DOI: 10.65322/j.srd.02162026.17

UDK: 004.056.53:004.738.5

AXBOROT-TELEKOMMUNIKATSIYA TIZIMLARIDA PAST INTENSIVLI TAQSIMLANGAN XIZMATDAN VOZ KECHISH (DDoS) HUJUMLARINI ANIQLASH MODELI VA METODIKASI

O‘rinov Nodirbek Toxirjonovich,
Dasturiy injiniringi kafedrasi dotsenti,
E-mail: nodirbekurinov1@gmail.com
Andijon davlat universiteti

Annotatsiya. *Maqolada axborot-telekommunikatsiya tizimlarida past intensivli taqsimlangan xizmatdan voz kechish (LR-DDoS) hujumlarini aniqlash masalasi ko‘rib chiqiladi. Mavzuning dolzarbligi shundaki, mavjud usullar asosan yuqori intensivli hujumlarga yo‘naltirilgan bo‘lib, LR-DDoS trafikining qonuniy foydalanuvchi xatti-harakatiga o‘xshashligi ularni aniqlashni murakkablashtiradi. Tadqiqot maqsadi – yuqori aniqlik va past yolg‘on ijobiy darajani ta’minlovchi gibrid model ishlab chiqishdir. Taklif etilgan ikki bosqichli model statistik-entropik tahlil va stacking-ansambl mashinaviy o‘qitish usullarini birlashtiradi. Metodika belgilarni tanlash, o‘qitish, optimallashtirish va baholash bosqichlarini o‘z ichiga oladi. Tajribalar CIC-DDoS2019, CIC-IDS2017 hamda laboratoriya trafiklari asosida o‘tkazildi. Natijalar yuqori samaradorlikni ko‘rsatdi.*

Аннотация: *В статье рассматривается проблема обнаружения низкоинтенсивных распределенных атак типа «отказ в обслуживании» (LR-DDoS) в информационно-телекоммуникационных системах. Актуальность темы заключается в том, что существующие методы в основном ориентированы на высокоинтенсивные атаки, а сходство LR-DDoS-трафика с поведением легитимных пользователей затрудняет их обнаружение. Цель исследования — разработка гибридной модели, обеспечивающей высокую точность и низкий уровень ложных срабатываний. Предложенная двухэтапная модель сочетает статистико-энтропийный анализ и методы ансамблевого машинного обучения. Методология включает этапы отбора признаков, обучения, оптимизации и оценки. Эксперименты проводились на основе трафика CIC-DDoS2019, CIC-IDS2017 и лабораторного трафика. Результаты показали высокую эффективность.*

Abstract: *The article considers the issue of detecting low-intensity distributed denial of service (LR-DDoS) attacks in information and telecommunication systems. The relevance of the topic is that existing methods are mainly focused on high-intensity attacks, and the similarity of LR-DDoS traffic to legitimate user behavior complicates their detection. The goal of the research is to develop a hybrid model that provides high accuracy and low false positive rate. The proposed two-stage model combines statistical-entropic analysis and stacking-ensemble machine learning methods. The methodology includes the stages of feature selection, training, optimization and evaluation. Experiments were conducted on the basis of CIC-DDoS2019, CIC-IDS2017 and laboratory traffic. The results showed high efficiency.*

Kalit so‘zlar: *Axborot xavfsizligi, DDoS, past intensivli hujum, LR-DDoS, Slowloris, Shrew, trafik tahlili, Shannon entropiyasi, mashinaviy o‘qitish, stacking-ansambl, anomaliyani aniqlash, kiberxavfsizlik.*

Ключевые слова: *Информационная безопасность, DDoS, низкоинтенсивная атака, LR-DDoS, Slowloris, Shrew, анализ трафика, энтропия Шеннона, машинное обучение, stacking-ансамбль, обнаружение аномалий, кибербезопасность.*

DOI: 10.65322/j.srd.02162026.17

Keywords: *Information security, DDoS, low-rate attack, LR-DDoS, Slowloris, Shrew, traffic analysis, Shannon entropy, machine learning, stacking ensemble, anomaly detection, cybersecurity.*

Kirish. Zamonaviy raqamli iqtisodiyot sharoitida axborot-telekommunikatsiya tizimlari (ATT) davlat boshqaruvi, moliya-bank xizmatlari, sog‘liqni saqlash, ta’lim, transport va energetika sohalarining uzluksiz faoliyatini ta’minlovchi asosiy infratuzilma hisoblanadi. Jamiyatning ushbu tizimlarga bog‘liqligi ortib borishi natijasida ularning ishonchliligi va xavfsizligiga qo‘yiladigan talablar ham yildan-yilga keskin oshib bormoqda. Shu bilan birga, kiberhujumlarning soni, murakkabligi va zarar keltirish darajasi ham jadal sur’atlarda ortmoqda. Mutaxassislarning hisob-kitoblariga ko‘ra, jahon bo‘yicha kiberxavfsizlik buzilishlaridan ko‘riladigan iqtisodiy zarar 2026-yilda 10 trillion AQSh dollaridan oshishi prognoz qilinmoqda, bu ko‘rsatkichning sezilarli qismi to‘g‘ridan-to‘g‘ri xizmatdan voz kechish hujumlari bilan bog‘liqdir.

Taqsimlangan xizmatdan voz kechish (Distributed Denial of Service, DDoS) hujumlari – bu ko‘p sonli zararlangan qurilmalar (botnet) yordamida nishon tizim resurslarini qasddan tugatishga qaratilgan kiberhujum turidir [1, 2]. An’anaviy DDoS hujumlari odatda yuqori hajmli trafik generatsiya qilish orqali amalga oshiriladi: masalan, UDP flood, SYN flood, ICMP flood va kuchaytirish (amplification) hujumlari. Bunday hujumlarni aniqlash uchun paketlar oqimining keskin o‘sishi, band kengligining to‘liq egallanishi, manba IP-manzillarning anomal xilma-xilligi kabi belgilardan foydalaniladi. Ushbu belgilar bevosita kuzatiladi, shu sababli an’anaviy imzoga asoslangan aniqlash tizimlari (Snort, Suricata, Zeek) va chegaraviy statistik tahlil vositalari yuqori intensivli hujumlarni aniqlashda yetarlicha samarali hisoblanadi.

Biroq so‘nggi yillarda DDoS hujumlarining sifat jihatidan yangi turi – past intensivli taqsimlangan xizmatdan voz kechish (Low-rate DDoS, LR-DDoS) hujumlari jiddiy tahdidga aylanmoqda. Bu turdagi hujumlar kichik trafik hajmi bilan amalga oshiriladi, biroq protokol darajasidagi zaifliklardan, xususan TCP qayta jo‘natish taymerlari, HTTP ilova qatlamidagi sessiya cheklovlari va server navbat boshqaruv mexanizmlaridan foydalanib, xizmat ko‘rsatish sifatini sezilarli darajada pasaytiradi. Eng mashhur LR-DDoS hujumlariga Shrew (TCP-targeted) [3], Slowloris (HTTP yarim ochiq sessiyalar), Slow Read, Slow POST, R-U-Dead-Yet (RUDY) [4] va HTTP/2 Rapid Reset [5] misol bo‘la oladi.

LR-DDoS hujumlarining asosiy xavfi shundaki, ular juda kam band kenglikda (ba’zan sekundiga bir necha paketdan ham kam) ishlashga qodir va shu bois klassik trafik monitoring tizimlari uchun deyarli ko‘rinmas bo‘lib qoladi. Masalan, Slowloris hujumi orqali 200–400 ochiq sessiya yordamida odatiy Apache veb-serverni to‘liq ishdan chiqarish mumkin [5], holbuki bunday trafik umumiy tarmoq yukiga nisbatan hech qanday anomal belgi ko‘rsatmaydi. Bundan tashqari, bu turdagi hujumlar qonuniy foydalanuvchi xatti-harakatiga statistik jihatdan yaqin bo‘lgani sababli, oddiy belgilarga asoslangan aniqlash usullari yuqori darajadagi yolg‘on ijobiy (false positive) va yolg‘on salbiy (false negative) xatolar keltirib chiqaradi.

Mazkur yo‘nalishda olib borilgan tadqiqotlarni tahlil qilish shuni ko‘rsatadiki, DDoS hujumlarini aniqlash bo‘yicha fundamental ishlar Mirkovic va Reiher tomonidan taklif qilingan taksonomiyadan boshlanadi [6]. Zargar, Joshi va Tipper DDoS himoya mexanizmlarini tarmoq joylashuviga qarab tasniflab bergan [6]. Somani va hamkasblari bulut muhitidagi DDoS tahdidlarining taksonomiyasi va istiqbolli himoya yo‘nalishlarini bayon etgan [6]. Past intensivli hujumlar bo‘yicha to‘g‘ridan-to‘g‘ri ishlar orasida Cambiaso va hamkasblarining Slow DoS tasnifi [7], Chen va Hwangning Shrew hujumlarini spektral tahlil yordamida aniqlashga bag‘ishlangan tadqiqoti [7], shuningdek, Hoque va hamkasblarining botnet tahlili diqqatga sazovordir. So‘nggi yillarda mashinaviy o‘qitishga asoslangan yondashuvlar ham faol rivojlanmoqda: Doriguzzi-Corin va hamkasblari LUCID loyihasi doirasida konvolyutsion neyron tarmoqlaridan foydalanish

DOI: 10.65322/j.srd.02162026.17

imkoniyatini ko‘rsatgan [8], Sharafaldin va hamkasblari esa CIC-DDoS2019 etalon ma’lumotlar to‘plamini tayyorlab, bu yo‘nalishdagi tadqiqotlarga jiddiy hissa qo‘shgan. Bundan tashqari, Yungaicela-Naula va hamkasblari SDN asosidagi arxitekturada mashinaviy va chuqur o‘qitish usullarini qo‘llash imkoniyatini ko‘rsatgan [8].

Adabiyotlar tahlili natijasida mavjud ishlarda quyidagi kamchiliklar va o‘rganilmagan muammolar aniqlandi. Birinchidan, mavjud tadqiqotlarning ko‘pchiligi bitta turdagi LR-DDoS hujumini (masalan, faqat Slowloris yoki faqat Shrew) tahlil qiladi, biroq real sharoitda hujumchilar har xil texnikalarni birlashtirib qo‘llashi mumkin, bu esa bir turdagi ma’lumotlarda o‘qitilgan modellarning amaliy qo‘llanilishini cheklaydi. Ikkinchidan, chegaraviy (threshold-based) entropik yondashuvlar oddiy bo‘lishiga qaramay, statik chegaralarga bog‘liqligi sababli turli tarmoq muhitlarida beqaror natija beradi. Uchinchidan, mashinaviy o‘qitishga asoslangan ishlarning ko‘pchiligida belgilarni tanlash jarayoni yetarlicha asoslanmagan bo‘lib, ortiqcha va shovqinli belgilarning mavjudligi modelning umumlashtirish qobiliyatini pasaytiradi. To‘rtinchidan, aniqlik ko‘rsatkichlari yuqori bo‘lgan ishlarning ayrimlarida False Positive Rate amaliy qo‘llanish uchun qabul qilib bo‘lmaydigan darajada yuqori qoladi. Beshinchidan, modelni eksperimental baholashning yagona, ko‘p bosqichli metodikasi yetarlicha ishlab chiqilmagan.

Yuqorida sanab o‘tilgan muammolardan kelib chiqib, tadqiqotning aniq maqsadi shakllantirildi: axborot-telekommunikatsiya tizimlarida past intensivli DDoS hujumlarini yuqori aniqlikda (Accuracy $\geq 0{,}95$) va past yolg‘on ijobiy daraja bilan (FPR $\leq 0{,}025$) aniqlashga imkon beruvchi, turli turdagi LR-DDoS hujumlariga umumlashtirilgan holda ishlay oladigan gibrid aniqlash modeli va unga mos metodikani ishlab chiqish. Ushbu maqsadga erishish uchun quyidagi ilmiy vazifalar hal qilindi:

• DDoS hujumlarining taksonomiyasini o‘rganib chiqish va past intensivli hujumlarning o‘ziga xos xususiyatlarini tizimlashtirish [9];

• LR-DDoS trafigining informativ statistik, vaqtli va entropik belgilarini aniqlash hamda ularning matematik ta’riflarini berish;

• Belgilarni tanlashning ikki bosqichli (RFE + Mutual Information) yondashuvi asosida eng informativ belgilar to‘plamini shakllantirish;

• Statistik tahlil va mashinaviy o‘qitishni birlashtirgan ikki bosqichli gibrid aniqlash modelini ishlab chiqish;

• Taklif etilgan modelni baholashning ketma-ket bosqichlardan iborat metodikasini ishlab chiqish;

• Modelni etalon ma’lumotlar to‘plamlari va laboratoriya stendida sinovdan o‘tkazish hamda natijalarni mavjud usullar bilan qiyosiy tahlil qilish.

Tadqiqotning ilmiy yangiligi shundan iboratki, birinchi marta LR-DDoS hujumlarini aniqlash uchun vaqt domeni, taqsimot domeni va entropik ko‘rsatkichlarni bir vaqtda hisobga oluvchi ko‘p o‘lchovli belgilar fazosi taklif qilindi va stacking-ansambl arxitekturasi asosida ikki bosqichli aniqlash modeli qurildi. Tadqiqotning amaliy ahamiyati taklif etilgan modelning mavjud IDS/IPS tizimlariga qo‘shimcha modul sifatida integratsiya qilinishi va real vaqtda ishlashga qodirligi bilan belgilanadi.

2. Material va metodlar

2.1. Tadqiqotni tashkil etish

Tadqiqot 2023-yil sentabr oyidan 2025-yil aprel oyigacha bo‘lgan davrda muallif tomonidan (Tashkilot nomi)ning Kiberxavfsizlik ilmiy-tadqiqot laboratoriyasida olib borildi. Ish quyidagi ketma-ket bosqichlardan iborat bo‘ldi: (1) adabiyotlar tahlili va muammoning qo‘yilishi – 4 oy; (2) matematik modelni ishlab chiqish va belgilarni asoslash – 5 oy; (3) dasturiy prototipni ishlab chiqish va laboratoriya stendini yig‘ish – 4 oy; (4) eksperimentlarni o‘tkazish va natijalarni tahlil qilish – 5 oy; (5) natijalarni umumlashtirish va maqolani tayyorlash – 2 oy.

DOI: 10.65322/j.srd.02162026.17

Eksperimental bosqich ikki muhitda amalga oshirildi: birinchidan, ochiq kirishdagi etalon ma'lumotlar to‘plamlari asosida boshlang‘ich baholash o‘tkazildi; ikkinchidan, laboratoriya stendida haqiqiy vaqtda generatsiya qilingan trafik asosida modelning amaliy qo‘llanish ko‘rsatkichlari aniqlandi. Dasturiy ta'minot sifatida Python 3.11 dasturlash tili, Scikit-learn 1.4 mashinaviy o‘qitish kutubxonasi, TensorFlow 2.15 chuqur o‘qitish platformasi, XGBoost 2.0 kutubxonasi, Wireshark 4.2 trafik analizatori, CICFlowMeter belgilar ekstraktori va tcpreplay vositalari qo‘llanildi. Texnik jihozlar tarkibiga Intel Xeon Silver 4314 protsessori, 128 GB operativ xotira va NVIDIA RTX A4000 grafik protsessori o‘rnatilgan server kiritildi.

2.2. Tadqiqot obyekti va predmeti

Tadqiqot obyekti sifatida axborot-telekommunikatsiya tizimlaridagi tarmoq trafigi, tadqiqot predmeti sifatida esa past intensivli DDoS hujumlarini aniqlash modellari, algoritmlari va metodikalari belgilandi. Tadqiqot past intensivli hujumlarning quyidagi asosiy turlarini qamrab oladi: Slowloris (HTTP sessiyalarni yarim ochiq holatda ushlab turish), Slow Read (javobni sekin o‘qish), Slow POST / RUDY (so‘rov tanasini sekin jo‘natish), Shrew (TCP qayta jo‘natish taymeriga moslangan davriy impulslar) va HTTP/2 Rapid Reset (HTTP/2 protokoli oqimlarini tez-tez bekor qilish). Ushbu hujumlarning har biri turli protokol qatlamlarida va har xil mexanizmlar orqali amalga oshirilsa-da, ular umumiy xususiyatga ega: past trafik intensivligi va qonuniy foydalanuvchi xatti-harakatiga o‘xshash statistik profil.

2.3. Ma'lumotlar manbalari

Tadqiqot uchun uchta asosiy manba qo‘llanildi. Birinchi manba – Kanada Kiberxavfsizlik Institutining CIC-DDoS2019 ma'lumotlar to‘plami bo‘lib, u 12 turdagi DDoS hujumi va qonuniy trafikdan tashkil topgan. Ikkinchi manba – CIC-IDS2017 to‘plami bo‘lib, undan qonuniy trafik namunalarini kengaytirish uchun foydalanildi. Uchinchi manba – laboratoriya stendida muallif tomonidan maxsus yig‘ilgan original trafik dumplari bo‘lib, bu Slowloris, Slow Read, Shrew va Rapid Reset hujumlarini haqiqiy sharoitda modellashtirish orqali olingan. Ma'lumotlar umumiy hajmi 14,6 GB ni tashkil etdi, undan 38% past intensivli hujumlar, 24% yuqori intensivli hujumlar va 38% qonuniy trafikni tashkil etdi. Oqimlarning umumiy soni 2 847 316 ta bo‘lib, ulardan 60% o‘qitish, 20% validatsiya va 20% yakuniy sinov to‘plamiga ajratildi.

2.4. Metodologik yondashuv

Tadqiqotning metodologik asosini quyidagi yondashuvlar majmuasi tashkil etdi. Tizimli tahlil yondashuvi DDoS hujumlari va aniqlash usullarini tasniflash, ular orasidagi o‘zaro bog‘liqliklarni aniqlash uchun qo‘llanildi. Statistik tahlil trafik belgilarining taqsimoti, korrelyatsiya matritsasi va chegaralarini aniqlash uchun ishlatildi. Axborot nazariyasi elementlari (Shannon entropiyasi [9], shartli entropiya) trafikning xilma-xilligini va tasodifiylik darajasini o‘lchash uchun qo‘llanildi. Nazorat ostidagi mashinaviy o‘qitish (supervised learning) yakuniy tasniflash qarorini qabul qilish uchun asos bo‘ldi. Eksperimental tadqiqot usuli taklif etilgan modelni empirik baholash va mavjud usullar bilan solishtirish uchun qo‘llanildi.

Trafikning statistik-entropik xususiyatlarini aniqlash uchun quyidagi matematik ifodalardan foydalanildi. Oqim uchun Shannon entropiyasi quyidagicha hisoblanadi [9]:

$$H(X) = -\Sigma\, p(x_i) \cdot \log_2 p(x_i), \qquad i = 1, 2, \ldots, n$$

bu yerda X – paketlararo intervallar yoki paket hajmlari kabi tasodifiy miqdor, $p(x_i)$ – x_i qiymatining paydo bo‘lish ehtimoli, n – diskret qiymatlar soni. Entropiya qiymati qanchalik yuqori bo‘lsa, trafikning xilma-xilligi shunchalik katta bo‘ladi va aksincha. LR-DDoS hujumlari davrida generatsiya qilinayotgan paketlar ma'lum davriylikka ega bo‘lgani uchun entropiya qiymati qonuniy trafikka nisbatan pasayadi.

Oqim darajasidagi asosiy statistik belgilar sifatida quyidagilar hisoblandi: oqim davomiyligi (Flow Duration), oldinga va orqaga paketlararo intervalning o‘rtacha qiymati

DOI: 10.65322/j.srd.02162026.17

(Fwd/Bwd IAT Mean) va standart og‘ishi (Fwd/Bwd IAT Std), oqimdagi paketlar soni (Total Fwd/Bwd Packets), paket uzunligining o‘rtacha qiymati va dispersiyasi (Packet Length Mean, Packet Length Variance), faol va sukut davrlari (Active Mean/Std, Idle Mean/Std), TCP bayroqlarining hisoblagichlari (PSH, URG, ACK, SYN, FIN, RST Count), shuningdek, sekundiga paketlar soni (Flow Packets/s) va baytlar soni (Flow Bytes/s). Ushbu belgilarni hisoblash uchun CICFlowMeter vositasidan foydalanildi, bu vosita har bir oqim uchun 84 ta statistik belgini avtomatik ekstraktsiya qiladi.

2.5. Belgilarni tanlash metodikasi

84 ta dastlabki belgidan eng informativlarini tanlash uchun ikki bosqichli yondashuv qo‘llanildi. Birinchi bosqichda Mutual Information (MI) metodi yordamida har bir belgining sinf yorlig‘i bilan o‘zaro axboroti hisoblandi:

$$I(X;\ Y) = \Sigma\Sigma\, p(x,\ y) \cdot \log_2 [p(x,\ y) / (p(x) \cdot p(y))]$$

bu yerda X – belgi qiymati, Y – sinf yorlig‘i (hujum yoki qonuniy trafik). MI qiymati past bo‘lgan belgilar ($I(X; Y) < 0{,}02$) ro‘yxatdan chiqarildi. Bu bosqichda 84 ta belgidan 47 tasi saqlanib qoldi.

Ikkinchi bosqichda Recursive Feature Elimination (RFE) usuli qo‘llanildi. Bu usulda Random Forest [10] asosiy baza modeli sifatida tanlandi va har bir iteratsiyada eng past ahamiyatga ega belgi olib tashlanib, model qayta o‘qitildi. Optimal belgilar soni 5-karrali kross-validatsiya yordamida aniqlandi va F1-score ko‘rsatkichi maksimal bo‘lgan nuqta tanlandi. Natijada yakuniy belgilar to‘plamida 17 ta belgi qoldi.

3. Taklif etilgan model va metodika

3.1. Aniqlash modelining arxitekturasi

Taklif etilgan LR-DDoS aniqlash modeli ikki bosqichli (two-stage) gibrid arxitekturaga ega bo‘lib, uning asosiy g‘oyasi – statistik tahlilning tez ishlash tezligini va mashinaviy o‘qitishning yuqori aniqligini birlashtirishdan iborat. Model quyidagi funksional bloklardan tashkil topgan: trafikni yig‘ish va oqimlarga ajratish bloki, belgilarni ekstraktsiya qilish bloki, dastlabki tasniflash bloki (1-bosqich), chuqur tasniflash bloki (2-bosqich) va yakuniy qaror qabul qilish bloki.

Birinchi bosqichda kiruvchi har bir oqim uchun 17 ta tanlangan belgi hisoblanadi va ularga asoslangan yengil tasniflagich – optimallashtirilgan chegaraviy qoidalar majmui qo‘llaniladi. Bu bosqichning asosiy vazifasi – ochiq qonuniy trafikni tezda filtrdan o‘tkazish va faqat shubhali oqimlarni keyingi bosqichga uzatish. Birinchi bosqich orqali umumiy trafikning taxminan 78% ajratib olinadi, bu ikkinchi bosqichdagi hisoblash yukini sezilarli darajada kamaytiradi.

Ikkinchi bosqichda shubhali deb topilgan oqimlar stacking-ansambl modeli [11] orqali yakuniy tasniflanadi. Stacking-ansambl tarkibiga uchta baza modeli va bitta meta-model kiritilgan. Baza modellari sifatida Random Forest [10] (500 ta daraxt, maksimal chuqurlik 25), XGBoost [11] (learning rate 0,05, maksimal chuqurlik 8, 300 ta daraxt) va yengil arxitekturadagi ko‘p qatlamli perseptron (MLP, 3 ta yashirin qatlam: 128, 64, 32 neyron, ReLU aktivatsiya, Dropout 0,3) tanlandi. Meta-model sifatida Logistic Regression qo‘llanildi, bu baza modellarining chiqish ehtimolliklarini birlashtirib, yakuniy qarorni chiqaradi.

Har uchala baza modelini birgalikda qo‘llashning nazariy asosi shundaki, ular turli ta’lim paradigmalariga mansub: Random Forest chetga chiquvchi qiymatlarga chidamli [10], XGBoost nozik naqshlarni yaxshi aniqlaydi [11], MLP esa belgilar orasidagi chiziqsiz o‘zaro bog‘liqliklarni modellashtiradi. Ularni stacking orqali birlashtirish [12] model umumlashtirish qobiliyatini oshiradi va ayrim modellarning kuchsiz tomonlarini kompensatsiya qiladi.

3.2. Aniqlash metodikasi

Taklif etilgan metodika quyidagi ketma-ket bosqichlardan iborat:

DOI: 10.65322/j.srd.02162026.17

• 1-bosqich. Trafikni yig‘ish: port-mirroring yoki tap orqali tarmoq trafigini yig‘ish, PCAP formatida saqlash.

• 2-bosqich. Oqimlarga ajratish: trafikni 5-li identifikator (manba IP, nishon IP, manba port, nishon port, protokol) asosida oqimlarga ajratish, oqim tugash mezoni – 120 soniya sukut yoki FIN/RST bayrog‘i.

• 3-bosqich. Belgilarni ekstraktsiya qilish: har bir oqim uchun 17 ta tanlangan belgini hisoblash, shu jumladan 4 ta entropik belgi.

• 4-bosqich. Normallashtirish: belgilar qiymatlarini MinMax usuli bilan [0, 1] oralig‘iga keltirish.

• 5-bosqich. 1-bosqich tasniflash: dastlabki qoidalar asosida aniq qonuniy oqimlarni filtrdan o‘tkazish.

• 6-bosqich. 2-bosqich tasniflash: shubhali oqimlarni stacking-ansambl orqali yakuniy tasniflash.

• 7-bosqich. Qaror qabul qilish: agar oqim hujum sifatida tasniflansa, xavfsizlik operatori markaziga ogohlantirish jo‘natish yoki avtomatik bloklash qoidasini shakllantirish.

• 8-bosqich. Natijalarni jurnal faylga yozish va davriy hisobot tayyorlash.

2.6. Eksperimental stend va baholash ko‘rsatkichlari

Eksperimental stend VMware ESXi 7.0 gipervizori asosida yig‘ildi va quyidagi komponentlardan tashkil topdi: nishon veb-server (Apache 2.4, PHP 8.1, MySQL 8.0, Ubuntu Server 22.04 LTS) konfiguratsiyasi standart holatda qoldirildi; besh dona qonuniy foydalanuvchi mijozlari avtomatlashtirilgan Selenium skriptlari orqali haqiqiy foydalanuvchi xatti-harakatini simulyatsiya qildi; o‘ntagacha hujumchi mijozlari Slowloris, Slow Read, slowhttptest, hulk va maxsus yozilgan Shrew skripti orqali hujum generatsiya qildi. Trafikni yig‘ish ikkita tarmoq interfeysini qamrab oluvchi port-mirroring rejimida amalga oshirildi. Har bir eksperimental ssenariy kamida 3 marta takrorlanib, natijalarning o‘rtacha qiymati va standart og‘ishi hisoblandi.

Modelni baholash uchun quyidagi ko‘rsatkichlar qo‘llanildi: Accuracy – to‘g‘ri tasniflangan namunalar ulushi; Precision – aniqlangan hujumlar orasida haqiqiy hujumlarning ulushi; Recall (Sensitivity) – haqiqiy hujumlar orasida to‘g‘ri aniqlanganlarining ulushi; F1-score – Precision va Recallning garmonik o‘rtachasi; False Positive Rate (FPR) – qonuniy trafikning noto‘g‘ri hujum deb belgilangan ulushi; AUC-ROC – ROC egri chizig‘i ostidagi maydon; shuningdek, amaliy baholash uchun bitta oqimni tasniflash vaqti va modelning umumiy kechikishi.

4. Tadqiqot natijalari

4.1. Trafik xususiyatlarining tahlili

Dastlabki tahlil bosqichida past intensivli DDoS hujumlari davrida kuzatilgan trafikning statistik va entropik xususiyatlari tizimli tarzda o‘rganildi. Tahlil natijalari shuni ko‘rsatdiki, LR-DDoS seanslarida paketlararo intervalning Shannon entropiyasi qonuniy trafikka nisbatan o‘rtacha 23–31% ga pasayadi. Bu qonuniyat, ayniqsa, Shrew turidagi hujumlarda yaqqol namoyon bo‘ldi, chunki Shrew hujumi TCP qayta jo‘natish taymeriga moslashgan davriy impulslardan iborat bo‘lib, bu impulslar deyarli bir xil intervallarda takrorlanadi. Slowloris va Slow Read hujumlarida esa entropiya pasayishi kamroq (17–23% atrofida), biroq oqim davomiyligi va yarim ochiq sessiyalar soni bo‘yicha keskin farqlar qayd etildi.

Ikkinchi muhim qonuniyat shundaki, LR-DDoS seanslarida TCP oqimlarining o‘rtacha davomiyligi qonuniy trafikka nisbatan 4,7–6,2 marta oshdi. Masalan, qonuniy HTTP sessiyalarining o‘rtacha davomiyligi 8,2 soniyani tashkil etgan bo‘lsa, Slowloris hujumi davrida bu ko‘rsatkich 42,6 soniyaga yetdi. Shu bilan birga, server tomonidagi yarim ochiq ulanishlar soni 8–12 marta ko‘payishi qayd etildi, bu esa server resurslarining tugashiga olib keladigan asosiy mexanizmdir. Uchinchi qonuniyat – bir vaqtning o‘zida ochiq oqimlar soni keskin oshishi; hujumchining har bir mijozi o‘rtacha 150–200 ta yarim ochiq sessiya saqlab turdi.

DOI: 10.65322/j.srd.02162026.17

4.2. Belgilarni tanlash natijalari

Belgilarni tanlash jarayonida 84 ta dastlabki belgi orasidan eng informativ 17 tasi aniqlandi. Mutual Information qiymatlari bo‘yicha birinchi o‘rinda Flow IAT Mean (I = 0,684), Fwd IAT Std (I = 0,641), Flow Duration (I = 0,628), Idle Mean (I = 0,597) va Fwd IAT Entropy (I = 0,573) turdi. RFE usuli ham shu belgilarni eng yuqori ahamiyatga ega deb topdi. Qiziq jihat shundaki, ba’zi an’anaviy belgilar – Total Bytes va Source IP Entropy – MI qiymati bo‘yicha past baholangan, bu LR-DDoS hujumlarining band kenglik bo‘yicha anomaliya ko‘rsatmasligi va cheklangan sonli manbalardan jo‘natilishi bilan izohlanadi.

1-jadval

Eng informativ 17 ta belgi va ularning ahamiyat koeffitsiyentlari

№	Belgi nomi	MI qiymati	RFE darajasi
1	Flow IAT Mean	0,684	1
2	Fwd IAT Std	0,641	2
3	Flow Duration	0,628	3
4	Idle Mean	0,597	4
5	Fwd IAT Entropy	0,573	5
6	Bwd IAT Mean	0,541	6
7	Active Mean	0,518	7
8	Packet Length Variance	0,492	8
9	Flow Packets/s	0,467	9
10	PSH Flag Count	0,441	10
11	Fwd Packet Length Std	0,418	11
12	Idle Std	0,394	12
13	Flow IAT Entropy	0,372	13
14	Min Packet Length	0,351	14
15	FIN Flag Count	0,329	15
16	Bwd IAT Std	0,308	16
17	ACK Flag Count	0,287	17

4.3. Aniqlash modelining natijalari

Taklif etilgan gibrid model va solishtirish ob’ekti sifatida tanlangan beshta mavjud usul CIC-DDoS2019 ma’lumotlar to‘plamida qiyosiy baholandi. Solishtirish uchun quyidagi usullar tanlandi: entropiyaga asoslangan chegaraviy tahlil, Random Forest (500 daraxt), XGBoost (300 daraxt), MLP (3 qatlam), shuningdek, adabiyotda tavsiflangan LUCID-CNN modeli. Natijalar quyidagi 2-jadvalda keltirilgan.

DOI: 10.65322/j.srd.02162026.17

2-jadval

Aniqlash usullarining qiyosiy natijalari (CIC-DDoS2019)

Usul	Accuracy	Precision	Recall	F1-score	FPR
Entropiyaviy chegara	0,842	0,811	0,796	0,803	0,094
Random Forest	0,921	0,908	0,895	0,901	0,051
XGBoost	0,934	0,927	0,912	0,919	0,043
MLP (baseline)	0,916	0,903	0,891	0,897	0,057
LUCID-CNN	0,948	0,939	0,931	0,935	0,034
Taklif etilgan model	0,976	0,971	0,968	0,969	0,018

2-jadvaldan ko‘rinib turibdiki, taklif etilgan gibrid model barcha ko‘rsatkichlar bo‘yicha solishtirish ob’ekti sifatida olingan usullardan ustun natija ko‘rsatdi. Xususan, Accuracy 0,976 ga, F1-score 0,969 ga yetdi, False Positive Rate esa 0,018 gacha pasaytirildi. Eng yaqin raqobatchi bo‘lgan LUCID-CNN modeliga [8] nisbatan Accuracy 2,8 foiz punkt, FPR esa deyarli 1,9 marta yaxshilandi. Bu ko‘rsatkichlar amaliy qo‘llanish uchun muhim, chunki yuqori FPR operator xodimlariga ortiqcha signallar yukini tashlaydi, past FPR esa xavfsizlik operatsiya markazining (SOC) samaradorligini oshiradi.

4.4. Hujum turlari bo‘yicha natijalar

Modelning har bir LR-DDoS turi bo‘yicha alohida samaradorligi ham tahlil qilindi. Natijalar quyidagi 3-jadvalda keltirilgan.

3-jadval

Taklif etilgan modelning LR-DDoS turlari bo‘yicha natijalari

Hujum turi	Precision	Recall	F1-score	Namunalar soni
Slowloris	0,981	0,976	0,978	42 318
Slow Read	0,973	0,965	0,969	38 142
Slow POST (RUDY)	0,968	0,959	0,963	29 847
Shrew	0,984	0,982	0,983	31 206
HTTP/2 Rapid Reset	0,951	0,944	0,947	18 732

3-jadvaldan ko‘rinadiki, model eng yuqori natijani Shrew (F1 = 0,983) va Slowloris (F1 = 0,978) hujumlarida ko‘rsatdi. Nisbatan pastroq natija HTTP/2 Rapid Reset hujumida (F1 = 0,947) kuzatildi, bu ushbu hujum turining yangiligi va o‘qitish to‘plamidagi namunalar sonining nisbatan kamligi bilan izohlanadi. Umuman olganda, barcha turlarda F1-score 0,94 dan yuqori bo‘ldi, bu modelning turli LR-DDoS turlariga umumlashtirilgan holda ishlay olishini tasdiqlaydi.

4.5. Natijalarning haqqoniyligini tekshirish

Olingan natijalarning haqqoniyligini (reliability) tekshirish maqsadida model alohida test to‘plami – laboratoriya stendida yig‘ilgan va o‘qitishda ishtirok etmagan original trafik bo‘yicha qo‘shimcha sinovdan o‘tkazildi. Bu holatda Accuracy 0,962, F1-score 0,954 va FPR 0,022 ni tashkil etdi. Ko‘rsatkichlarning CIC-DDoS2019 dagi natijalardan atigi 1–2 foiz punktga pasayishi modelning o‘qitish to‘plamiga ortiqcha moslashmaganini (overfitting kuzatilmaganini) va turli muhitlarda barqaror ishlashga qodirligini tasdiqlaydi. Bundan tashqari, bitta oqimni tasniflash

DOI: 10.65322/j.srd.02162026.17

uchun sarflangan o‘rtacha vaqt 2,3 ms ni tashkil etdi, bu real vaqtda ishlash talablariga to‘liq javob beradi.

5. Tadqiqot natijalari tahlili

Olingan natijalarni chuqur tahlil qilish shuni ko‘rsatadiki, past intensivli DDoS hujumlarini aniqlashda bitta turdagi belgilar (faqat statistik, faqat entropik yoki faqat vaqtli) yetarli emas. Muallif fikricha, LR-DDoS trafigining qonuniy trafikka o‘xshashligi ayni bitta o‘lchovda kuzatilsa-da, vaqt domeni, taqsimot domeni va entropik domenda birgalikda qaralganda farqlar sezilarli darajada namoyon bo‘ladi. Shu sababli belgilarning ko‘p o‘lchovli fazosidan foydalanish va ularni birlashtirgan ansambl modelini qo‘llash LR-DDoS aniqlash muammosiga maqbul yondashuv hisoblanadi. Bu xulosa nafaqat nazariy mulohazalar bilan, balki ikki bosqichli model va bitta bosqichli modellarning qiyosiy natijalari bilan ham asoslanadi: ikki bosqichli model bitta bosqichli XGBoost [13] modelidan 4,2 foiz punktga yuqori Accuracy ko‘rsatdi.

Mazkur tadqiqot natijalarini boshqa mualliflarning ishlari bilan solishtirganda quyidagi xulosalar olinadi. Sharafaldin va hamkasblari (CIC-DDoS2019 mualliflari) Random Forest yordamida LR-DDoS bo‘limida taxminan 0,93 F1-score ko‘rsatgan edilar [14]. Hoque va hamkasblari entropiyaga asoslangan yondashuvda 0,88–0,90 atrofidagi natijalarni bayon qilishgan [14]. Doriguzzi-Corin va hamkasblarining LUCID-CNN modeli 0,94 atrofida F1-score ko‘rsatgan [15]. Taklif etilgan model ushbu natijalardan 3–8 foiz punktga ustun kelishi, shuningdek, FPR ni 2–3 barobar kamaytira olishi bilan ajralib turadi. Bu ustunlik, birinchidan, belgilarni tanlashning ikki bosqichli (MI + RFE) metodikasi; ikkinchidan, stacking-ansambl arxitekturasi; uchinchidan, dastlabki filtratsiya orqali shubhali oqimlargagina chuqur tahlil qo‘llash hisobiga erishildi.

Shu bilan birga, tadqiqot davomida bir qator cheklovlar va yechimini talab qiluvchi muammolar ham yuzaga keldi. Birinchidan, model oqim tugagandan so‘ng yakuniy qaror chiqaradi, bu esa juda uzoq sessiyalardan foydalanadigan Slow Read turidagi hujumlarda aniqlashning kechikishiga olib keladi. Kelgusi ishlarda oqim tugashini kutmasdan qisman oqim (partial flow) asosida qaror qabul qilish – masalan, har 10 soniyada oraliq hisob-kitoblarni yangilash yo‘llarini o‘rganish maqsadga muvofiqdir. Ikkinchidan, shifrlangan trafik (TLS 1.3, QUIC) sharoitida ba’zi statistik belgilarning informativligi pasayadi, biroq taklif etilgan modeldagi asosiy belgilar (oqim davomiyligi, paketlararo interval, entropiya) trafik mazmuniga bog‘liq emas va shifrlash sharoitida ham ishlashda davom etadi. Uchinchidan, adversarial mashinaviy o‘qitish hujumlari orqali model ishonchliligini buzish imkoniyati hisobga olinishi zarur; bu yo‘nalishda adversarial o‘qitish (adversarial training) va mudofaa distilatsiyasi kabi texnikalardan foydalanish istiqbolli yo‘nalishlardan biridir.

Taklif etilgan metodikaning amaliy qiymati shundaki, u mavjud IDS/IPS tizimlariga qo‘shimcha modul sifatida osonlikcha integratsiya qilinishi mumkin, chunki kirish ma’lumotlari sifatida standart PCAP fayllardan yoki NetFlow/IPFIX yozuvlaridan foydalanadi. Modelning hisoblash talablari nisbatan past bo‘lib (bitta oqimni tasniflash 2,3 ms, 100 Mbit/s trafikni real vaqtda tahlil qilish uchun o‘rtacha server quvvati yetarli), bu uni o‘rta va yirik korporativ tarmoqlarda, shuningdek, davlat axborot tizimlari segmentlarida joriy etishga imkon beradi. Mamlakatimizda raqamli iqtisodiyotning jadal rivojlanishi va davlat xizmatlarining elektronlashtirilishi sharoitida bunday yechimlarning dolzarbligi yanada ortadi.

6. Xulosalar

Tadqiqot natijalari shuni ko‘rsatdiki, axborot-telekommunikatsiya tizimlarida past intensivli taqsimlangan xizmatdan voz kechish (LR-DDoS) hujumlari zamonaviy kiberxavfsizlikning dolzarb va murakkab tahdidlaridan biri hisoblanadi. Ushbu turdagi hujumlarni samarali aniqlash uchun vaqt, taqsimot va entropik xususiyatlarni birgalikda hisobga oluvchi ko‘p o‘lchovli belgilar fazosiga asoslangan gibrid yondashuv zarur. Taklif etilgan ikki bosqichli model dastlabki filtratsiya va stacking-ansambl klassifikatsiya usullarini integratsiyalash orqali yuqori aniqlik va past yolg‘on ijobiy darajani ta’minladi. Xususan, CIC-DDoS2019 [3] ma’lumotlar

DOI: 10.65322/j.srd.02162026.17

to‘plamida Accuracy – 0,976, F1-score – 0,969 va FPR – 0,018 ko‘rsatkichlariga erishilib, bu natijalar mavjud entropik, statistik va mashinaviy o‘qitishga asoslangan yondashuvlardan ustun ekanligini ko‘rsatdi.

Belgilarni tanlash jarayonida Mutual Information va Recursive Feature Elimination usullarini uyg‘unlashtirgan ikki bosqichli metodika qo‘llanildi. Natijada dastlabki 84 ta belgidan 17 ta eng informativ belgi ajratib olinib, modelning hisoblash samaradorligi sezilarli darajada oshirildi hamda ortiqcha o‘lchamli ma’lumotlar ta’siri kamaytirildi. Ishlab chiqilgan metodika trafikni yig‘ish, belgilarni ekstraktsiya qilish, tasniflash va qaror qabul qilish bosqichlarini tizimli ravishda qamrab olib, tadqiqot natijalarining takrorlanuvchanligini va amaliy qo‘llanish imkoniyatini ta’minlaydi. Model beshta asosiy LR-DDoS hujum turlari (Slowloris, Slow Read, Slow POST, Shrew, HTTP/2 Rapid Reset) bo‘yicha barqaror yuqori natijalarni (F1 > 0,94) namoyish etdi, bu uning umumlashtirish qobiliyati yuqori ekanligini tasdiqlaydi.

Amaliy jihatdan, taklif etilgan yechim mavjud IDS/IPS tizimlariga qo‘shimcha modul sifatida integratsiya qilinishi mumkin bo‘lib, bank, davlat xizmatlari va sog‘liqni saqlash kabi kritik axborot infratuzilmalarini LR-DDoS hujumlaridan himoya qilishda samarali qo‘llanishi mumkin. Kelgusidagi tadqiqot yo‘nalishlari sifatida real vaqt rejimida oqimga asoslangan aniqlash mexanizmlarini ishlab chiqish, shifrlangan trafik (TLS 1.3, QUIC) sharoitida model samaradorligini oshirish, adversarial hujumlarga chidamli modellarni yaratish hamda turli masshtabdagi tarmoqlarda keng qamrovli sinovlarni o‘tkazish muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms // ACM SIGCOMM Computer Communication Review. – 2004. – Vol. 34, No. 2. – P. 39–53.

2. Zargar S.T., Joshi J., Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, No. 4. – P. 2046–2069.

3. Sharafaldin I., Lashkari A.H., Hakak S., Ghorbani A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy // IEEE ICCST. – 2019. – P. 1–8.

4. Hoque N., Bhattacharyya D.K., Kalita J.K. Botnet in DDoS Attacks: Trends and Challenges // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, No. 4. – P. 2242–2270.

5. Cambiaso E., Papaleo G., Chiola G., Aiello M. Slow DoS attacks: definition and categorisation // International Journal of Trust Management in Computing and Communications. – 2013. – Vol. 1, No. 3/4. – P. 300–319.

6. Somani G., Gaur M.S., Sanghi D., Conti M., Buyya R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions // Computer Communications. – 2017. – Vol. 107. – P. 30–48.

7. Chen Y., Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis // Journal of Parallel and Distributed Computing. – 2006. – Vol. 66, No. 9. – P. 1137–1151.

8. Doriguzzi-Corin R., Millar S., Scott-Hayward S., Martínez-del-Rincón J., Siracusa D. LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection // IEEE Transactions on Network and Service Management. – 2020. – Vol. 17, No. 2. – P. 876–889.

9. Shannon C.E. A Mathematical Theory of Communication // The Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423, 623–656.

10. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32.

DOI: 10.65322/j.srd.02162026.17

11. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD. – 2016. – P. 785–794.

12. Wolpert D.H. Stacked Generalization // Neural Networks. – 1992. – Vol. 5, No. 2. – P. 241–259.

13. Yungaicela-Naula N.M., Vargas-Rosales C., Perez-Diaz J.A. SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning // IEEE Access. – 2021. – Vol. 9. – P. 108495–108512.

14. Praseed A., Thilagam P.S. DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, No. 1. – P. 661–685.

15. Imperva. HTTP/2 Rapid Reset: CVE-2023-44487 Technical Analysis. – 2023. – [Elektron resurs] https://www.imperva.com/blog/http-2-rapid-reset/