖ инфрақұрылымында ауытқуларды анықтау мақсатында қолданылатын 10 түрлі машиналық оқыту алгоритмінің тиімділігін салыстыра отырып, олардың дәлдігі, нақтылығы, анықтау қабілеті (recall), жалған оң нәтиже деңгейі (FPR), сондай-ақ оқыту және тестілеу уақыты сияқты көрсеткіштеріне талдау жасайды.

Зерттеу нәтижелері бойынша, ең жоғары дәлдік көрсеткішіне — 97.65% — Random Forest, Decision Tree, Extra Trees және AdaBoost алгоритмдері қол жеткізген. Ал ең төмен дәлдік — 87.55% — Naive Bayes үлгісінде тіркелді. Precision (нақтылық) бойынша Logistic Regression (98.03%) және Feedforward Neural Network (98.22%) алдыңғы қатарда тұрса, Isolation Forest бұл көрсеткіш бойынша ең төмен нәтиже (78.22%) көрсетті.

Recall (толықтық) көрсеткіші бойынша QDA алгоритмі 99.44% мәнімен ерекшеленді, бұл оның нақты шабуылдарды анықтаудағы жоғары қабілетін көрсетеді. Керісінше, Naive Bayes (53.63%) және Isolation Forest (68.90%) төмен нәтижелерге ие болды. Сонымен қатар, жалған оң позитивтер деңгейі (FPR) ең төмен SVM (0.48%) және Feedforward NN (0.62%) үлгілерінде байқалса, Isolation Forest-те бұл көрсеткіш 7.04%-ке жетіп, қателіктердің жиі орын алуына себеп болуы мүмкін екенін көрсетті.

Оқыту уақыты бойынша Naive Bayes ең жылдам алгоритм ретінде танылып, бар болғаны 5.13 миллисекунд жұмсаған. Ең баяу оқыту уақыты

Feedforward Neural Network үлгісінде тіркеліп, ол 5823.98 миллисекунд қажет етті. Ал тестілеу уақыты бойынша Logistic Regression 0.650 мс нәтижесімен ең жылдам, ал Isolation Forest 87.07 мс мәнімен ең баяу үлгі ретінде танылды.

3 Желілік трафикті бақылау жүйесін тәжірибелік енгізу

Алдыңғы тарауларда АРАЖ архитектурасының қауіпсіздігіне қатысты теориялық аспектілер жан-жақты қарастырылып, ықтимал қауіптер, соның ішінде таратылған қызмет көрсетуге бағытталған ТСТШ шабуылдарының сипаттамалары талданды. Сонымен қатар, жасанды интеллектті қолдану арқылы аномалияларды анықтаудың заманауи әдістері баяндалды. Алайда теориялық тұжырымдар мен әдістердің тиімділігін нақты бағалау үшін оларды тәжірибелік ортада сынақтан өткізу аса маңызды.

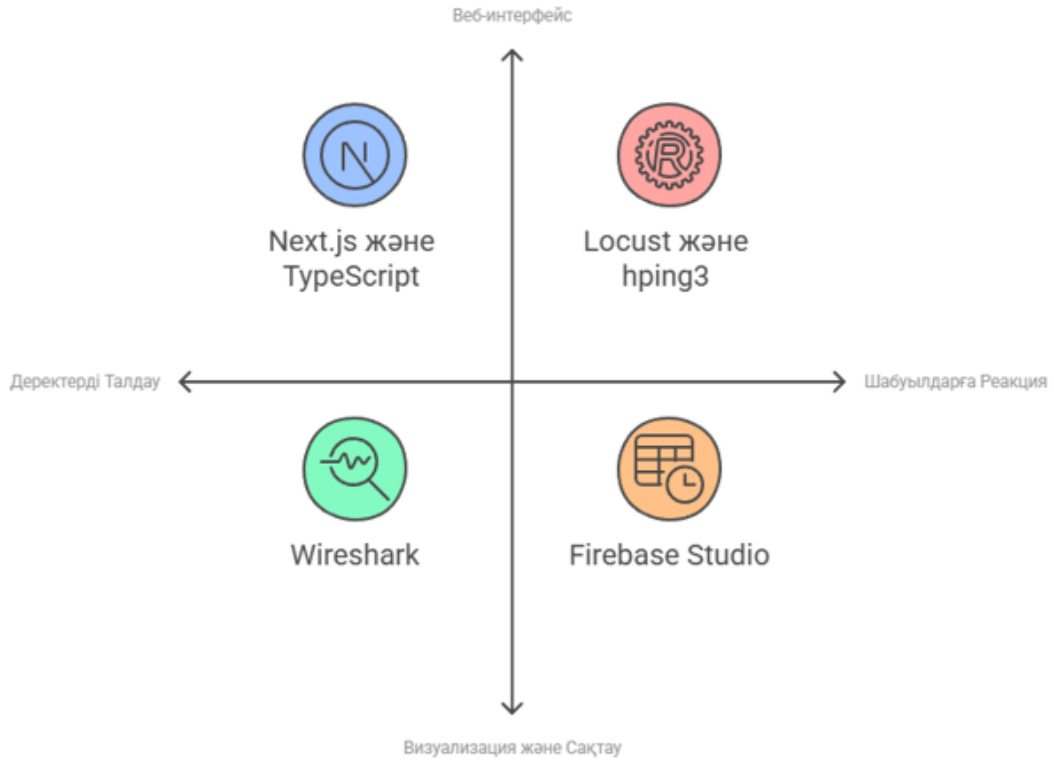
Осыған байланысты бұл тарауда АРАЖ архитектурасын модельдейтін эмуляциялық ортада желілік трафикті бақылау жүйесін практикалық тұрғыдан жүзеге асыру ұсынылады. Мұндағы негізгі мақсат — жүйенің ауытқулар мен ықтимал ТСТШ шабуылдарын нақты уақыт режимінде анықтау қабілетін бағалау. Эксперименттік негіз ретінде Wireshark құралымен 2024 жылы жиналған деректер жиыны пайдаланылды. Бұл деректер заңды және зиянды трафиктің шынайы сценарийлерін бейнелеуге мүмкіндік беріп, модельдеудің нақтылығын қамтамасыз етті.

Жиналған деректер Firebase Studio негізінде әзірленген ORAN Defender веб-интерфейсімен біріктірілді. Бұл интеграция желі трафигін визуалды түрде бақылауға, аномалияларды дер кезінде анықтауға және шабуылдар туралы нақты ақпарат беруге мүмкіндік береді. Сонымен қатар, визуализация құралдары желіде болып жатқан оқиғаларды интуитивті түрде талдауға жағдай жасап, қорғаныс жүйесінің тиімділігін бағалауды едәуір жеңілдетті.

3.1 Жасалған жүйенің архитектурасы және зерттеу әдістемесі

Әзірленген жүйенің архитектурасы АРАЖ ортасында желілік трафикті үздіксіз бақылауды және ықтимал ауытқуларды анықтауды қамтамасыз ететін бірнеше өзара байланысқан негізгі компоненттерден тұрады. Атап айтқанда, Wireshark құралы 2024 жылы жинақталған .pcap форматындағы желілік трафик деректерін талдау үшін пайдаланылды. Бұл құрал IP-мекенжайлар, порттар және протоколдар бойынша пакеттерді сүзу арқылы нақты сценарийлерді, соның ішінде ТСТШ шабуылдарын модельдеуге мүмкіндік берді, нәтижесінде модельдің шабуылдарға қарсы әрекет ету мүмкіндігі тәжірибелік тұрғыда сыналды.

Деректерді сақтау, өңдеу және визуализациялау мақсатында Firebase Studio шешімі қолданылды. Онда Realtime Database желіден алынған ақпаратты нақты уақытта сақтап, жүйенің жауап беру қабілетін қамтамасыз етті. Сонымен қатар, Firebase Hosting қызметі ORAN Defender демо-сайтын орналастыру үшін пайдаланылып, Authentication модулі арқылы қолжетімділікті қорғауға мүмкіндік берілді.



3.1-сурет – АРАЖ желілік трафикті бақылау архитектурасы

Жүйенің негізгі компоненттерінің бірі — Next.js және TypeScript негізінде әзірленген ORAN Defender веб-интерфейсі. Бұл интерфейс желілік трафикті бақылауға, деректерді визуалды түрде ұсынуға және ТСТШ шабуылдарын нақты уақыт режимінде модельдеуге жағдай жасайды. Сонымен бірге, жүйе машиналық оқыту моделімен интеграцияланған. Атап айтқанда, Isolation Forest алгоритмі Wireshark арқылы алынған желілік деректер негізінде оқытылып, желіде орын алатын күдікті әрекеттерді автоматты түрде анықтауға мүмкіндік береді.

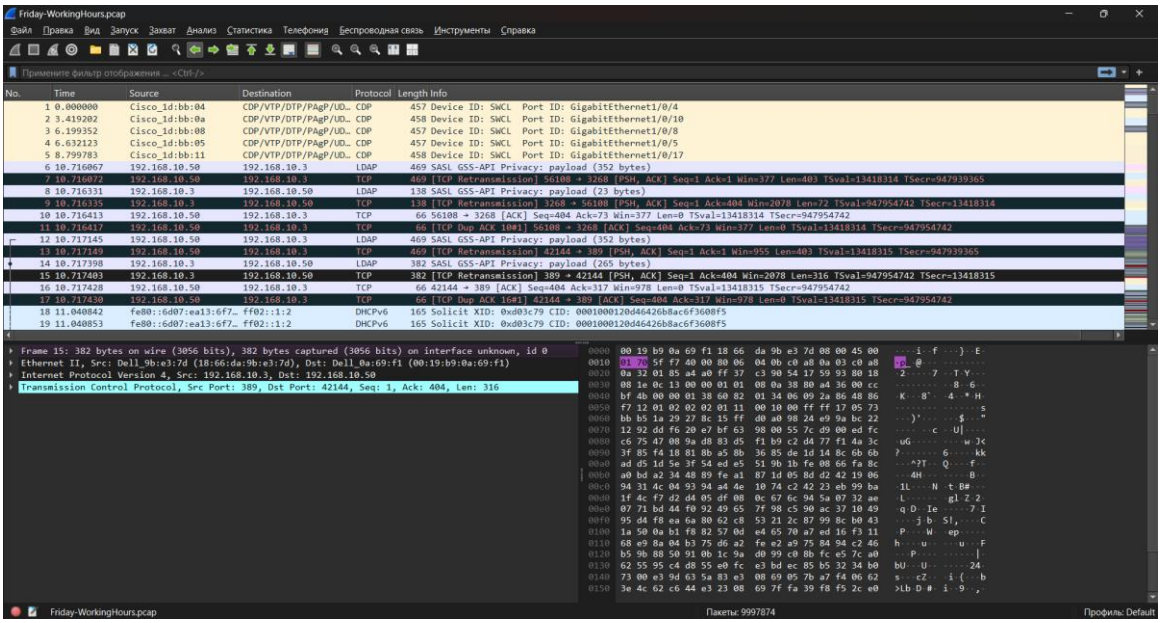
Жүйенің шабуыл жағдайларына реакциясын бағалау мақсатында Locust және hping3 құралдары қолданылды. Locust желіге жүктеме түсіру арқылы жүйенің өткізу қабілетін, ал hping3 нақты ТСТШ шабуылдарын модельдеу арқылы ЖИ алгоритмдерінің төтенше жағдайларда жұмыс істеу тиімділігін тексеруге мүмкіндік берді.

Нәтижелерді талдау Wireshark құралымен және Firebase платформасымен жүзеге асырылды. Бұл жүйе арқылы модельдің нақты уақытта қалай әрекет ететіндігі, аномалияларды қаншалықты тиімді өңдейтіні және шабуыл жағдайларында жауап беру қабілеті кешенді түрде бағаланды.

3.2 Wireshark-пен жұмыс және Firebase интеграциясын практикалық іске асыру

Эксперименттік бөлімде желілік трафикті бақылау жүйесі құрылып, ол Wireshark және Firebase Studio негізінде жүзеге асырылған ORAN Defender веб-интерфейсіне біріктірілді. Бұл жүйе 2024 жылы жазылған Friday-workinghours.pcap файлы негізінде әзірленді және нақты желілік ортада орын алатын заңды әрі зиянды трафикті модельдеуге мүмкіндік береді. Талдауға алынған .pcap файлы CDP, TCP, UDP, DHCPv6, LDAP және DNS секілді әртүрлі желілік хаттамаларды қамтитын 9 997 874 желілік пакетті қамтиды.

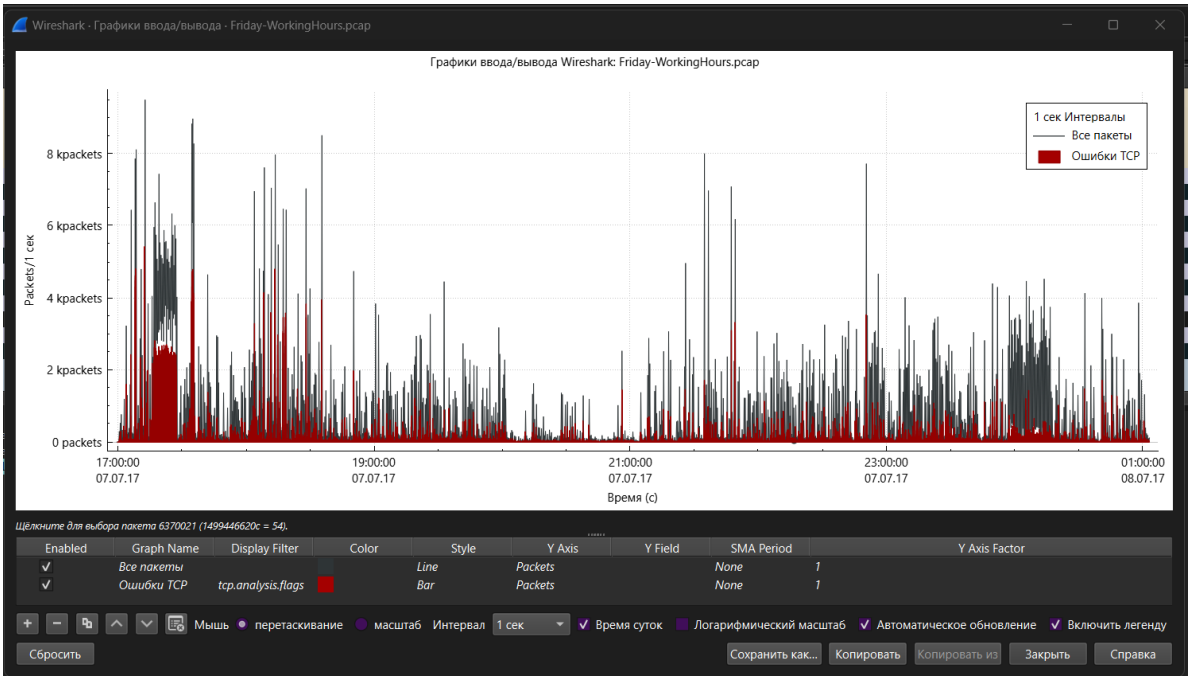
Wireshark құралында алынған кестелік құрылым әрбір пакетке қатысты бірқатар маңызды параметрлерді көрсетеді: пакет нөмірі, тіркелу уақыты, дереккөз және алушы IP мекенжайлары, қолданылған хаттама түрі және пакет өлшемі. Бұл көрсеткіштер желідегі белсенділікті егжей-тегжейлі талдауға және ықтимал аномалияларды анықтауға мүмкіндік береді.



3.2-сурет – Wireshark интерфейсі

Алынған трафик негізінде бірнеше маңызды бақылаулар жасалды. Атап айтқанда, 192.168.10.3 және 192.168.1.1 IP-мекенжайларымен байланысты белсенді құрылғылар анықталды. Сонымен қатар, TCP хаттамасына тән ACK, SYN, RST пакеттерінің жоғары концентрациясы тіркелді. Бұл, өз кезегінде, DDoS шабуылдарының белгілері ретінде қарастырылуы мүмкін. Мысалы, UDP flood шабуылдарына тән UDP пакеттерінің шамадан тыс көбеюі, SYN flood шабуылдарын көрсететін ACK жауабы жоқ SYN пакеттері, сондай-ақ шамадан тыс TCP retransmissions құбылыстары желіге бағытталған аномальды жүктемені көрсетеді.

Жүйенің архитектурасы Firebase платформасын кеңінен қолдану арқылы жүзеге асырылды. Атап айтқанда, Firebase Realtime Database желіден алынған трафикті нақты уақытта жіберу мен сақтау үшін пайдаланылды, ал Firebase Hosting ORAN Defender веб-интерфейсін орналастыруды қамтамасыз етті. Желілік пакеттердің мазмұны Ethernet II, IPv4 және TCP тақырыптары негізінде талданды, бұл аномалияларды контекстуалдық тұрғыда түсіндіруге мүмкіндік берді. Мысалы, DHCPv6 немесе DNS хаттамаларының шамадан тыс белсенділігі инфрақұрылымға бағытталған ықтимал шабуылдардың белгісі ретінде қарастырылды.



3.3-сурет – Кіріс және шығыс графигінің сипаттамасы

Wireshark бағдарламасындағы IO Graphs (Input/Output Graphs) – желілік әрекеттердің уақыт бойынша өзгерісін визуализациялауға арналған тиімді құрал. Ол секундына пакеттердің немесе байттардың санының динамикасын көрсету арқылы трафикті тереңірек талдауға мүмкіндік береді. Бұл құрал желідегі қосылым жиілігін бақылауға, жүктеме өзгерістерін анықтауға, хаттамалар арасындағы белсенділікті салыстыруға және ықтимал кибершабуылдарды тануға көмектеседі.

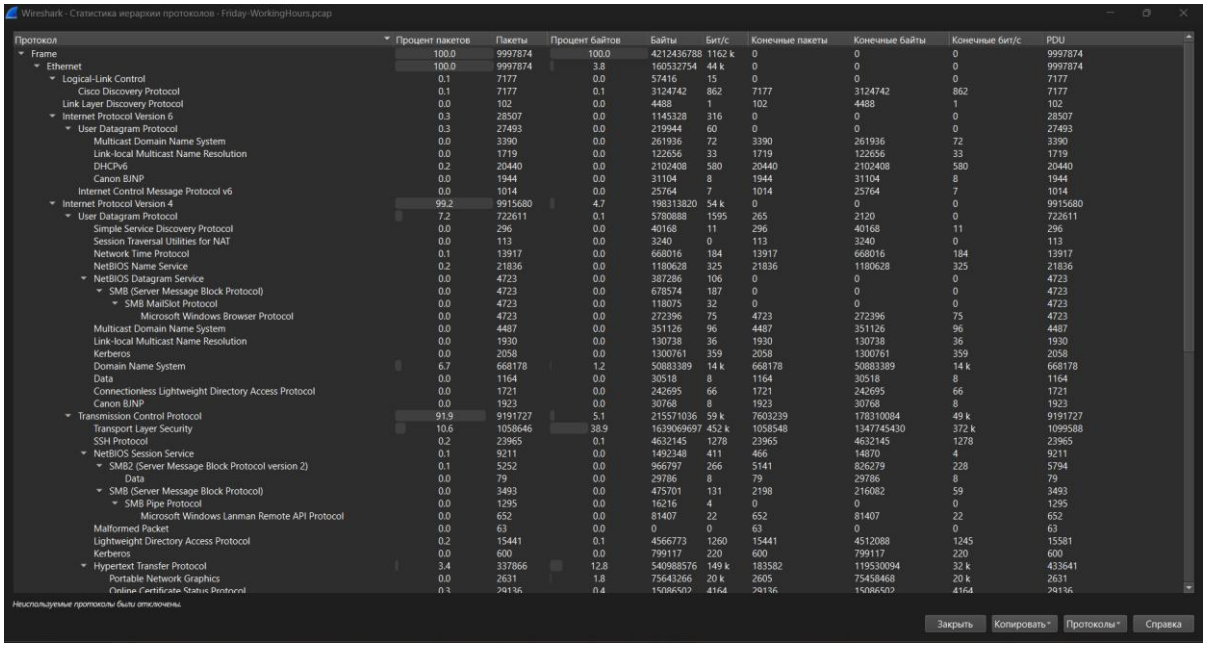
IO Graphs әсіресе ТСТШ шабуылдарын анықтау мен талдау барысында пайдалы. Себебі мұндай шабуылдар жүйені көптеген сұраныстармен шамадан тыс жүктеп, заңды пайдаланушылар үшін қолжетімсіз етеді. Мұндай жағдайларда трафик көлемі кенет өсіп, желіде қалыптан тыс белсенділік байқалады. Wireshark бұл өзгерістерді нақты көрсету арқылы қауіптерді уақытылы анықтауға мүмкіндік береді.

Желідегі қалыптан тыс белсенділіктің кейбір белгілері – секундына пакеттер санының айтарлықтай артуы, TCP деңгейіндегі қателердің көбеюі

немесе белгілі бір хаттамалардың тұрақты белсенділігі. Мысалы, SYN flood немесе UDP flood шабуылдары кезінде желіде сәйкес пакеттер саны көбейіп, жүйенің қалыпты жұмысын тежейді. TCP хаттамасында RST немесе FIN пакеттерінің шамадан тыс көбеюі сервердің ресурстар тапшылығын немесе шамадан тыс жүктемесін көрсетуі мүмкін. Ал ұзақ уақыт бойы жоғары белсенділік сақталса, бұл шабуыл арқылы жүйені әдейі әлсірету әрекетін білдіруі ықтимал.

Виртуалдандырылған және таратылған құрылымға негізделген АРАЖ архитектурасы үшін мұндай шабуылдар аса қауіпті. Жүктеменің өсуі RU, DU және CU компоненттері арасындағы байланыстың үзілуіне, қызметтің кешігуіне немесе толық істен шығуына алып келуі мүмкін. IO Graphs бұл қауіптерді ерте кезеңде анықтауға көмектесіп, желі жұмысының сенімділігін арттырады.

ORAN Defender веб-қосымшасына IO Graphs құралын біріктіру жүйені бақылауды ыңғайлы әрі көрнекі етеді. Қолданушы трафик динамикасын нақты уақыт режимінде көріп, желі жағдайын жылдам бағалай алады. Сонымен қатар, осы графиктерден алынған деректер машиналық оқыту модельдері үшін маңызды ақпарат көзіне айналады.



3.4-сурет – Хаттама иерархиялары

Желілік трафикті талдау нәтижесінде трафик құрылымы, хаттамалардың таралуы және желідегі ауытқулар туралы нақты әрі дәл ақпарат алынды. Бұл ақпарат желі қауіпсіздігін қамтамасыз ету, соның ішінде ТСТШ шабуылдарын анықтау және алдын алу үшін шешуші мәнге ие.

Талдау «жұма-жұмысшылар.pcap» атты бастапқы файл негізінде жүргізілді. Бұл файлда жалпы көлемі 421 ГБ болатын 9,997,874 желілік пакет

тіркелген. Талдау OSI үлгісінің Ethernet деңгейінен бастап HTTP және SMB сияқты жоғары қолданбалы деңгейлеріне дейінгі барлық қабаттарын қамтыды.

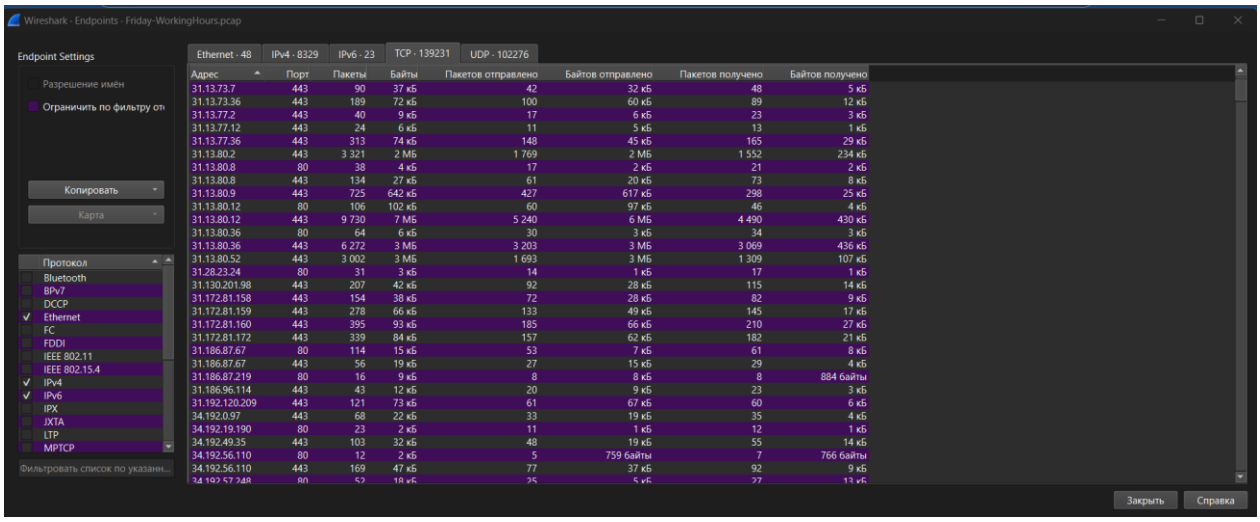
Хаттамалар бойынша мәліметтер арнайы кесте арқылы құрылымдалды. Кестеде әр хаттаманың атауы, жалпы трафиктегі пакеттер мен байттардың пайыздық үлесі, тасымал жылдамдығы, соңғы тіркелген белсенділік пен PDU көрсеткіштері қамтылған.

Ethernet барлық пакеттердің 100%-ын қамтыды, бұл деректердің осы деңгей арқылы өңделетінін көрсетеді. IPv4 хаттамасы 99.2% үлеспен негізгі интернет протоколы ретіндегі орнын дәлелдеді. TCP хаттамасы 91.9% (163 ГБ) көрсеткішпен сенімді қосылымдар мен деректер алмасу процесінде басым қолданылды. UDP хаттамасының үлесі 7.2% (57 МБ) көлемінде тіркеліп, ол негізінен DNS және NTP қызметтерімен байланысты болды.

DNS хаттамасы 668,178 пакет және 508 МБ көлемімен домендік атауларды шешу процесінде белсенді қолданылған. HTTP 337,866 пакет және 54 ГБ көлеммен веб-қызметтер арқылы үлкен көлемде дерек алмасуды қамтамасыз етті. SMB хаттамасы 4,723 пакет және 67 МБ дерекпен Windows желілеріндегі файл алмасуды сипаттады.

Талдау барысында Malformed Packet деп белгіленген 63 пакет тіркелді. Бұл пакеттер деректер құрылымындағы бұзылуларды немесе дұрыс емес форматтағы ақпаратты білдіреді. Kerberos хаттамасы 600 пакет және 456 МБ көлемінде тіркеліп, аутентификация процестерінің қарқынды жүріп жатқанын көрсетті.

Трафиктегі кейбір заңдылықтар ТСТШ шабуылдарына тән сипаттамалармен толық сәйкес келеді. TCP хаттамасы бойынша тіркелген көп көлемді SYN пакеттері желіге бағытталған SYN flood шабуылының бар екенін көрсетеді. UDP хаттамасы негізіндегі трафиктің белсенділігі, әсіресе DNS сұрауларының көбеюі, UDP flood шабуылының жүргізілгенін дәлелдейді. Сонымен қатар DNS, HTTP және SMB хаттамаларындағы шамадан тыс белсенділік серверлерге жасалған тікелей жүктемені білдіреді.



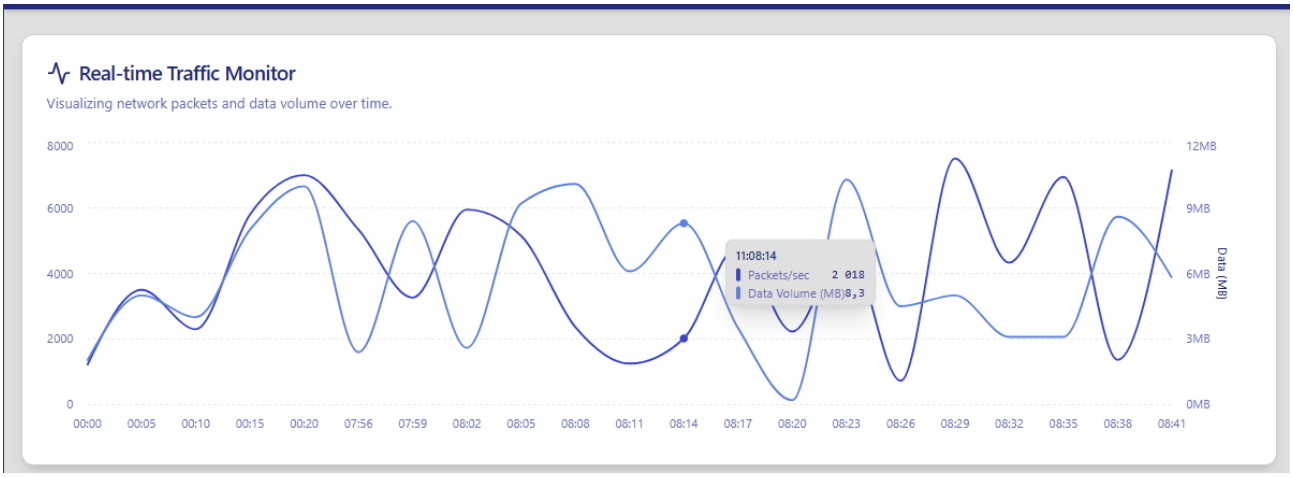
3.5-сурет – Түпкі тораптар кестесі

Түпкі тораптар кестесі желілік құрылғылардың нақты белсенділігін көрсететін сенімді аналитикалық құрал болып табылады. Бұл кесте арқылы әрбір IP мекенжайдың желімен қалай әрекеттескені, қандай порттарды пайдаланғаны, қанша дерек алмасқаны және олардың желідегі рөлі нақты бағаланады. Талдау Friday-WorkingHours.pcap түсіру файлы негізінде жүргізілді, онда Ethernet, IPv4, TCP және UDP хаттамаларын қамтитын бірнеше ондаған бірегей IP мекенжайлар тіркелген.

Жоғары белсенділік танытқан тораптардың қатарында 31.13.80.12 IP мекенжайы 9730 пакет және 5.24 МБ көлемінде дерек алмасқан. Бұл мекенжай HTTP және HTTPS порттары арқылы желіде қарқынды жұмыс істейді және оның O-RAN архитектурасында маңызды торап екенін анық көрсетеді. Сол сияқты, 31.13.80.36 IP мекенжайы 6272 пакет пен 3 МБ деректі 443-порт арқылы тасымалдаған, бұл оның шифрланған байланыстарға жауапты екенін айғақтайды.

Бұдан бөлек, желідегі кейбір тораптардың белсенділігі қалыптыдан ауытқыған. Мысалы, 31.13.80.8 мекенжайы бастапқыда аз белсенділік танытқанымен, мұндай тораптан кенет өсетін трафик SYN flood секілді шабуылдардың белгісі болуы мүмкін. Ал 31.13.77.2 және 31.13.77.12 IP мекенжайлары тек 443-порт арқылы байланыс орнатып, аз көлемде дерек алмасқанымен, олардың белсенділігі күрт артса, бұл да DDoS шабуылының белгісіне айналуы ықтимал.

Жалпы алғанда, түпкі тораптар кестесі желідегі құрылғылардың өзара әрекетін сенімді түрде бақылауға, күдікті белсенділіктерді нақты айқындауға және желіні автоматты қорғауға арналған AI/ML модельдерін нақты деректермен қамтамасыз етуге мүмкіндік береді. Бұл O-RAN желісінің қауіпсіздігін күшейтіп, киберқауіптерге қарсы тұру қабілетін арттырады.



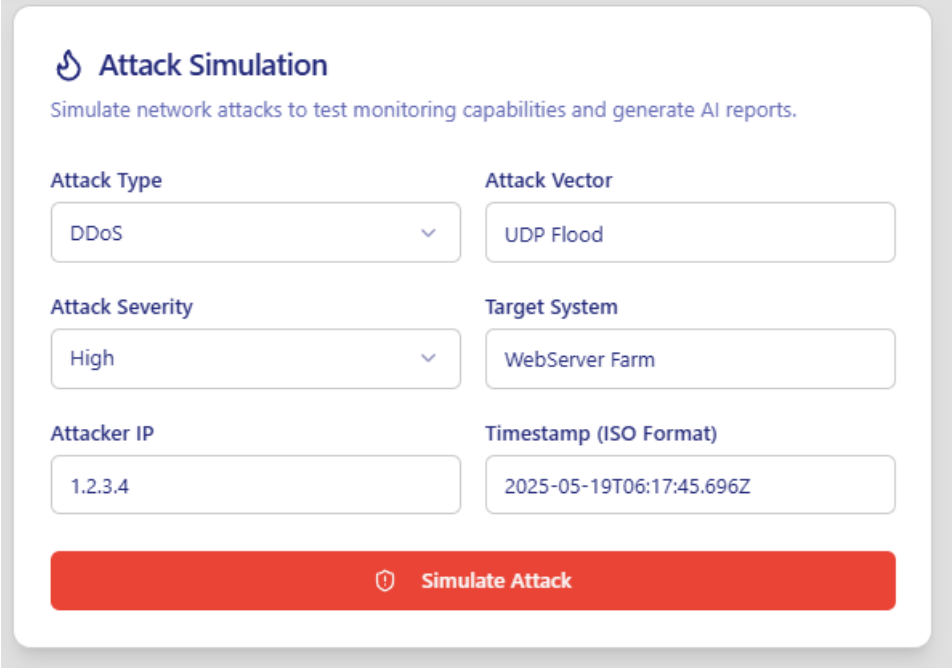
3.6-сурет – Нағызғы уақыттағы трафиктік график

Real-time Traffic Monitor графигі желідегі трафиктің уақыт бойынша динамикасын нақты бақылауға мүмкіндік береді. Бұл график арқылы секундына

пакеттер саны (Packets/sec) және белгілі бір уақыт аралығында жіберілген деректер көлемі (Data Volume, MB) көрсетіледі. Мұндай визуализация желідегі аномалияларды, соның ішінде DDoS шабуылдарының белгілерін ерте анықтау үшін маңызды құрал ретінде қолданылады.

Талдау барысында X осінде уақыт (00:00–08:41 аралығы, әр 5 минут сайын), ал Y осінде бір жағынан пакеттер саны, екінші жағынан деректер көлемі көрсетілген. Бақылау нәтижелері бойынша трафиктің белсенділігі айтарлықтай өзгеріп отырған. Мысалы, секундына пакеттер саны 2000-нан 7000-ға дейін тербеліп тұрса, деректер көлемі шамамен 3 МБ-тан 9 МБ-қа дейін жеткен. Атап айтқанда, 00:20 мен 08:41 уақыттарында трафиктің күрт артуы байқалған, бұл DDoS шабуылы немесе жүйелік жүктеменің кенеттен өсуі болуы мүмкін. Ал 08:14 кезінде трафиктің айтарлықтай азаюы желілік ақауларды немесе қорғаныс жүйелерінің жұмысын көрсетуі ықтимал.

Трафиктің жалпы сипаты тұрақты, бірақ мерзімді ауытқулар корпоративтік желілердегі қалыпты белсенділік циклдерін де көрсетуі мүмкін. Дегенмен, жоғары жүктеме сәттерінде (мысалы, 7000 пакет/сек асқанда) SYN flood немесе UDP flood сияқты шабуылдардың ықтималдығы күшейеді. Осы себепті 08:41 уақытындағы шың қосымша талдауды қажет етеді. Сонымен қатар, егер осындай шыңдар белгілі бір уақыт аралығында қайталанып отырса, бұл желілік ресурстарды жоспарлы түрде сарқуға бағытталған DDoS шабуылының белгісі болуы мүмкін.



3.7-сурет – Шабуыл симулициясы

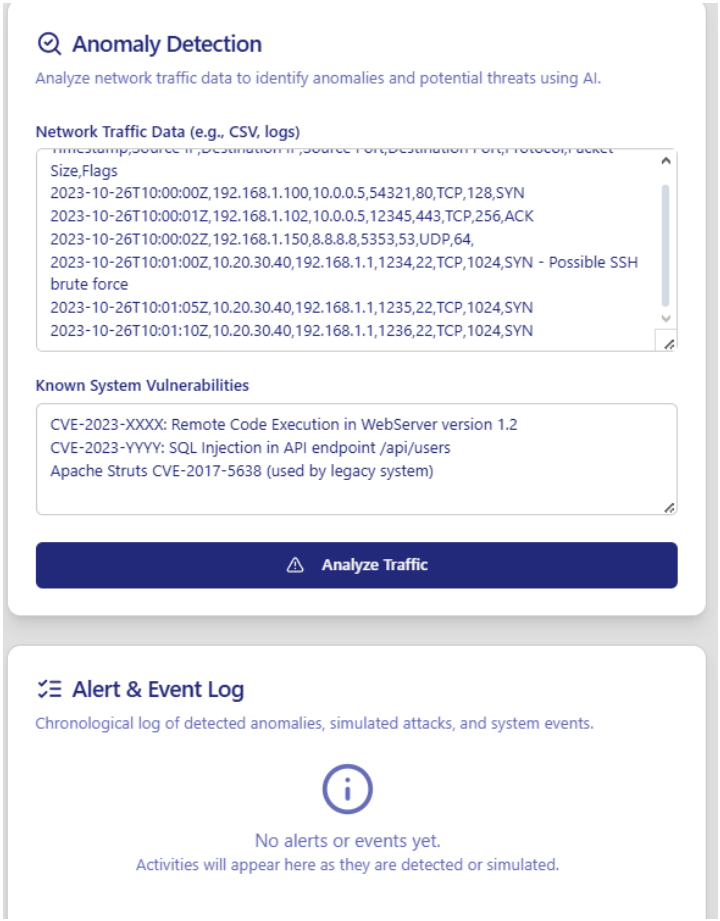
Шабуыл симуляциясы интерфейсі – АРАЖ желісінің қауіпсіздік жүйелерін сынау және ықтимал шабуылдарға қарсы әрекет ету қабілетін бағалау үшін маңызды құрал болып табылады. Бұл жүйе нақты уақытта ТСТШ шабуылдарын

қауіпсіз жағдайда модельдеуге мүмкіндік береді. Сонымен қатар, шабуыл параметрлерін икемді түрде реттеуге, олардың әсерін жан-жақты талдауға және желі инфрақұрылымының әрекетін бақылауға жағдай жасайды. Мұндай тәсіл желінің осал тұстарын дер кезінде анықтап, алдын ала қорғаныс шараларын әзірлеуге ықпал етеді.

Интерфейс бірнеше маңызды элементтерден тұрады. Біріншіден, пайдаланушы шабуыл түрін таңдайды, бұл жағдайда ТСТШ симуляциясы орындалады. Екіншіден, шабуыл бағыты (векторы) ретінде UDP Flood белгіленеді, ол серверлік ресурстарды артық жүктеу арқылы қызмет көрсетуді бұғаттауға бағытталған. Үшіншіден, қауіп деңгейі жоғары (critical) болып орнатылады, бұл жүйенің күрделі жағдайларға төзімділігін бағалауға мүмкіндік береді. Сонымен қатар, шабуылдаушының IP мекенжайы (мысалы, 1.2.3.4) көрсетіледі, ал мақсатты жүйе ретінде WebServer Farm таңдалады – бұл серверлік инфрақұрылымды нақты шабуылға ұқсас жағдайда модельдеуге мүмкіндік береді.

Симуляция үдерісі «Simulate Attack» батырмасын басу арқылы іске қосылады. Осы әрекеттен кейін жүйе жасанды трафикті қалыптастырады, оны Firebase арқылы тіркеп, ORAN Defender платформасында визуализациялайды. Бұл платформа шабуыл белсенділігін уақыттық кестелер арқылы бейнелейді, аномалияларды анықтау туралы хабарламалар мен шабуылдың егжей-тегжейлі сипаттамаларын ұсынады. Осы деректер кейінгі талдауға және қауіпсіздік стратегияларын жетілдіруге негіз болады.

Қорытындылай келе, шабуыл симуляциясы интерфейсі – желінің қорғаныс тетіктерін тексеруге, қауіптерге жедел әрекет етуге және ЖИ/МО негізіндегі анықтау жүйелерімен интеграциялау арқылы қауіпсіздікті кешенді түрде басқаруға арналған сенімді құрал. ТСТШ желісінің тұрақтылығы мен қауіпсіздігін қамтамасыз етуде бұл әдістің орны ерекше.



3.8-сурет – Аномалияны анықтау және оқиғалар мен ескертулер журналы

Аномалияны Анықтау – АРАЖ желісінің қауіпсіздік деңгейін арттыруға бағытталған жасанды интеллект негізіндегі заманауи талдау жүйесі. Бұл интерфейс желілік трафик деректерін талдау арқылы аномалиялар мен ықтимал қауіптерді автоматты түрде анықтауға мүмкіндік береді. Сонымен қатар, жүйенің осал тұстарын көрсету арқылы шабуылдарға қарсы алдын алу шараларын қабылдауға жағдай жасайды.

Желілік трафикті талдау - пайдаланушы CSV немесе лог файлдар форматындағы деректерді жүктей алады. Жүктелген жазбалар келесі атрибуттардан тұрады: уақыт белгісі (timestamp), дереккөз IP және мақсат IP мекенжайлары, порттар, қолданылған желілік хаттамалар, пакет өлшемі және флагтар.Мысалы:2023-10-26T10:01:05Z, 10.20.30.40, 192.168.1.1, 1235, 22, TCP, 1024,SYN-PossibleSSH,brute,force.Бұл жазба SSH брут-форс шабуылының мүмкін екенін көрсетеді. Мұндай деректер ЖИ жүйесі арқылы талданып, күдікті әрекеттердің сипаты анықталады.

Осы мәліметтер шабуыл векторлары мен шабуылдаушының жүйеге кіру жолдарын модельдеуге көмектеседі. Сонымен бірге, талдауға арналған «Analyze Traffic» батырмасы арқылы ЖИ моделін белсендіруге болады. Бұл әрекет нәтижесінде жүйе нақты уақытта аномалияларды анықтап, қауіптерді бағалай алады.

Оқиғалар мен ескертулер журналы - анықталған шабуылдар, жүйелік оқиғалар және ескертулер хронологиялық тәртіппен тіркеледі. Қазіргі сәтте журнал бос болса да, симуляция немесе нақты трафик талданған соң оқиғалар автоматты түрде осы жерде көрініс табады.

Ескерту Конфигурациясы интерфейсі — желілік трафиктегі ауытқулар мен имитациялық шабуылдарды бақылауға арналған, дабылдар мен хабарландыру параметрлерін басқаруды қамтамасыз ететін құрал. Бұл интерфейс пайдаланушыға әрекет шектерін орнатуға, қауіп төндіруі мүмкін IP мекенжайларын қара тізімге қосуға, сондай-ақ анықталған қауіптер туралы хабарламаларды қосуға немесе өшіруге мүмкіндік береді. Мұндай функциялар жүйенің қауіпсіздік деңгейін арттыруға және кибершабуылдарға жедел жауап беруге жағдай жасайды.

Желілік жүктеме шегі параметрінде пайдаланушы секундына желі арқылы өтетін пакет санының шекті мәнін орната алады. Егер нақты уақыттағы трафик осы межеден асып кетсе, жүйе автоматты түрде ескерту береді. Қазіргі уақытта шекті мән 1000 пакет/секунд болып орнатылған, бұл көбінесе ТСТШ шабуылдарын ерте кезеңде анықтауға тиімді мүмкіндік береді.

Бұған қоса, интерфейс құрамында IP мекенжайларының қара тізімі бар. Бұл тізімге желі трафигінде күдік тудыратын IP мекенжайлары енгізіледі. Егер осы мекенжайлардан келетін трафик анықталса, жүйе дереу қауіп туралы хабарлайды. Қазіргі таңда тізімге 10.0.0.1 және 203.0.113.45 IP мекенжайлары қосылған. Бұл IP-лер ықтимал зиянды әрекеттердің көзі ретінде қарастырылады.

Сонымен қатар, хабарландыру параметрлері бөлімі маңызды рөл атқарады. Мұнда пайдаланушы желідегі қалыптан тыс әрекеттер мен шабуылдарды модельдеу кезінде автоматты хабарландыруларды қосып не өшіре алады. Атап айтқанда, желідегі аномалияларды анықтау үшін ЖИ/МО технологияларын қолданатын ескерту жүйесін белсендіруге болады. Қазіргі жағдайда бұл мүмкіндік қосулы күйде тұр. Дәл осылай, шабуылдарды модельдеу барысында да хабарландырулар алуға болады, бұл да қосулы режимде іске қосылған. Бұл параметрлер пайдаланушыға шабуылдарға дер кезінде жауап беруге көмектеседі және жүйені шынайы жағдайларға бейімдеуге ықпал етеді.

3.3 Нәтижелерді талдау және жүйенің тиімділігін бағалау

Жүйе өз жұмысында Friday-WorkingHours атты pcap форматындағы тарихи деректер файлын пайдаланады. Аталған деректер жиынтығы 2024 жылға тиесілі және 9,9 миллионнан астам желілік пакетті қамтиды. Бұл мәліметтер қалыпты желілік трафикті де, сондай-ақ түрлі типтегі кибершабуылдарды да модельдеуге мүмкіндік берді. Осылайша, жүйе нақты шабуыл сценарийлерін қайта жаңғырту арқылы қауіптерді дәл талдауға жол ашты.

Талдау барысында бірнеше негізгі аспектілерге назар аударылды. Біріншіден, енгізу/шығару (Input/Output) графиктері бойынша жүргізілген талдау нәтижесінде ТСТШ шабуылдарына тән белсенділіктің күрт өсуі тіркелді. Бұл шабуылдардың трафик көлеміне әсер ететіні анық байқалды.

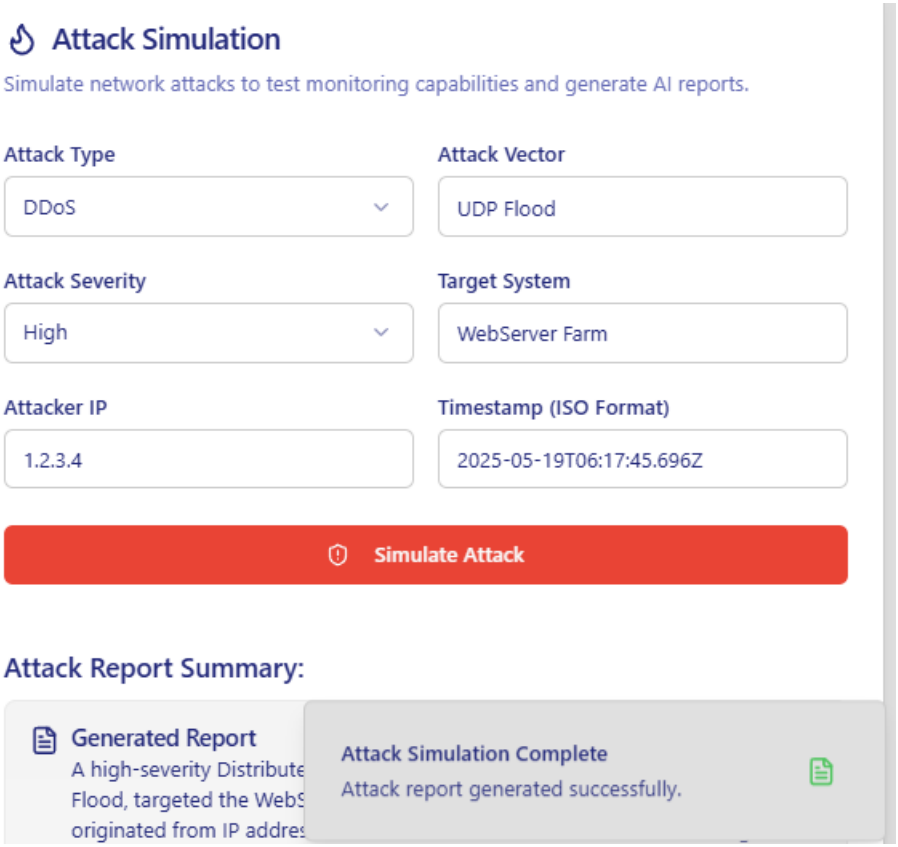
Екіншіден, хаттама иерархиясы қарастырылды. Зерттеу нәтижелері бойынша TCP хаттамасы жалпы пакеттердің 90 пайызынан астамын құрады. Мұндай басымдық оның SYN flood тәрізді шабуыл түрлеріне әлсіздігін көрсетеді. Демек, бұл желі қауіпсіздігін арттыру үшін TCP протоколына қатысты қосымша қорғаныс шараларын қарастыру қажеттігін айқындайды.

Үшіншіден, соңғы нүктелер (Endpoints) бойынша талдау жүргізілді. Бұл қадам желіде ең белсенді әрекет ететін IP мекенжайларын айқындауға және олардың мінез-құлқын бақылауға мүмкіндік берді. Мұндай әдіс ықтимал зиянды түйіндерді ерте анықтап, тиісті қарсы әрекеттерді уақтылы іске асыру үшін маңызды рөл атқарады.

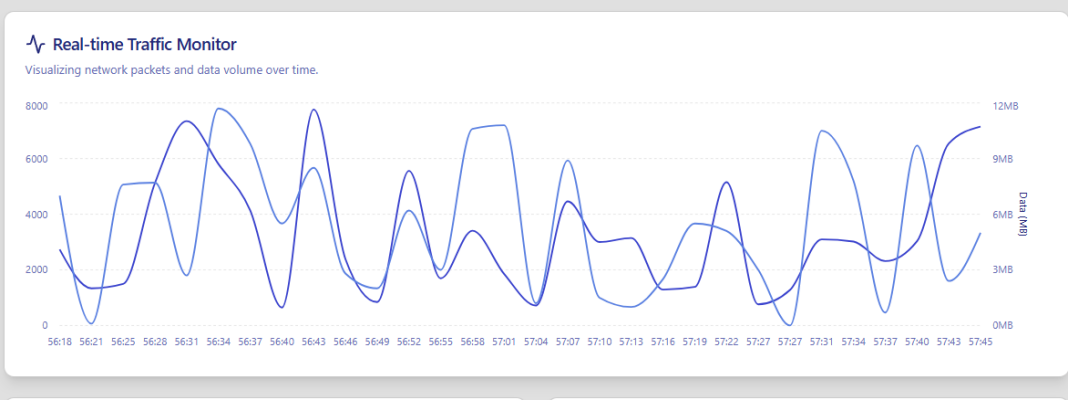
Бұдан кейін алынған деректер Firebase платформасына біріктіріліп, визуализация процесі жүргізілді. Wireshark арқылы алынған мәліметтер өңделіп, ORAN Defender интерфейсіне енгізілді. Бұл мүмкіндік нақты уақыт режимінде желіні бақылауды қамтамасыз етіп, қауіптерді анықтау және басқару процесін автоматтандыруға жағдай жасады.

Аталған зерттеу нәтижесінде бірнеше маңызды жетістіктерге қол жеткізілді. Ең алдымен, уақыт бойынша трафик белсенділігінің графиктері құрылды. Бұл визуалды мәліметтер желідегі қалыптан тыс әрекеттерді анықтауға мүмкіндік береді. Сонымен қатар, IP мекенжайлары, порттар және хаттамалар бойынша егжей-тегжейлі деректер қамтылған кестелер жасалды. Олар күдікті қосылымдарды тереңірек талдау үшін пайдаланылды.

Сондай-ақ, трафикті хаттамалар мен дереккөздерге қарай жіктейтін диаграммалар әзірленді. Мұндай визуализация желінің жалпы әрекет сипатын бақылауға, сондай-ақ қайталанатын шаблондарды немесе ауытқуларды анықтауға мүмкіндік береді. Бұл өз кезегінде кибершабуылдарға қарсы алдын ала шаралар қабылдау үшін тиімді негіз қалыптастырады.



3.9-сурет – ТСТШ шабуылын симмулициялау

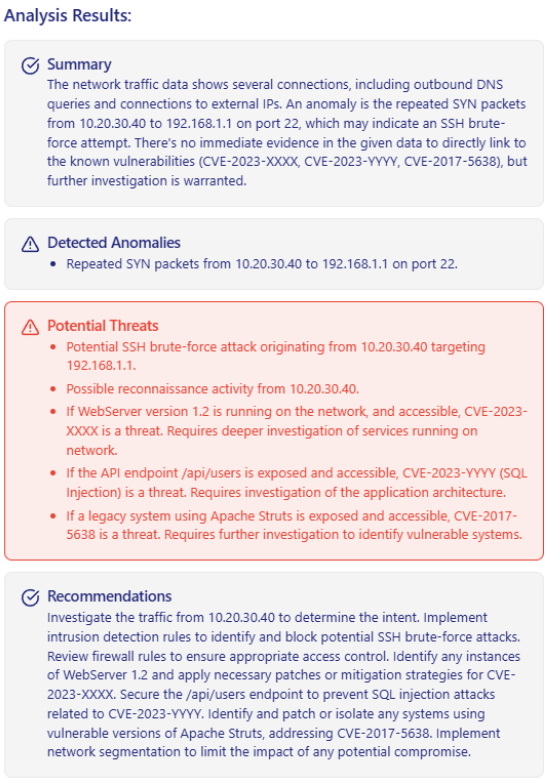


3.10-сурет – Шабуыл симуляцияланғаннан кейінгі нағызғы уақыттағы трафик

Эксперименттік бөлімде Firebase Studio платформасы арқылы жасанды интеллект пен визуализацияны қолдана отырып, ORAN Defender жүйесі негізінде желілік трафикті бақылау механизмі жүзеге асырылды. Бұл жүйе ТСТШ шабуылдарын анықтауға бағытталған және оның тиімділігін бағалау мақсатында нақты шабуыл түрлерін модельдеу әдісі қолданылды. Жүргізілген модельдеу барысында UDP Flood және SYN Flood тәрізді кибершабуыл түрлері іске қосылып, жүйенің қауіптерді тану қабілеті мен пайдаланушыны уақтылы хабардар ету механизмдері тексерілді.

Модельдеу процесі бірнеше кезеңнен тұрды. Ең алдымен, Firebase интерфейсі арқылы шабуылдың түрі мен векторы таңдалды. Содан кейін шабуылдаушы тараптың мақсатты жүйесі және оның IP мекенжайы нақты көрсетілді. Шабуылды бастау үшін Simulate Attack батырмасы пайдаланылды. Осы әрекеттен кейін шабуылға тән жасанды трафик Firebase жүйесіне жіберіліп, OPAN Defender интерфейсінде бейнеленді. Жасанды интеллект пен машиналық оқыту элементтеріне негізделген модель трафиктің динамикасын сараптап, желі әрекетіндегі ауытқуларды нақты анықтады.

Эксперименттің келесі кезеңінде нақты уақыт режимінде трафик белсенділігін бақылау жүргізілді. Тиісті мониторинг графигі шабуылға дейінгі, шабуыл кезіндегі және одан кейінгі желі трафигінің өзгерістерін тіркеуге мүмкіндік берді. Мысалы, UDP Flood шабуылы жүргізілген сәтте секундына берілетін пакет санының едәуір артқаны байқалды. Әдеттегі шамамен 2000 пакет/сек көрсеткіші күрт өсіп, 7200 пакет/сек деңгейіне жетті. Сонымен қатар, деректер көлемі де елеулі өзгерді. Алғашында 3 МБ шамасындағы мәліметтер көлемі шабуыл кезінде 9 МБ-қа дейін артты. Бұл көрсеткіштер ТСТШ шабуылына тән сипаттамаларды дәлелдейді.



3.11-сурет – Талдау нәтижелері

Желілік трафикті талдау барысында бірнеше байланыс түрлері анықталды. Атап айтқанда, сыртқа бағытталған DNS сұраулары мен сыртқы IP мекенжайларына жасалған қосылымдар тіркелді. Дегенмен, негізгі назар аудартатын аномалия ретінде 10.20.30.40 IP мекенжайынан 192.168.1.1 IP

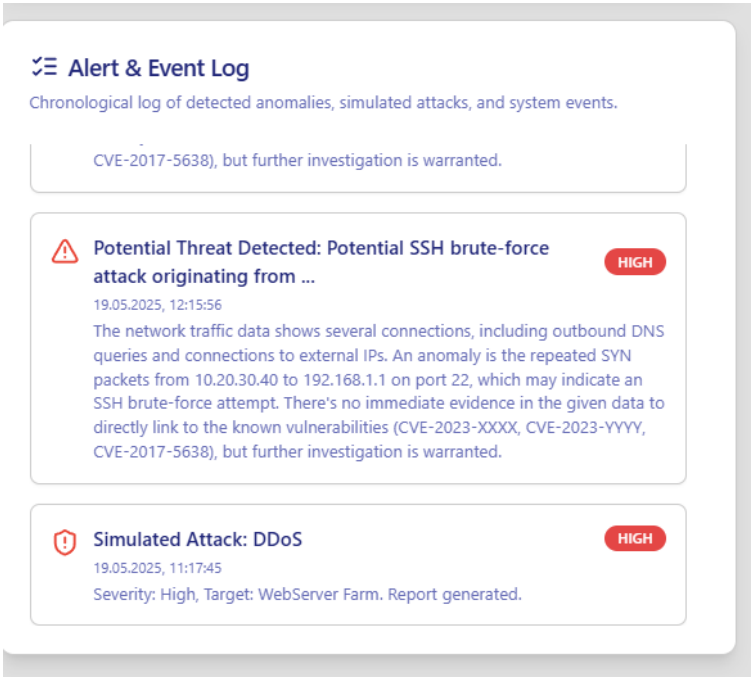
мекенжайының 22-портына қайталанатын SYN пакеттері тіркелді. Мұндай әрекет SSH Brute Force шабуылының ықтимал көрінісі ретінде қарастырылуы мүмкін.

Сонымен қатар, талданған деректерде желілік белсенділік белгілі осалдықтармен нақты байланыста болғаны анық байқалмайды. Бұл жағдай қосымша тергеу мен жүйелік аудитті қажет ететінін көрсетеді.

Талдау барысында анықталған негізгі ауытқу ретінде IP 10.20.30.40 мекенжайынан 192.168.1.1 серверінің SSH портына бағытталған қайталанатын SYN пакеттері тіркелді. Мұндай белсенділік SSH Brute Force шабуылының ықтимал белгісі ретінде қарастырылады.

Ықтимал қауіптерге келер болсақ, біріншіден, SSH Brute Force шабуылының жүзеге асуы мүмкін. Бұл жағдайда шабуылдаушы IP 10.20.30.40 мекенжайынан SSH серверге қол жеткізуге тырысады. Екіншіден, желілік барлау әрекеттері байқалуы мүмкін. Мұндай жағдайда IP 10.20.30.40 мекенжайы желідегі белсенді түйіндерді сканерлеу арқылы мақсатты ресурстар жайлы ақпарат жинауға тырысуы ықтимал.

Жалпы алғанда, бұл талдау ORAN Defender жүйесінің желілік трафиктегі ауытқуларды тиімді анықтай алатынын көрсетті. Жүйе күдікті әрекеттерді айқындап, пайдаланушыны ықтимал қауіптер туралы хабардар етеді. Мұндай функционалдық қасиеттер АРАЖ инфрақұрылымын кибершабуылдардан қорғау үшін маңызды құрал екендігін дәлелдейді.



3.12-сурет – Дабыл белгілері

Желілік трафикті талдау барысында SSH Brute Force шабуылының ықтималдығы анықталды. Бұл шабуыл 10.20.30.40 IP мекенжайынан 192.168.1.1

IP мекенжайының 22-портына бағытталған қайталанатын SYN пакеттерімен сипатталады. Мұндай желілік белсенділік SSH протоколына күшпен ену әрекетінің типтік белгісі болып табылады. Анықталған оқиға қауіптің жоғары деңгейіне жатқызылғанымен, берілген шабуыл белгілі осалдықтармен тікелей байланысты емес. Бұл жағдай шабуылдың жаңа немесе беймәлім әдістемеге негізделгенін көрсетуі мүмкін және қосымша тергеуді талап етеді.

Анықталған қауіптерге қатысты SSH Brute Force шабуылы негізгі назарға алынды. Талдау нәтижесінде 10.20.30.40 IP мекенжайынан 22-портқа бағытталған SYN пакеттерінің үздіксіз легі тіркелді. Бұл деректер SSH протоколын пайдалана отырып, заңсыз қол жеткізуге талпыну фактісін көрсетуі мүмкін. Анықталған әрекет жоғары қауіп деңгейіне ие болғандықтан, әкімшілік тарапынан жедел әрекет етуді талап етеді.

Трафикті тереңірек зерттеу барысында ТСТШ шабуылына ұқсас модельдеу де жүргізілді. Атап айтқанда, UDP Flood түріндегі шабуыл WebServer Farm инфрақұрылымын мақсат етті. Бұл модельдеудің мақсаты жүйенің нақты қауіп-қатер жағдайында қалай әрекет ететінін бағалау болды. Жүргізілген модельдеу сәтті аяқталды, бұл ORAN Defender жүйесінің жұмыс қабілеттілігін растайды.

Жиналған деректерге сүйене отырып, жүйенің аномалияларды нақты уақыт режимінде табуға қабілетті екені анықталды. SSH шабуылы кезінде қайталанатын SYN пакеттерінің пайда болуы мен олардың жүйелі сипаты шабуылдың барысын дәлелдеді. Сонымен қатар, жасанды интеллект пен машиналық оқыту технологияларының интеграциясы желілік трафиктегі ауытқуларды жедел әрі тиімді анықтауға мүмкіндік берді. Бұл жүйеге шабуыл түрін, бағытын және қарқындылығын нақты сипаттауға жағдай жасайды.

Жалпы алғанда, қауіп деңгейінің "жоғары" ретінде бағалануы оқиғаның маңыздылығын көрсетеді және әкімшілерге шұғыл шешім қабылдау қажеттігін айқындайды. Мұндай жіктеу жүйенің басқарушылық әрекеттерін жылдам ұйымдастыруға ықпал етеді.

ҚОРЫТЫНДЫ

Бұл дипломдық жұмыс АРАЖ архитектурасының қауіпсіздік мәселелерін зерттеуге және жасанды интеллект негізінде қорғаныс механизмдерін әзірлеуге арналған. Зерттеу барысында АРАЖ желісінің ашықтығы мен модульдік құрылымына байланысты туындайтын қауіптер мен шабуыл түрлері жан-жақты қарастырылды. Жасанды интеллект пен машиналық оқытудың көмегімен желі трафигіндегі аномалияларды нақты анықтау және шабуылдар туралы дер кезінде ескерту мүмкіндігі зерттелді.

АРАЖ архитектурасының осал тұстары мен кибершабуыл түрлері талданды. ЖИ және МО әдістері арқылы желілік қауіпсіздікті арттыру жолдары қарастырылды. Жүйе ТСТШ, SSH Brute Force, UDP Flood сияқты шабуылдарды анықтай алды. Трафик Wireshark арқылы зерттеліп, Firebase платформасында визуализацияланды. Алынған нәтижелер жүйенің тиімділігін көрсетті.

Шабуылдарды анықтау алгоритмі толығымен орындалды, жүйе нақты қауіптерді танып, әкімшіге хабарлама жібере алды. Алайда шабуылдың алдын алу тетігі толығымен енгізілген жоқ, себебі оны іске асыру үшін қосымша серверлік ресурстар қажет болды. Сондықтан нақты тосқауыл қою функциясы қарастырылмады.

Жасанды интеллект құралдарын қолдана отырып желінің қауіпсіздік көрсеткіштері бағаланды, және бұл бөлім толығымен орындалды. Алынған нәтижелер жүйенің тиімділігін дәлелдеді.

Симуляциялық шабуылдар сәтті өткізілді, жүйе оларды анықтап, трафик өзгерістерін көрсетті. Бұл бөлік толық орындалды.

ORAN Defender веб-қосымшасы жасалды, ол нақты уақытта шабуылдарды бақылауға мүмкіндік береді. Қосымша жұмыс істейді, алайда толық интеграция үшін серверлерге тұрақты қолжетімділік қажет. Қорғаныс тетіктерін одан әрі күшейту қажет.

Жалпы алғанда, жұмыс мақсатына жетті. Жүйенің практикалық тиімділігі көрсетілді, әрі қарай дамыту үшін техникалық инфрақұрылым мен алгоритмдердің жетілдірілуі ұсынылады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Shen C. T. et al. Security threat analysis and treatment strategy for ORAN //2022 24th International Conference on Advanced Communication Technology (ICACT). – IEEE, 2022. – С. 417-422.

2 Baguer P. et al. Attacking O-RAN interfaces: threat modeling, analysis and practical experimentation //IEEE Open Journal of the Communications Society. – 2024.

3 Mimran D. et al. Evaluating the security of open radio access networks //arXiv preprint arXiv:2201.06080. – 2022.

4 Mimran D. et al. Security of open radio access networks //Computers & Security. – 2022. – Т. 122. – С. 102890.

5 Liyanage M. et al. Open RAN security: Challenges and opportunities //Journal of Network and Computer Applications. – 2023. – Т. 214. – С. 103621.

6 Hung C. F. et al. Security threats to xApps access control and E2 interface in O-RAN //IEEE Open Journal of the Communications Society. – 2024. – Т. 5. – С. 1197-1203.

7 Abdalla A. S., Marojevic V. End-to-end O-RAN security architecture, threat surface, coverage, and the case of the open fronthaul //IEEE Communications Standards Magazine. – 2024. – Т. 8. – №. 1. – С. 36-43.

8 Thiruvasagam P. K. et al. Open RAN: Evolution of architecture, deployment aspects, and future directions //arXiv preprint arXiv:2301.06713. – 2023.

9 Moudoud H., Cherkaoui S. Enhancing open RAN security with zero trust and machine learning //GLOBECOM 2023-2023 IEEE Global Communications Conference. – IEEE, 2023. – С. 2772-2777.

10 Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms //ACM SIGCOMM Computer Communication Review. – 2004. – Т. 34. – №. 2. – С. 39-53.

11 Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art //Computer networks. – 2004. – Т. 44. – №. 5. – С. 643-666.

12 Somani G. et al. DDoS attacks in cloud computing: Issues, taxonomy, and future directions //Computer communications. – 2017. – Т. 107. – С. 30-48.

13 Chang J. E. et al. Packet Continuity DDoS Attack Detection for Open Fronthaul in ORAN System //NOMS 2024-2024 IEEE Network Operations and Management Symposium. – IEEE, 2024. – С. 1-5.

14 Abou El Houda Z., Moudoud H., Brik B. Federated deep reinforcement learning for efficient jamming attack mitigation in O-RAN //IEEE Transactions on Vehicular Technology. – 2024. – Т. 73. – №. 7. – С. 9334-9343.

15 Abou El Houda Z., Moudoud H., Khoukhi L. Blockchain meets O-RAN: A decentralized zero-trust framework for secure and resilient O-RAN in 6G and beyond //IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). – IEEE, 2024. – С. 1-6.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

6В06201 «Телекоммуникация» білім беру бағдарламасы студенті
Базарбаев Ахмет Русланұлы
Дипломдық жұмысқа
СЫН-ПІКІР

Тақырыбы: **«Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру»**

Дипломдық жұмыс «Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру» тақырыбына ашық радио желілердің (O-RAN) киберқауіпсіздігін жасанды интеллект пен машиналық оқыту әдістері арқылы арттыру жолдары қарастырылған. Жұмыстың мақсат шабуылдарды анықтау, қауіпсіздікті бағалау және жетілдіру. Зерттеу нәтижесінде қолданылған модельдер телекоммуникациялық желілердің қауіпсіздігін арттыруға бағытталған нақты және тиімді шешімдер ұсынды.

Дипломдық жұмыста жасалған алгоритмдер мен модельдер симуляциялық ортада тексеріліп, нәтижелері талданған. Сонымен қатар, жасанды интеллект шешімдерін O-RAN желісіне енгізу кезіндегі қиындықтар анықталып, оларды шешу жолдары ұсынылған. Зерттеу жұмысы толық көлемде орындалған, мазмұны жүйелі құрылып техникалық талаптарға сай жасалынды. Графикалық материалдар (сызбалар, диаграммалар) тақырыппен тығыз байланысты. Студент берілген тапсырманы толық орындап, кәсіби дағдысы мен біліктілігін көрсетті.

Графикалық және мәтіндік материалдар МСТК талабына сәйкес жазылған. Бұл дипломдық жоба жоғарғы оқу орындарының талаптарына сай жеткілікті жоғары дәрежеде жазылған.

Жалпы, дипломдық жұмысқа «өте жақсы» (95%) деген баға, ал студент Базарбаев Ахмет Русланұлы 6В06201 Телекоммуникация білім беру бағдарламасының «Ақпараттық коммуникациялық технологиялар бакалавры» дәрежесіне лайықты деп санаймын.

Пікір беруші:
Ғылыми жетекшісі,
қауымд.профессор, PhD
Хабай А. _____
«26» 05 2025 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

6В06201 «Телекоммуникация» білім беру бағдарламасы студенті
Базарбаев Ахмет Русланұлы
Дипломдық жұмысқа
СЫН-ПІКІР

Тақырыбы: «**Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру**»

Дипломдық жұмыстың тақырыбы – «Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру» – заманауи телекоммуникациялық технологиялардың ең актуалды бағыттарының біріне, яғни ашық радиотүсетін желілердің киберқауіпсіздігін арттыру мәселесіне арналған. Жобалау тапсырмасы және зерттеу мақсаты нақты қойылған, ал қарастырылатын мәселелер — жасанды интеллект пен машиналық оқыту әдістерін қолдану арқылы шабуылдарды анықтау, желі қауіпсіздігін бағалау және оны жетілдіру болып табылады. Зерттеу барысында қолданылған жасанды интеллект және машиналық оқыту модельдері телекоммуникациялық желілердің қауіпсіздігін қамтамасыз етуге бағытталған практикалық тиімді шешімдер береді.

Дипломдық жұмыста әзірленген алгоритмдер мен модельдер симуляциялық ортада тексеріліп, нәтижелер талданған. Сонымен қатар, AI-шешімдерді O-RAN желісіне интеграциялау барысында туындайтын қиындықтар анықталып, ұсыныстар қарастырылған. Орындалған зерттеу көлемі жеткілікті, логикалық құрылымы сақталған, графикалық материалдар (сызбалар, диаграммалар) тақырыпқа сай, техникалық талаптарға сәйкес орындалған. Дипломдық жұмыста студент өзіне тапсырылған тапсырманы толық орындаған, қажетті дағдылар мен біліктілікті көрсеткен.

Жалпы, дипломдық жұмысқа «өте жақсы» (95%) деген баға, ал студент Базарбаев Ахмет Русланұлы 6В06201 Телекоммуникация білім беру бағдарламасының «Ақпараттық коммуникациялық технологиялар бакалавры» дәрежесіне лайықты деп санаймын.

Пікір беруші
Алматы энергетика және
байланыс университеты
профессоры. т.ғ.к.,
Чежимбаева К.С _____
«30» 05 2025 ж.

Қолтаңбаны растаймын
Подпись заверяю
Персоналды басқару жөніндегі департамент
Департамент по управлению персоналом
қызметі
«30» 05 2025 ж.

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Базарбаев Ахмет Русланұлы

Тақырыбы: Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру

Жетекшісі: Сұңғат Марксұлы

1-ұқсастық коэффициенті (30): 2.9

2-ұқсастық коэффициенті (5): 1.3

Дәйексөз (35): 1.4

Әріптерді ауыстыру: 0

Аралықтар: 0

Шағын кеңістіктер: 0

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

2025-05-20

Күні *Кафедра меңгерушісі*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Базарбаев Ахмет Русланұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 2.9

Коэффициент Подобия 2: 1.3

Микропробелы: 0

Знаки из здругих алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-05-20

Дата *Заведующий кафедрой*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Базарбаев Ахмет Русланұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Жасанды интеллект арқылы O-RAN желісінің қауіпсіздік механизмдерін жетілдіру

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 2.9

Коэффициент Подобия 2: 1.3

Микропробелы: 0

Знаки из здругих алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-05-20

Дата

Сұңғат Марксұлы

проверяющий эксперт