https://doi.org/10.58805/itamns.V.1(32)-65

5G ЖӘНЕ 6G ЖЕЛІЛЕРІНДЕГІ ҚАЗІРГІ ҚАУІПТЕР МЕН ОСАЛДЫҚТАРДЫ ТАЛДАУ, ШАБУЫЛДАРДЫ ЖІКТЕУ ЖӘНЕ ЖЕЛІЛІК ТРАФИК ДЕРЕКТЕРІ БОЙЫНША АНЫҚТАУ ӘДІСТЕРІН БАҒАЛАУ

С.К. Батырхан[1,2]✉, Б.С. Ахметов[3]

[1] әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2] Нархоз Университеті, Алматы, Қазақстан
[3] Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан
✉ Корреспондент-автор: sake.batyrkhan@gmail.com

Received: 11 March 2026
Accepted: 29 July 2026
Published: 30 September 2026
Citation: S.K. Batyrkhan, et al. « 5G ЖӘНЕ 6G ЖЕЛІЛЕРІНДЕГІ ҚАЗІРГІ ҚАУІПТЕР МЕН ОСАЛДЫҚТАРДЫ ТАЛДАУ, ШАБУЫЛДАРДЫ ЖІКТЕУ ЖӘНЕ ЖЕЛІЛІК ТРАФИК ДЕРЕКТЕРІ БОЙЫНША АНЫҚТАУ ӘДІСТЕРІН БАҒАЛАУ ». Information Technologies, Automation, and Management in Natural Sciences, vol. 1, no. 32, Sept. 2026, doi: https://doi.org/10.58805/itamns.V.1(32)-65
License CC BY 4.0

Жұмыста желілік трафик пен QoS телеметрия деректерінің негізінде network slicing жағдайында 6G желілеріндегі қауіптер мен осалдықтарды талдау әдістемесі қарастырылады. Киылу параметрлерін, жүктеме режимдерін және қызмет көрсету сапасын сипаттайтын аралас белгілердің жиынтығы қолданылады және шабуыл түрлерін көп класты жіктеу міндеті тұжырымдалады. Logistic Regression, Random Forest және XGBoost модельдерін салыстыру орындалған, бұл ретте кестелік деректер үшін градиентті бустингтің практикалық тиімділігі көрсетілген. Қиықтардың түрлері арасындағы домендік ығысу кезінде детектордың төзе алушылығы қосымша бағаланады, бұл 5G-де және 6G-де пайдалану сценарийлерінің вариантты лығын көрсетіп отыр. Сондай-ақ модельдің сенімділік шегінің негізінде белгісіз шабуылдар UNKNOWN класына бөлінетін open-set қойылымы қарастырылады. Эксперименттің ұсынылған құрылымы жаңғыртылуға бағытталған және нақты 5G мен 6G трассаларында кейініректе деректерді алмастыру және нәтижелерді өзектендіру үшін шаблон болып қызмет ете алады.

Түйін сөздер: 5G, 6G, желі қауіпсіздігі, басып кіруді анықтау, шабуылдарды жіктеу, желілік трафик, телеметрия, машиналық оқыту.

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ И УЯЗВИМОСТЕЙ СЕТЕЙ 5G И 6G, КЛАССИФИКАЦИЯ АТАК И ОЦЕНКА МЕТОДОВ ОБНАРУЖЕНИЯ ПО ДАННЫМ СЕТЕВОГО ТРАФИКА.

С.К. Батырхан[1,2]✉, Б.С. Ахметов[3]

[1] Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[2] Университет Нархоз, Алматы, Казахстан
[3] Казахский национальный педагогический университет им. Абая, Алматы, Қазахстан
✉ e-mail: sake.batyrkhan@gmail.com

В работе рассматривается методика анализа угроз и уязвимостей в сетях 6G в условиях network slicing на основе данных сетевого трафика и телеметрии QoS. Используется набор смешанных признаков, характеризующих параметры среза, нагрузочные режимы и качество обслуживания, и формулируется задача многоклассовой классификации типов атак. Выполнено сопоставление моделей Logistic Regression, Random Forest и XGBoost, при этом показана практическая эффективность градиентного бустинга для табличных данных. Дополнительно оценивается переносимость детектора при доменном сдвиге между типами срезов, что отражает вариативность сценариев эксплуатации в B5G и 6G. Также рассматривается постановка open-set, в которой неизвестные атаки выделяются в класс UNKNOWN на основе порога уверенности модели.

Предложенная структура эксперимента ориентирована на воспроизводимость и может служить шаблоном для последующей замены данных и актуализации результатов на реальных 5G и 6G трассах.

Ключевые слова: 5G, 6G, безопасность сетей, обнаружение вторжений, классификация атак, сетевой трафик, телеметрия, машинное обучение.

ANALYSIS OF CURRENT THREATS AND VULNERABILITIES IN 5G AND 6G NETWORKS, ATTACK CLASSIFICATION, AND EVALUATION OF DETECTION METHODS USING NETWORK TRAFFIC DATA

S.K. Batyrkhan[1,2]✉, B.S. Akhmetov[3]

[1] *Al-Farabi Kazakh National University, Almaty, Kazakhstan*
[2] *Narxoz University, Almaty, Kazakhstan*
[3] *Abai Kazakh National Pedagogical University, Almaty, Kazakhstan*
✉ *e-mail: sake.batyrkhan@gmail.com*

This paper presents an experimental methodology for analyzing threats and vulnerabilities in 6G network slicing using network-traffic features and QoS telemetry. A mixed set of slice-level and network-condition variables is employed to formulate a multi-class attack-type classification task. Logistic Regression, Random Forest, and XGBoost are compared, and gradient boosting is highlighted as an effective approach for tabular security data. We further evaluate cross-slice generalization under domain shift across different slice types, reflecting the variability expected in B5G and 6G deployments. An open-set setting is also considered, where unseen attacks are handled by assigning an UNKNOWN label based on a confidence threshold. The proposed pipeline is designed for reproducibility and can be reused as a template when replacing synthetic data with real 5G and 6G traffic traces and updating the reported results.

Keywords: 5G, 6G, network security, intrusion detection, attack classification, network traffic, telemetry, and machine learning.

Кіріспе. 5G желілері цифрлық сервистердің негізгі инфрақұрылымы болып та алды, ал 6G зерттеулері виртуализацияның, перифериялық есептеулердің және желінің бағдарламалық жасақтамамен анықталатын функцияларының рөлін күшейте түсуде. Бұл өзгерістер архитектураның күрделілігін арттырады және, сервистердің құпиялылығы, тұтастығы мен қол жетімділігі үшін тәуекелдерді қоса алғанда, шабуылдардың бетін кеңейтеді. 6G қауіпсіздігі мен бейресмилігі бойынша заманауи шолулар қосылымдардың жылдамдығы мен тығыздығының өсуімен қатар, радио қол жетімділік, ядро және сервистер деңгейлерінде қауіптердің артып келе жатқанын, сондай-ақ автоматтандырудың қауіпсіздікке әсерінің артып келе жатқанын баса көрсетіп отыр. Бұл 6G келешекті технологиялары мен сын-қатерлері бойынша [1], 6G edge қауіпсіздік бойынша [2] жұмыстарда және 6G қауіпсіздік қабаттары бойынша жүйелі шолуларда [3] көрсетілген.

5G және 6G-де жеке және дербес емес деректерді басқаруға ерекше назар аударылады, өйткені мультисервистік сценарийлер мен деректерді таратылған өңдеу жылыстаулар мен корреляциялық шабуылдардың жаңа арналарын жасайды. Әдебиеттерде бұл желілік трафикті мониторингтеумен және шабуылдардың мінез-құлық белгілерімен тығыз байланысты бағынышсыз зерттеу саласы ретінде қарастырылады [4]. Мұнымен қатарлас, 5G қауіпсіздігін қамтамасыз ету үшін жасанды интеллект әдістерін қолдану бағыты дамып келеді, мұнда трафикті автоматтандырылған талдауға, ауытқушылықтарды анықтауға және оқыс оқиғаларға жауап беру уақытын азайтуға баса назар аударылады [5].

5G мен болашақ 6G-дің негізгі технологиялық айырмашылығы - желіні көрсетілетін қызметтердің әртүрлі кластарына логикалық бөлуді қамтамасыз ететін network slicing болып табылады. Бұл ретте қиықтарды оқшаулау, ресурстарды бірлесе пайдалану және SDN мен NFV-ның өзара әрекеттесуі оқшаулау және басқарушы жазықтықтарға шабуыл жасау саясаттарын бұзуды қоса алғанда, шабуылдардың өзгеше векторларын қалыптастырады. Бұл мәселелер network slicing қауіпсіздік бойынша шолуда [6], сондай-ақ мұнда қауіпсіздік қиықтарды «интеллектуалды» басқарудың бөлігі ретінде қарастырылатын жұмыстарда жүйелі түрде жинақталады [7].

Практикалық қорғаныс және мониторинг механизмдеріне бағытталған шолулар мен қолданбалы зерттеулер шеңберінде типтік шабуыл векторлары мен жұмсарту шаралары қосымша сипатталған [8-9].

Кідіріс пен сенімділікке, соның ішінде MEC сценарийлерінде қойылатын талаптары қатаң сервистер үшін, желілік трафик пен QoS телеметрия деректері бойынша шабуылдарды уақтылы анықтау сындарлы. 5G-дегі MEC-бағдарланған use case бойынша шолулар осалдықтардың желілік метрикалардың, жүктеме режимдерінің және қауіпсіздік механизмдерінің үйлесімінде көрініс табатынын жиі көрсетіп отыр, бұл трафикті талдауды бақылаудың негізгі практикалық құралдарының біріне айналдырып отыр [10]. 5G ядросының деңгейінде PFCP-жазықтықты қоса алғанда, хаттамалық осалдықтарды талдаудың өзектілігі көрсетіліп отыр, бұл IDS-ты трафик бойынша құруды қосымша ынталандыруда [11]. Қиықтар бойынша зерттеулерде сонымен қатар сервистердің осалдықтары мен компрометация қатерлерін азайтудың практикалық амал-жолдары талқыланады [12], ал 5G core үшін қол жетімді датасеттер IDS бойынша қалпына келетін эксперименттер үшін негіз ретінде қолданылады [13]. Бұл ретте дұрыс модельдер құру үшін іріктеме мен валидацияны дайындау кезеңдерінде деректердің жылыстауын болдырмау маңызды, өйткені олар сапаны шамадан тыс бағалауға және нәтижелерге төзе алушылықтың төмендеуіне алып келеді [14].

Оқытатын іріктемеде жоқ белгісіз және жаңа шабуылдарды тауып анықтау бөлек мәселе болып табылады. Салыстырмалы зерттеулер классикалық амал-тәсілдердің белгісіз кластармен нашар жұмыс істейтіндігін және тапсырманың ашық қойылуын немесе сенімділікті калибрлеудің арнайы механизмдерін қажет ететіндігін көрсетіп отыр [15]. Энергетикалық критерийлер мен сенімділік шектерінің негізіндегі open-set детекция модельдері, сондай-ақ белгілі кластарды жіктеу және «белгісіз» трафикті сәйкестендіру мәселелерін бірлесіп шешуге бағытталған әдістер дамып отыр [16].

Осы жұмыстың шеңберінде 6G slicing сценарийінде желілік трафик деректері мен қызмет көрсету сапасының көрсеткіштері бойынша шабуылдарды анықтауды бағалауға арналған эксперименттік әдістеменің шаблоны қалыптастырылады. Амал-әсіл көп кластық жіктеуді, қиықтар арасындағы төзе алушылықты тексеруді және белгісіз шабуыл типін бөліп көрсете отырып негізгі open-set сценарийді қосады. Эксперименттің мұндай құрылымы, модельдер мен сапа критерийлерін салыстырудың қалпына келетін процедурасын сақтап қалып, кейініректе синтетикалық деректерді нақты трассаларға алмастыруға мүмкіндік береді.

Бұл жұмыстың мақсаты 5G және 6G желілерінің заманауи қауіптері мен осалдықтарын талдау, сондай-ақ машиналық оқыту әдістерін қолдана отырып, желілік трафикті талдаудың негізінде шабуылдарды анықтап табу әдістерінің тиімділігін бағалау болып табылады. Алға қойылған мақсатқа қол жеткізу үшін шабуылдарды көп класты жіктеу есебінде Logistic Regression, Random Forest және XGBoost модельдерін салыстырмалы талдау жүргізіледі және домендік ығысу және белгісіз шабуылдардың пайда болуы жағдайларында детектордың тұрақтылығы зерттеледі.

Материалдар мен әдістер. Жұмыста желілік трафик пен қызмет көрсету сапасының жиынтық көрсеткіштері бойынша шабуылдарды анықтау және жіктеу міндеттеріне бағытталған, 6G желілік қиықтарының қауіпсіздігі бойынша синтетикалық деректер жиынтығы пайдаланылған. Датасетте 1000 бақылау мен 21 белгі бар. Мақсатты айнымалы

Attack Type өрісімен белгіленеді және үш класты қосады. Бұл DDoS, Spoofing және Eavesdropping. Кластардың таралуы бірқалыптыға жақын, бұл теңгерімсіздікке орай көрсеткіштердің жылжу қатерін төмендетеді.

Белгілер аралас түрлермен көрсетілген. Белгілердің бір бөлігі сандық болып табылады және өткізу қабілеттілігінің, кідірістердің және шығындардың сипаттамаларын көрсетеді. Мысалдар Slice Bandwidth, Latency, Packet Loss Rate, Data Rate, Throughput, Energy Efficiency, Packet Delivery Ratio, End-to-End Delay қосады. Белгілердің басқа бір бөлігі категориялық болып табылады және қиықтың жұмыс істеу режимдері мен шарттарын сипаттайды. Мысалдар Slice Type, Traffic Load, Signal Strength, Network Congestion, Transmission Path, Security Mechanism-ді қосады.

Мақсатты ақпараттың жылыстауын болдырмау үшін, белгілерден детектор жұмысының немесе қорғаныс саясатының тікелей салдары болуы мүмкін өрістер алынып тасталған. Атап айтқанда, кіріс белгілерінен Security Status, Attack Detection Time, IGJO-SVM Prediction, Adjustment Action және Accuracy of Security алынып тасталды.

Модельдерді оқытардың алдында бағандардың атауларын үндестіру және дұрыс емес мәндерді бақылау орындалды. Шексіз мәндер бос орындармен алмастырылды. Сандық белгілер медианамен толтырылды, категориялық белгілер ең көп таралған мәнмен толтырылды. Категориялық белгілер тестілеу кезеңінде белгісіз категорияларды қолдайтын

one-hot әдісімен кодталды. Сандық белгілер орташа және стандартты ауытқу бойынша стандартталды. Алдын ала өңдеудің барлық кезеңдері, оқыту мен тестілеу арасындағы сәйкессіздікті болдырмау үшін, бірыңғай конвейер түрінде жүзеге асырылды.

Сапаны бағалау үшін үш негізгі модель қолданылды. Бұл логистикалық регрессия, кездейсоқ орман және XGBoost градиентті тармақтар бустингі. Логистикалық регрессия желілік базалық деңгей ретінде қолданылды. Кездейсоқ орман белгілердің өзара әрекеттесуіне сезімтал келетін тұрақты желілік емес әдіс ретінде пайдаланылды. XGBoost көп класты жіктеу есептері үшін күшті кестелік алгоритм ретінде пайдаланылды.

XGBoost дұрыс жұмыс істеуі үшін мақсатты айнымалы LabelEncoder көмегімен тұтас кластарға кодталды. Қалған модельдер үшін оқыту тікелей сынып жол белгілерінде орындалды. Модельдердің гиперпараметрлері негізгі әдістеменің салыстырмалылығы мен жаңғыртылуын сақтап қалу үшін дәл баптаусыз, тіркелген түрде белгіленді.

Гиперпараметрлер бекітілген мәндермен белгіленді, себебі автоматты іздеу кезінде байқалатын айырмашылық алгоритмнің өзіне тән қасиетінен емес, іздеу процесінің ерекшеліктерінен туындауы мүмкін. Мұндай жағдайда модельдер арасындағы салыстыру нәтижесі жаңғыртылмайды. Гиперпараметрлерді тіркеу осы қауіпті болдырмайды және эксперименттің reproducibility шартын орындайды: кез келген орта мен іске асыруда бірдей нәтиже алынуы тиіс.

Негізгі эксперимент train-test бөлу сызбасы бойынша құрылды. Модельдердің сапасын бағалаудың сенімділігін арттыру үшін қосымша k-fold кросс-валидация (k=5) қолданылды. Мұндай амал-тәсіл деректерді кездейсоқ бөлудің әсерін азайтуға және жіктеу метрикаларының тұрақтырақ бағаларын алуға мүмкіндік береді. Тестілік іріктеменің үлесі 25 пайызды құрады. Бөлу мақсатты класс бойынша стратификацияланған түрде орындалды. Кездейсоқ күй 42 мәнімен тіркелді.

Домен деңгейінде желі жағдайларының өзгеруіне төзімділікті тексеру қосымша жүргізілді. Бұл үшін Slice Type белгісі бойынша топтастыру қолданылды. Оқыту ең көп көрсетілген Slice type категориясында орындалды. Тестілеу қалған категорияларда жүргізілді. Мұндай хаттама детектордың желілік қиықтардың әртүрлі түрлері арасында тасымалдануын имитациялайды.

Open-set режимінде белгісіз шабуылдар класын анықтауға қабілеттілік бөлек бағаланды. Мақсатты айнымалының бір класы оқытудан алынып тасталды және тестілеуде белгісіз ретінде қарастырылды. Белгісіздерді бағалау үшін кластың максималды апостериорлы ықтималдығы бойынша шек қолданылды. Шектен төмен мәндер кезінде болжам UNKNOWN класына көшіріліп отырылды. Шек белгілі кластардың валидациялық бөлігінде сенімділіктің бөліну квантилі бойынша анықталды.

Сенімділік шегінің мәні белгілі кластардың валидациялық бөлігінде анықталды. Бұл үшін валидациялық іріктемедегі барлық үлгілер бойынша кластың максималды апостериорлы ықтималдығының таралуы есептелді. Шек ретінде осы таралудың 10-шы перцентилі алынды: аталған квантильдің астына түсетін ықтималдық мәндері сенімділік жеткіліксіз деп бағаланды. Тестілеу кезінде берілген шектен төмен ықтималдықпен жіктелген үлгілер UNKNOWN класына тағайындалды. Шекті тестілік іріктемеден алдын ала есептеу деректердің жылыстауына (data leakage) әкеледі, сондықтан тек валидациялық бөлік пайдаланылды.

Алдын ала өңдеу бірыңғай конвейер түрінде жүзеге асырылған. Сандық белгілер медианалық импутация және стандарттау арқылы өңделді. Категориялық белгілер ең жиі таралған мәннің импутациясымен және one hot кодтаумен өңделді. Мұндай амал-тәсіл өткізулердің дұрыс өңделуін және кестелік белгілерді қолданатын модельдердің үйлесімділігін қамтамасыз етеді.

Open-set режимі үшін AUROC негізінде белгілі және белгісіз үлгілердің бөлінгіштігін бағалау қолданылды. Скорингтік функция ретінде 1 минус кластың максималды ықтималдығы мәні қолданылды. Мұндай қойылым белгісіз шабуылдарды анықтау үшін модельдің сенімділігінің жарамдылығын сандық тұрғыдан бағалауға мүмкіндік береді.

Эксперименттер Python-да Google Colab-та орындалған. Деректерді өңдеу және конвейерлерді құру үшін NumPy, pandas және scikit-learn қолданылған. Градиенттік бустинг үшін xgboost пакеті қолданылған. Кездейсоқ күйді тіркеп бекіту нәтижелердің жаңғыртылуын қамтамасыз ету үшін, деректерді бөлу және модельдерді оқыту кезеңдерінде қолданылды.

Қауіпті типтендіру міндеті үшін accuracy, balanced accuracy, macro F1 және weighted F1 қолданылды. Негізгі интерпретация метрикасы болып macro F1 таңдалды, өйткені ол барлық кластар бойынша сапа-

ны бірдей ескереді. Мазмұнды талдау үшін қателіктер матрицалары құрылды, олар бойынша өзара қателіктердің ең көп санын беретін класс жұптары бөліп алынды және белгілер тұрғысынан шатасудың себептері туралы қорытындылар қалыптастырылды.

Эксперименттер Google Colab-та Python мен NumPy кітапханаларын, pandas, scikit-learn және XGBoost қолдана отырып орындалды. Нәтижелер кейінге қалдырылған іріктеме үшін метрикалар кестелері түрінде және кросс-тексеру бойынша орташа мәннің және стандартты ауытқудың құрама кестелері түрінде тіркеліп жазылды.

Нәтижелер және талқылау. Негізгі қойылымда трафиктің жиынтық белгілері бойынша шабуылдардың түрлерін және желілік қиықтың күйін көп класты жіктеу қарастырылды. Салыстыру үшін үш модель қолданылды. Бұл логистикалық регрессия, кездейсоқ орман және XGBoost. Бағалау стратификацияланған бөлу кезінде кейінге қалдырылған тесттік іріктемеде жүргізілді.

Жиынтық нәтижелер 1-кестеде келтірілген. Логистикалық регрессия модельдің сызықтық сипатына және сызықтық емес тәуелділіктерді есепке алу қабілетінің шектеулі болуына байланысты күтілетін төменірек сапаны көрсетеді. Кездейсоқ орман белгілердің өзара әрекеттесуі мен шуға төзімділігін модельдеудің арқасында көрсеткіштерді жақсартады. Ең жақсы нәтижені XGBoost қамтамасыз етеді, бұл сандық та, категориялық та белгілер болған кезде оның кестелік деректердегі тиімділігімен үйлеседі.

1-кесте. Attack Type жіктеу тапсырмасындағы модельдердің сапасы

Модель	Accuracy	Balanced Accuracy	Macro-F1
Logistic Regression	0.78	0.77	0.77
Random Forest	0.85	0.84	0.84
XGBoost	0.90	0.90	0.90

Алынған мәндер таңдалған белгілер жинағының ақпараттылығы DDoS, Spoofing және Eavesdropping кластарын тұрақты ажырату үшін жеткілікті екенін көрсетіп отыр. XGBoost-тағы ең жоғары Macro-F1 барлық кластар бойынша теңдестірілген сапаны және шабуылдардың бір типінің пайдасына айқын ауытқудың жоқтығын көрсетеді.

Үздік модель үшін қателер матрицасы талданды. Негізгі шатасулар Spoofing пен Eavesdropping арасында байқалады, бұл күтілетін жағдай болып табылады, өйткені екі сценарий де трафик көлемінің күрт өсуі болмаған кезде жүктеме мен қызмет көрсету сапасының индикаторларындағы ұқсас өзгерістер арқылы көрініс табуы мүмкін. Бұл ретте DDoS класы ең сенімді айырып танылады, өйткені ол өткізу қабілеттілігінің, шамадан тыс жүктеме деңгейінің және кідірістердің айқын көрінген өзгерістерімен бірге жүреді.

Қателердің таралып бөлінуі модельдің QoS-тың елеулі деградациясын тудыратын шабуылдар мен желілік сипаттамалардағы нәзігірек өзгерістер арқылы көрініс табатын шабуылдар арасындағы айырмашылықтарды дұрыс тіркеп жазатынына көрсетіп отыр.

Төзе алушылықты бағалау үшін Slice Type белгісі бойынша домендік ығысу хаттамасы қолданылды. Оқыту қиықтың бір типінде, ал тестілеу қалғандарында орындалды. Мұндай режим детектор сервистің профилімен және QoS параметрлерімен ерекшеленетін жаңа пайдалану жағдайларында өріс алған кездегі практикалық сценарийді модельдейді.

Нәтижелер 2-кестеде келтірілген. Базалық бағалаумен салыстырғанда метрикалардың төмендеуі байқалады. Алайда, сапа қолайлы деңгейде қалады, бұл модельдің доменнің өзгеруіне төзімділігін және оның бір сценарийдің жеке корреляцияларына емес, жалпы заңдылықтарға сүйенетіндігін көрсетеді.

2-кесте. Slice Type домендері арасында тасымалдау кезіндегі XGBoost сапасы

Модель	Accuracy	Balanced Accuracy	Macro-F1
Доменішілік бағалау	0.90	0.90	0.90
Доменаралық бағалау	0.82	0.81	0.81

Доменаралық қойылымда Macro-F1 төмендеуі 0.10-дан аз шаманы құрайды, бұл осы әдісті қиық

параметрлері ауысқан кезде салыстырмалы түрде тұрақты ретінде сипаттайды. Осындай нәтиже мұнда жолаққа, кідіріске және сенімділікке қойылатын талаптары әртүрлі желілік қиықтардың кең спектрі күтілетін 6G сценарийлері үшін маңызды.

Детектордың шабуылдардың оқытатын іріктемеде жоқ белгісіз класын бөліп көрсету қабілеттілігі қосымша бағаланды. Бұл режимде кластардың бірі оқытудан алынып тасталды және тестілеуде белгісіз ретінде қарастырылды. Белгісіздік туралы шешім кластар бойынша максималды ықтималдылық ретінде есептелген сенімділік шегі бойынша қабылданды.

Нәтижелер 3-кестеде келтірілген. AUROC мәні кездейсоқ деңгейден едәуір асып түседі, бұл таңдап алынған сенімділік шарасының белгісіз шабуылдарды анықтап табу үшін жарамдылығын растап отыр. UNKNOWN класын енгізу сенімді жаңсақ болжамдардың үлесін төмендетуге және жаңа немесе модификацияланған шабуылдардың пайда болуы жағдайында детектордың практикалық сенімділігін арттыруға мүмкіндік береді

3-кесте. Open-set режимінде белгісіз шабуылдарды анықтау көрсеткіштері

Метрика	Мәні
AUROC (known vs unknown)	0.88
Macro-F1 (UNKNOWN класымен)	0.80
Дұрыс бөлінген unknown үлесі	0.83

Нәтижелер модельдің сенімділігі бойынша шектік сызбаны пайдаланудың шабуылдардың толық емес таксономиясы жағдайларында IDS тұрақтылығын арттыру үшін тиімді механизм болып табылатынын көрсетіп отыр. Мұндай амал-тәсіл осында жаңа шабуыл векторларының жылдам пайда болуы жабық жіктеуді жеткіліксіз ететін 5G және 6G желілері үшін ерекше өзекті болып отыр.

Нәтижелер желілік трафиктің жиынтық белгілері мен қызмет көрсету сапасының көрсеткіштері бойынша желілік қиықтар ортасында шабуылдардың негізгі түрлерін сенімді ажыратуға болатындығын көрсетіп отыр. Ең жоғары сапаны XGBoost көрсетіп отыр, бұл оның сызықтық емес тәуелділіктерді анықтау және жүктеме, кідіріс, шығындар және өткізу қабілеттілігі параметрлері арасындағы өзара әрекеттесуді ескеру қабілеттілігімен байланысты болып отыр. Желілік модель негізгі деңгей ретінде әрекет етеді және күтілетіндей жол береді, дәл сол кезде тармақтар ансамбльдері шешуші шекаралардың икемділігінің есебінен кластардың дәлірек бөлінуін қамтамасыз етеді.

Slice Type белгісі бойынша доменаралық тексеру домендік ығысу әсерінің болуын растап отыр. Қиықтардың түрлері арасында тасымалдау кезінде метрикалар төмендейді, өйткені трафиктің профильдері мен ресурстарды басқару режимдері өзгереді. Осыған қарамастан, қолайлы сапаны сақтап қалу модельдің шамадан тыс жүктемемен, кідірістердің өсуімен және пакетті жеткізудің деградациясымен байланысты шабуылдардың жалпы көріністеріне сүйенетініне көрсетеді. Мұндай тұрақтылық мұнда сервистер мен қиықтардың алуан түрлілігі желіні пайдаланудың басты ерекшелігі болып табылатын 5G және 6G үшін маңызды.

Open-set режимі детектордың жаңа немесе модификацияланған шабуылдар жағдайында практикалық қолданылуын арттырады. Сенімділік шегі бойынша UNKNOWN класын енгізу сенімді қателер қаупін төмендетеді және, тереңдете талдау мен қауіпсіздік саясатын күшейтуді қоса алғанда, қосымша жауап беру шараларын бастауға мүмкіндік береді. Бұл амал-тәсіл мұнда қауіптердің жоғары динамикасы және шабуылдардың толық таксономиясын алдын ала белгілеудің мүмкін еместігі күтілетін 6G сценарийлері үшін әсіресе өзекті.

Қорытынды. Жұмыста трафиктің жиынтық белгілері мен желілік қиықтардың QoS көрсеткіштерінің негізінде 6G желілеріндегі шабуылдарды анықтап табу және жіктеу әдістемесі ұсынылған. Негізгі модельдерді салыстыру ең жақсы сапаны XGBoost қамтамасыз ететінін көрсетті, бұл кестелік деректер үшін градиентті бустинг әдістерінің тиімділігін растап отыр. Қиықтардың түрлері бойынша доменаралық бағалау домендік ығысудың әсерін және желі жағдайлары өзгерген кезде детектордың төзе алушылығын тексеру қажеттілігін анықтап берді. UNKNOWN класын бөліп алумен open-set режимі жүйенің жаңа немесе модификацияланған шабуылдардың пайда болуына төзімділігін арттырады және сенімді қате шешімдер қаупін төмендетеді. Ұсынылған эксперимент шаблонын, кейініректе

кіріс деректерін алмастыра және сандық нәтижелерді жаңарта отырып, нақты 5G/6G датасеттеріне тікелей көшіруге болады. Нәтижелердің практикалық маңыздылығы ұсынылған амал-тәсілді келесі буын желілері үшін басып енуді анықтап табу жүйелерін әзірлеу кезінде қолдану мүмкіндігінен тұрады. Әдістеме 5G инфрақұрылымдарында және келешекті 6G желілерінде желілік трафикті талдау үшін қолданыла, сондай-ақ желілік қауіпсіздікті қамтамасыз етудің интеллектуалды жүйелері саласындағы одан әрі зерттеулер үшін негіз болып қызмет ете алады.

Ұсынылған тәсілді бар IDS шешімдерімен тікелей салыстыру синтетикалық датасет пайдаланылғандықтан шектеулі. Алайда [13] жұмысында нақты 5G core трафигінде алынған нәтижелермен шамалас талдауға болады: сол жұмыста Random Forest үшін Macro-F1 = 0.87-0.92 диапазонында хабарланған. Осы жұмыстағы XGBoost моделі негізгі қойылымда Macro-F1 = 0.90 көрсетті, бұл аталған диапазонның шегінде. Нәтижелер арасындағы жақындық датасеттердің сипаты мен бағалау хаттамаларының айырмашылығына байланысты тікелей тұжырым жасауға мүмкіндік бермейді. Нақты 5G/6G трассаларында тікелей бенчмаркинг болашақ зерттеудің міндеттерінің бірі болып табылады.

Зерттеудің шектеулері. Жұмыста синтетикалық датасет пайдаланылды, бұл бірқатар шектеулерді туындатады. Синтетикалық деректер нақты 5G/6G желілерінің барлық ерекшеліктерін – хаттама артефактілерін, жабдыққа тән ауытқуларды және трафиктің стохастикалық мінез-құлқын толығымен қамти алмайды. Осыған орай алынған метрикалар нақты желілік ортада өзгеруі мүмкін. Бұл ретте синтетикалық деректер эксперименттің жаңғыртылуын және конвейердің логикалық дұрыстығын тексеруге мүмкіндік береді. Болашақ зерттеуде деректерді нақты трассалары бар 5G-NIDD немес 5GCID датасеттерімен алмастыру, сондай-ақ LSTM және Transformer негізіндегі терең оқыту модельдерімен салыстырмалы бағалау жоспарланып отыр.

Әдебиеттер

1. Nguyen V.-L., Lin P.-C., Cheng B.-C., Hwang R.-H., Lin Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges // IEEE Communications Surveys & Tutorials. −2021. –P. 1-45. DOI10.1109/COMST.2021.3108618.
2. Mao B., Liu J., Wu Y., Kato N. Security and Privacy on 6G Network Edge: A Survey// IEEE Communications Surveys & Tutorials. −2023. -Vol. 25(2). -P.1095-1127. DOI 10.1109/COMST.2023.3244674.
3. Saeed M.M., Saeed R.A., Hasan M.K., Ali E.S., Mazha T., Shahzad T., Khan S., Hamam H. A comprehensive survey on 6G-security: physical connection and service layers // Discover Internet of Things. - 2025. Vol. 5: 28. DOI 10.1007/s43926-025-00123-7.
4. Sandeepa C., Siniarski B., Kourtellis N., Wang S., Liyanage M. A Survey on Privacy of Personal and Non-Personal Data in B5G/6G Networks \// ACM Computing Surveys. −2024. -Vol.56(10): 266. -P. 1-37. DOI 10.1145/3662179.
5. He C., Fei Sh., Yan Zh. Advancing 5G Security and Privacy with AI: A Survey // ACM Computing Surveys. −2025. -Vol. 58(2): 47. -P. 1-36. DOI 10.1145/3744555.
6. De Alwis C., Porambage P., Dev K., Gadekallu T.R., Liyanage M. A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions // IEEE Communications Surveys & Tutorials. −2024. Vol. 26(1). -P. 534-570. DOI 10.1109/COMST.2023.3312349.
7. Salahdine F., Liu Q., Han T. Towards Secure and Intelligent Network Slicing for 5G Networks // IEEE Open Journal of the Computer Society. 2022. -Vol.3.-P.23-38. DOI 10.1109/OJCS.2022.3161933.
8. Dangi R., Jadhav A., Choudhary G., Dragoni N., Mishra M.K., Lalwani P. ML-Based 5G Network Slicing Security: A Comprehensive Survey // Future Internet. −2022. -Vol. 14(4): 116. DOI 10.3390/fi14040116.
9. Dias J., Pinto P., Santos R., Malta S. 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Approaches // Sensors. 2025. -Vol. 25(13): 3940. DOI:10.3390/s25133940.
10. Ranaweera P., Jurcut A., Liyanage M. MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures // ACM Computing Surveys. −2021. -Vol. 54(9):186. DOI 10.1145/3474552.
11. Amponis G., Radoglou-Grammatikis P., Nakas G., Goudos S., Argyriou V., Lagkas T., Sarigiannidis P. 5G core PFCP intrusion detection dataset \//2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST). −2023. -P. 1-4. DOI 10.1109/MOCAST57943.2023.10176693.
12. Breeden J., Khan M.S., Silvestri S., Bajracharya B., Scott C. Mitigating slice vulnerabilities in 5G core networks // Ad Hoc Networks. −2025. -Vol. 183: 104118. DOI 10.1016/j.adhoc.2025.104118.

13. HuY., Sun Q., Dang T., Wu G., & Tian L. 5GCID: Dataset of 5GC intrusion detection system //Computer Communications. - 2025. - Vol.247:108375. DOI 10.1016/j.comcom.2025.108375.
14. Patnaik P., et al. TinyML Driven Intrusion Detection for 5G Network Slices with Leakage-Free Validation // Next-Generation Computing Systems and Technologies. −2026. -Vol. 2(1). -P. 10-20. DOI 10.62762/NGCST.2026.664893.
15. Zoppi T., Ceccarelli A., Puccetti T., Bondavalli A. Which algorithm can detect unknown attacks? Comparison of supervised, unsupervised and meta-learning algorithms for intrusion detection // Computers & Security. −2023. -Vol. 127: 103107. DOI 10.1016/j.cose.2023.103107.
16. Souza M.M.C., Pontes C.T., Gondim J.J.C., Garcia L.P.F., DaSilva L., Cavalcante E.F.M., Marotta M.A. A novel open set Energy-based Flow Classifier for Network Intrusion Detection // Computers & Security. 2025. -Vol. 157: 104569. DOI 10.1016/j.cose.2025.104569.

Авторлар туралы мәліметтер

Батырхан С.К. - PhD докторанты, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, e-mail: sake.batyrkhan@gmail.com;

Ахметов Б.С. - техника ғылымдарының докторы, профессор-зерттеушісі, Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан, e-mail: bakhytzhan.akhmetov.54@gmail.com.

Information about the authors

Batyrhan S.K. - PhD student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: sake.batyrkhan@gmail.com;

Akhmetov B.S. - Doctor of Technical Sciences, Research Professor, Abai Kazakh National Pedagogical University, Almaty, Kazakhstan, e-mail: bakhytzhan.akhmetov.54@gmail.com.