



MOBIL ALOQA YADRO TARMOQLARIDA SIGNALIZATSIYA HUJUMLARINI INTELLEKTUAL ANIQLASH USULLARINING QIYOSIY TAHLILI

**Axmedova Nozima
Farxod qizi**

*Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti, Kriptologiya kafedrası
dotsenti v.b., tel: 935083123,
email: nozimaaxmedova@tuit.uz*

Annotatsiya. Maqolada mobil operatorlar yadro tarmog'idagi SS7, Diameter, GTP va 5G yadro (PFCP, SBA) protokollariga qaratilgan hujumlarni mashinali va chuqur o'qitish asosida aniqlashga bag'ishlangan 2017–2026-yillardagi to'qqizta tadqiqot qiyosiy tahlil qilingan. Ishlar protokol qamrovi, ma'lumot manbai, o'qitish paradigmasi va hisobot qilingan metrikalar bo'yicha taqqoslangan. Tahlil yondashuvlarning aksariyati bitta protokol bilan cheklanganini, real operator trafigi juda kam qo'llanganini hamda laboratoriya muhitida olingan yuqori ko'rsatkichlar boshqa tarmoqqa ko'chirilganda keskin pasayishini (hujumlarni aniqlash recall'i 0,26 gacha) ko'rsatdi. Protokollararo korrelyatsiya, yarim nazoratli o'qitish va baholash metodikasini standartlashtirishga asoslangan rivojlanish yo'nalishlari taklif etilgan.

Kalit so'zlar: mobil yadro tarmog'i, SS7, Diameter, GTP, PFCP, 5G, signalizatsiya hujumlari, hujumlarni aniqlash tizimi, mashinali o'qitish, chuqur o'qitish, protokollararo korrelyatsiya.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ ОБНАРУЖЕНИЯ СИГНАЛЬНЫХ АТАК В ЯДРЕ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ

Аннотация. В статье проведён сравнительный анализ девяти исследований 2017–2026 гг., посвящённых обнаружению атак на протоколы ядра сетей мобильных операторов (SS7, Diameter, GTP, PFCP и SBA 5G) методами машинного и глубокого обучения. Работы сопоставлены по охвату протоколов, источнику данных, парадигме обучения и используемым метрикам. Установлено, что большинство подходов ограничены одним протоколом, реальный трафик оператора используется крайне редко, а высокие показатели, полученные в лабораторной среде, резко снижаются при переносе модели в другую сеть (полнота обнаружения атак падает до 0,26). Предложены направления развития на основе межпротокольной корреляции, частично контролируемого обучения и стандартизации методики оценки.

Ключевые слова: ядро мобильной сети, SS7, Diameter, GTP, PFCP, 5G, сигнальные атаки, система обнаружения вторжений, машинное обучение, глубокое обучение, межпротокольная корреляция.

A COMPARATIVE ANALYSIS OF INTELLIGENT METHODS FOR DETECTING SIGNALLING ATTACKS IN MOBILE CORE NETWORKS

Abstract. The paper presents a comparative analysis of nine studies published in 2017–2026 that apply machine learning and deep learning to detect attacks on mobile core network protocols (SS7, Diameter, GTP, and 5G core PFCP and SBA). The studies are compared by protocol coverage, data source, learning paradigm, and reported metrics. The analysis shows that most approaches are limited to a single protocol, real operator traffic is rarely used, and high scores obtained in laboratory settings drop sharply when a model is transferred to another network (attack recall falls to 0.26). Development directions based on cross-protocol correlation, semi-supervised learning, and a standardized evaluation methodology are proposed.

Keywords: mobile core network, SS7, Diameter, GTP, PFCP, 5G, signalling attacks, intrusion detection system, machine learning, deep learning, cross-protocol correlation.

KIRISH

Mobil aloqa operatorlarining yadro tarmog‘i abonentlarni ro‘yxatdan o‘tkazish, joylashuvni boshqarish, autentifikatsiya va ma’lumot uzatish seanslarini boshqaruvchi signalizatsiya protokollariga tayanadi. 2G/3G tarmoqlarida SS7 (MAP), 4G tarmoqlarida Diameter, paket ma’lumotlari uchun GTP, 5G yadrosida esa PFCP va xizmatlarga yo‘naltirilgan arxitektura (SBA) interfeyslari qo‘llanadi. Bu protokollarning aksariyati operatorlar bir-biriga ishonadigan yopiq muhit uchun loyihalangan bo‘lib, rouming va tarmoqlararo ulanishlar kengaygani sari tashqi hujumlar uchun ochiq bo‘lib qolgan.

Signalizatsiya hujumlari orqali abonent joylashuvini kuzatish, SMS va qo‘ng‘iroqlarni ushlab qolish, xizmat ko‘rsatishni rad etish va billing firibgarligini amalga oshirish mumkin [1–3]. Masalan, GTP protokoli orqali amalga oshiriladigan real tahdidlar 4G tarmoqlarida qayd etilgan [3], SS7 esa 4G/5G qamrovi bo‘lmagan hududlarda zaxira sifatida yana 5–10 yil saqlanib qolishi kutilmoqda [2]. Bundan tashqari, SS7 zaifliklaridan 4G va 5G xavfsizlik mexanizmlarini chetlab o‘tuvchi pasaytirish (downgrade) hujumlarida foydalanish mumkin [1].

Qoidaviy filtrlar va signalizatsiya ekranlari ma’lum hujum shablonlariga qarshi samarali bo‘lsa-da, yangi va holatga bog‘liq hujumlarni aniqlashda cheklangan [1]. Shu sababli so‘nggi yillarda mashinali (ML) va chuqur o‘qitish (DL) asosidagi yondashuvlar faol rivojlanmoqda. Biroq ular turli protokollar, ma’lumotlar to‘plamlari va metrikalarda baholangani uchun natijalarini bevosita taqqoslash qiyin.

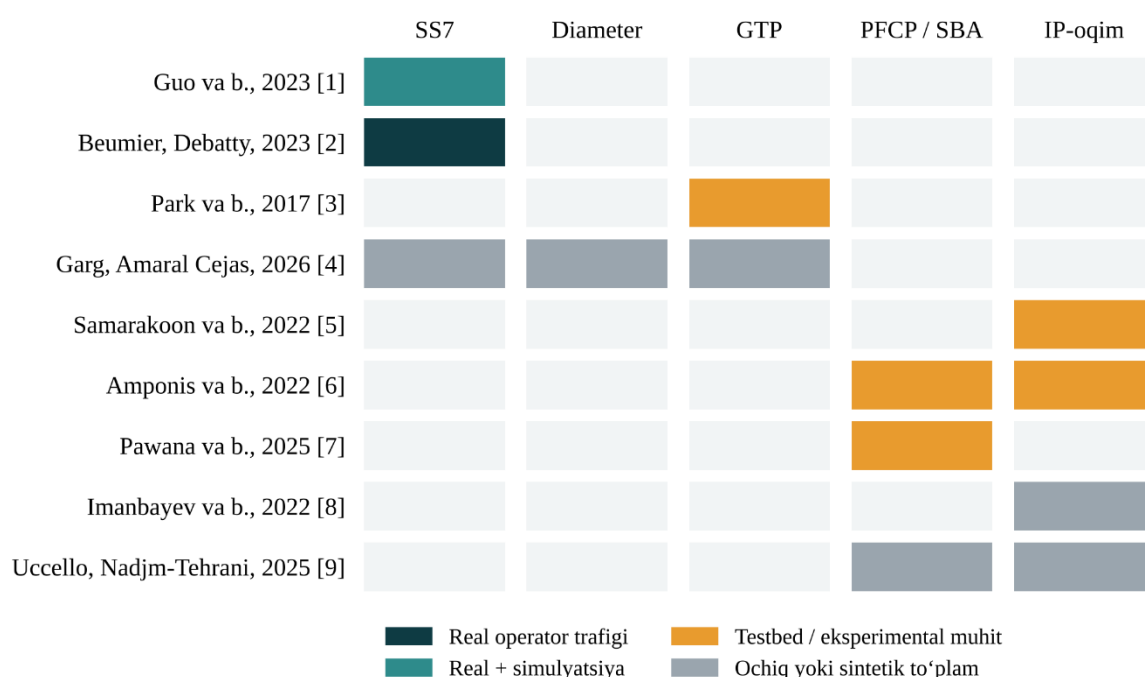
Maqolaning maqsadi – mobil yadro tarmog‘ida signalizatsiya hujumlarini intellektual aniqlash bo‘yicha mavjud tadqiqotlarni yagona mezonlar asosida qiyosiy tahlil qilish va hal etilmagan ilmiy masalalarni aniqlash.

TADQIQOT METODOLOGIYASI

Tahlil tizimli adabiyotlar sharhi tamoyillari asosida o‘tkazildi. Manbalar 2016–2026-yillar oralig‘ida ochiq ilmiy qidiruv tizimlari orqali «SS7/Diameter/GTP attack

detection», «5G core intrusion detection» va «machine learning» kalit iboralari bo'yicha izlandi; tanlangan ishlar MDPI, Tech Science Press, Inderscience, SpringerOpen nashriyotlarida, arXiv va IEEE DataPort platformalarida e'lon qilingan. Tanlash mezonlari quyidagilar: (1) ish mobil yadro tarmog'i protokollari yoki 5G yadro trafiga qaratilgan bo'lishi; (2) aniqlash usuli ML/DL yoki ular bilan qiyoslangan qoidaviy usul bo'lishi; (3) natijalar miqdoriy baholangan yoki ochiq ma'lumotlar to'plami taqdim etilgan bo'lishi. Natijada to'qqizta ish tanlandi [1–9].

Har bir ish to'rtta mezon bo'yicha tavsiflandi: protokol qamrovi (SS7, Diameter, GTP, PFCP/SBA, IP-oqim); ma'lumot manbai (real operator trafigi, testbed, ochiq yoki sintetik to'plam); o'qitish paradigmasi (nazoratli, yarim nazoratli, nazoratsiz) va hisobot qilingan metrikalar. Qo'shimcha ravishda natijalarning boshqa tarmoq muhitiga ko'chirilishi, ishlov berish tezligi va qarorlarning izohlanuvchanligi ko'rib chiqildi. Ishlarning protokollar va ma'lumot manbalari bo'yicha taqsimoti 1-rasmda keltirilgan.



1-rasm. Tahlil qilingan ishlarning protokollar va ma'lumot manbalari bo'yicha qamrovi

NATIJALAR

1-jadvalda tanlangan ishlarning asosiy tavsiflari umumlashtirilgan.

1-jadval. Mobil yadro tarmog'ida hujumlarni aniqlash bo'yicha ishlarning qiyosiy tavsifi

Ish	Protokol	Ma'lumot	Usul	Asosiy natija
[1] Guo va b., 2023	SS7	Real (POST Luxembourg) + JSS7 simulyatori	Yarim nazoratli DL (PReNet, DevNet, Deep SAD), NODE	PReNet: aksariyat tajribalarda recall $\approx$ 100 %
[2] Beumier, Debatty, 2023	SS7	Real SS7 trafigi (loyiha maqsadi)	ML detektorlari, MARK orqali birlashtirish	Shubhali trafikni izohlash va tavsiyalar ishlab chiqish
[3] Park va b., 2017	GTP (4G)	4G eksperimental muhiti	Signatura va xulq evristikasi	F-score 98,7 %

Ish	Protokol	Ma'lumot	Usul	Asosiy natija
[4] Garg, Amaral Cejas, 2026	SS7, Diameter, GTP	219 294 yozuv, sintetik anomaliyalar	Nazoratsiz, 6 ta embedding modeli konsensusi	≥ 5 model belgilagan yozuvlar to'liq sintetik
[5] Samarakoon va b., 2022	5G, IP-oqim	5G test tarmog'i	Belgilangan to'plam, ML modellari	Ochiq 5G-NIDD to'plami
[6] Amponis va b., 2022	5G PFCP, IP-oqim	Testbed	PFCP DoS hujumlari to'plami	TCP/IP va PFCP oqim xususiyatlari
[7] Pawana va b., 2025	5G SBA (rouming)	5G SA testbed, 59 380 oqim	MLP, 1D-CNN, AE, RNN, GRU, LSTM	LSTM: BACC 98,26 %
[8] Imanbayev va b., 2022	IP-oqim (5G yadro uchun)	CICIDS2017, CSE-CIC-IDS2018	LR, RF, gradient busting, AE, DNN	O'z testida recall 0,99; boshqa muhitda 0,26
[9] Uccello, Nadjm-Tehrani, 2025	5G, IP-oqim, PFCP	5G-NIDD, MSA, PFCP	XGBoost + SHAP / VoTE-XAI	Izoh usullari tanlagan xususiyatlar farqlanadi

Birinchi muhim natija – protokol qamrovining torligi. To'qqizta ishdan sakkiztasi bitta signalizatsiya protokoli (SS7, GTP, PFCP yoki SBA) yoki faqat IP-oqim trafigi bilan cheklangan. Uchta signalizatsiya protokolini birgalikda tahlil qilgan yagona ish [4] nazoratsiz yondashuvga tayanadi va sintetik anomaliyalarda baholangan: 219 294 yozuvning 44,15 % i kamida bitta model tomonidan belgilangan, barcha olti model kelishgan yozuvlar esa atigi 0,97 % ni tashkil etgan. Demak, modellar konsensusisiz yolg'on signallar ulushi juda yuqori bo'ladi.

Ikkinchi natija – real ma'lumotlarning tanqisligi. Real operator trafigidan foydalanilgani faqat [1] da aniq qayd etilgan, [2] loyihasida esa real SS7 trafigida hujumlarni aniqlash maqsad qilingan va bunday ma'lumotlarni olish qiyinligi alohida ta'kidlangan. Belgilangan hujum namunalari juda kam: [1] dagi real to'plam 17 603 ta belgilanmagan yozuv va bor-yo'g'i 62 ta belgilangan namunadan (22 tasi hujum) iborat. Bunday sharoitda nazoratli NODE modeli ko'plab tajribalarda 60 % va undan past natija bergan, yarim nazoratli PReNet esa eng barqaror ishlagan [1]. 5G bo'yicha barcha to'plamlar [5–7] testbedlarda yaratilgan.

Uchinchi natija – metrikalar va ko'chirish muammosi. [7] da barcha modellar 99 % dan yuqori aniqlikka (accuracy) erishgan, ammo trafikning qariyb 82,5 % i normal bo'lgani sababli makro-F1 88–89 % atrofida qolgan va mualliflar balanslangan aniqlikni (BACC) asosiy mezon sifatida qo'llagan. [8] da CSE-CIC-IDS2018 to'plamida o'qitilgan gradient busting modeli o'z test to'plamida 0,99 recall ko'rsatgan bo'lsa-da, boshqa tarmoq muhitida yig'ilgan CICIDS2017 trafigida hujumlarni aniqlash recall'i 0,26 gacha pasaygan. Bundan tashqari, [7] dagi rekurrent modellar sekundiga atigi 139–288 ta namunani qayta ishlagan (to'g'ri tarqaluvchi modellarda 2 939–3 568 ta), bu esa operator miqyosidagi oqimlar uchun yetarli emas.

To'rtinchi natija – izohlanuvchanlik. [9] da 92 xususiyatli 5G to'plamida ICMPFlood hujumi uchun VoTE-XAI 6 ta, SHAP esa 20 dan ortiq muhim xususiyatni ajratgan va ikki usul tanlagan xususiyatlar sezilarli farqlangan. Demak, xavfsizlik operatoriga beriladigan izohning ishonchligi alohida baholanishi kerak.

MUHOKAMA

Natijalar mobil yadro tarmog'ida hujumlarni aniqlash tadqiqotlari protokollar kesimida parchalanib qolganini ko'rsatadi. Amalda esa hujumchi bir protokoldagi zaiflikdan boshqa protokoldagi himoyani chetlab o'tish uchun foydalanadi [1]. Shu sababli bitta abonent identifikatori (IMSI/MSISDN) atrofida SS7, Diameter va GTP hodisalarini vaqt bo'yicha bog'lovchi protokollararo korrelyatsiya alohida protokol detektorlariga qaraganda to'liqroq manzara beradi. [4] bu yo'nalishdagi birinchi qadam bo'lsa-da, unda nazoratli yoki yarim nazoratli o'qitish, billing (CDR) ma'lumotlari bilan integratsiya va oqimli rejimda baholash hali amalga oshirilmagan.

Belgilangan real hujum namunalarining tanqisligi yarim nazoratli va nazoratsiz usullarni ustuvor qiladi [1, 4]. Operatorlarning ma'lumot almashishiga to'sqinlik qiladigan asosiy omil – abonentlarning shaxsga doir ma'lumotlarini himoya qilish talabi; O'zbekistonda bu masala tegishli qonun bilan tartibga solinadi [10]. Shu bois psevdonimlashtirilgan identifikatorlar va federativ o'qitishga asoslangan hamkorlikdagi aniqlash sxemalari istiqbolli hisoblanadi.

Baholash metodikasini standartlashtirish ham zarur: nomutanosib to'plamlarda accuracy o'rniga BACC, makro-F1 va yolg'on signal darajasi (FPR) keltirilishi, modellar boshqa tarmoq muhitida qo'shimcha sinovdan o'tkazilishi hamda o'tkazuvchanlik (hodisa/s) ko'rsatilishi kerak [7, 8].

XULOSA

Birinchidan, mobil yadro tarmog'ida signalizatsiya hujumlarini aniqlash bo'yicha tahlil qilingan to'qqizta ishdan sakkiztasi bitta signalizatsiya protokoli yoki faqat IP-oqim trafigi bilan cheklangan, uchta protokolni birgalikda tahlil qilgan yagona ish esa sintetik anomaliyalarda baholangan. Ikkinchidan, real operator trafigi juda kam qo'llanilgan va belgilangan hujum namunalari o'nlab birliklarni tashkil etadi, bu esa yarim nazoratli o'qitishning afzalligini ko'rsatadi. Uchinchidan, laboratoriya muhitida olingan yuqori ko'rsatkichlar boshqa tarmoqqa ko'chirilganda keskin pasayadi, accuracy esa nomutanosib to'plamlarda haqiqiy samaradorlikni yashiradi. Keyingi tadqiqotlar abonent identifikatori bo'yicha protokollararo korrelyatsiya, shaxsga doir ma'lumotlarni himoyalagan holda hamkorlikda o'qitish va oqimli rejimda standart metrikalar bilan baholashga yo'naltirilishi maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Guo Y., Ermis O., Tang Q., Trang H., De Oliveira A. An empirical study of deep learning-based SS7 attack detection // Information. – 2023. – Vol. 14, № 9. – Art. 509.
2. Beumier C., Debatty T. Security issues related to SS7: project DAP20-01 (poster). – Brussels: Royal Military Academy, 2023. – URL: <https://cylab.be/publications/60/download/2023-security-issues-related-to-ss7.pdf>
3. Park S., Kim S., Son K., Kim H., Park J., Yim K. Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment // International Journal of Web and Grid Services. – 2017. – Vol. 13, № 1.
4. Garg A., Amaral Cejas O. Unsupervised cross-protocol anomaly analysis in mobile core networks via multi-embedding models consensus. arXiv preprint arXiv:2603.15344. – 2026.

5. Samarakoon S., Siriwardhana Y., Porambage P., Liyanage M., Chang S.-Y., Kim J., Kim J., Ylianttila M. 5G-NIDD: A comprehensive network intrusion detection dataset generated over 5G wireless network. arXiv preprint arXiv:2212.01298. – 2022.
6. Amponis G., Radoglou-Grammatikis P., Lagkas T., Mallouli W., Cavalli A., Klonidis D., Markakis E., Sarigiannidis P. Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications // EURASIP Journal on Wireless Communications and Networking. – 2022. – Vol. 2022. – DOI: 10.1186/s13638-022-02204-5.
7. Pawana I.W.A.J., Abella V., Lastre J.K., Ko Y., You I. Enhancing roaming security in cloud-native 5G core network through deep learning-based intrusion detection system // Computer Modeling in Engineering & Sciences. – 2025. – Vol. 145, № 2. – P. 2733–2760.
8. Imanbayev A., Tynymbayev S., Odarchenko R., Gnatyuk S., Berdibayev R., Baikenov A., Kaniyeva N. Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond // Sensors. – 2022. – Vol. 22, № 24. – Art. 9957.
9. Uccello F., Nadjm-Tehrani S. Feature attribution in 5G intrusion detection: a statistical vs. logic-based comparison. arXiv preprint arXiv:2509.10206. – 2025.
10. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – 2019-yil 2-iyul, O‘RQ-547.