MIRZO ULUG'BEK NOMIDAGI
O'ZBEKISTON MILLIY UNIVERSITETINING
JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

RESPUBLIKA ILMIY-TEXNIK ANJUMAN MATERIALLARI TO‘PLAMI

15-16-MAY
2026-YIL

doi

Google Scholar

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami

(2026-yil 15-16-may)

JIZZAX-2026

Foydalanilgan adabiyotlar.

1.Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University Doctoral Dissertation.

2.Acar, A., et al. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys,51(4), 1-38.

3.Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT).

4.Fan, J., & Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive.

5.Microsoft Research. (2023). Microsoft SEAL (Simple Encrypted Arithmetic Library) Manual. GitHub Repository.

6.Zokirov, S., & Karimov, A. (2022). Kriptografik usullar va ma'lumotlar himoyasi: Oliy o'quv yurtlari uchun darslik. Toshkent: "Fan va texnologiya".

7.Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM).

8.National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography Standardization Process.

LOKAL TARMOQLARDA DoS/DDoS HUJUMLARNI ERTA ANIQLASH ALGORITMI

Yusupov Behzod Ismoil o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universitetining Jiizzax filiali
Axborot tizimlari va texnologiyalari kafedrasi o'qituvchisi
Abduazimov Ravshan Azamat o'g'li, Elmurodov Xusan Ulug'bek o'g'li va Akaboyev Xolboy O'ralboy o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston
Milliy universitetining Jizzax filiali Amaliy matematika fakulteti
Axborot tizimlari va texnologiyalari yo'nalishi talabalari
ravshan200605@gmail.com

Annotatsiya. Ushbu maqolaning asosiy maqsadi lokal kompyuter tarmoqlarida yuzaga keladigan Denial-of-Service attack (DoS) va DDoS hujumlarini erta bosqichda aniqlash usullarini o'rganishdan iborat. Ishda tarmoq trafigidagi o'zgarishlarni tahlil qilish orqali anomaliyalarni aniqlashga asoslangan algoritm ishlab chiqish ko'zda tutilgan. Shuningdek, paketlar oqimi va trafik intensivligi asosida hujumlarni aniqlash mexanizmi taklif etiladi. Maqolada ishlab chiqilgan algoritmning amaliy jihatdan qo'llanilishi va samaradorligi ko'rib chiqiladi. Tadqiqot natijalari tarmoq xavfsizligini oshirish hamda xizmat uzilishlarini oldini olishga xizmat qiladi.

Kalit so‘zlar: DoS, DDoS, tarmoq xavfsizligi, trafik tahlili, anomaliya aniqlash, IDS/IPS, paketlar oqimi, kiberxavfsizlik, lokal tarmoqlar.

Denial-of-Service attack (DoS) — bu kompyuter tizimi yoki tarmoq xizmatining foydalanuvchilar uchun mavjudligini vaqtincha yoki butunlay izdan chiqarishga qaratilgan kiberhujum turidir. Bunday hujumning asosiy maqsadi server, tarmoq qurilmasi yoki xizmat resurslarini (protsessor, xotira, tarmoq kanali) ortiqcha yuklash orqali uning normal ishlashini to‘xtatishdan iborat. Natijada qonuniy foydalanuvchilar tizimdan foydalana olmaydi yoki xizmat sifati keskin pasayadi. DoS hujumlarining asosiy xususiyati shundaki, ular odatda bitta manbadan amalga oshiriladi. Masalan, hujumchi bir dona kompyuterdan serverga juda ko‘p miqdorda so‘rovlar yuboradi. Bu esa serverni haddan tashqari band qilib qo‘yadi. Biroq, zamonaviy himoya tizimlari bunday hujumlarni nisbatan oson aniqlay oladi, chunki trafik bitta IP manzildan keladi.

Shundan farqli ravishda, DDoS (Distributed Denial of Service) hujumlari ancha murakkab va xavfli hisoblanadi. Bu turdagi hujumlarda bir nechta, hatto minglab kompyuterlar bir vaqtning o‘zida nishon tizimga hujum qiladi. Odatda bu kompyuterlar “botnet” deb ataluvchi tarmoqni tashkil qiladi, ya’ni zararli dastur bilan zararlangan qurilmalar hujumchining buyrug‘i bilan ishlaydi. Shu sababli DDoS hujumlarini aniqlash va oldini olish ancha qiyin, chunki trafik turli manbalardan keladi va u oddiy foydalanuvchi faoliyatiga o‘xshab ko‘rinishi mumkin.

DoS va DDoS hujumlari bir nechta turlarga bo‘linadi. Eng keng tarqalgan turlaridan biri — SYN Flood hujumi. Bu hujum TCP protokolining ulanish o‘rnatish mexanizmidagi zaiflikdan foydalanadi. Hujumchi serverga ko‘plab SYN so‘rovlar yuboradi, lekin ulanishni oxirigacha yakunlamaydi. Natijada server yarim ochiq ulanishlar bilan to‘lib qoladi va yangi ulanishlarni qabul qila olmaydi. Yana bir keng tarqalgan tur — UDP Flood hujumi. Bu holatda hujumchi serverga katta hajmda UDP paketlar yuboradi. Server esa har bir paketga javob qaytarishga harakat qiladi, bu esa tizim resurslarini tezda tugatadi. UDP protokoli ulanishsiz bo‘lgani sababli bunday hujumlarni filtrlash qiyinroq bo‘ladi.

Anomaliyalarni aniqlash esa tarmoqdagi odatiy holatdan chetga chiqadigan faoliyatni topishga qaratilgan. Anomaliya deganda normal trafikdan keskin farq qiladigan yoki shubhali harakatlar tushuniladi. Bunday holatlarga trafikning keskin oshib ketishi, noma’lum IP manzillardan ko‘p so‘rovlar kelishi, g‘ayritabiiy portlardan foydalanish yoki tizimga ruxsatsiz kirishga urinishlar kiradi. Anomaliyalar ko‘pincha kiberhujumlar belgisi bo‘lishi mumkin. Masalan, DDoS hujumlar vaqtida tarmoqqa juda katta hajmda so‘rovlar yuborilib, server ishlashini sekinlashtiradi yoki butunlay ishdan chiqaradi. Shuningdek, zararli dasturlar tarmoq orqali yashirincha ma’lumot yuborishi ham anomaliya sifatida aniqlanishi mumkin.

Anomaliyalarni aniqlashning bir nechta usullari mavjud. Statistik usullarda tarmoqning normal ishlash ko‘rsatkichlari o‘rganilib, undan chetga chiqishlar aniqlanadi. Imzo asosidagi usulda esa oldindan ma’lum bo‘lgan hujumlar yoki xavfli harakatlar bazasi bilan solishtirish amalga oshiriladi. Eng zamonaviy usullardan biri esa sun’iy intellekt va mashinaviy o‘rganish algoritmlaridan foydalanish bo‘lib, bunda tizim o‘zi normal trafikni o‘rganadi va undan og‘ishlarni mustaqil aniqlay oladi.

Tarmoq trafigini tahlil qilish va anomaliyalarni aniqlash jarayonida turli vositalardan foydalaniladi. Masalan, Wireshark dasturi tarmoq paketlarini chuqur tahlil

qilish imkonini beradi. Snort tizimi esa kiberhujumlarni aniqlash va ularga qarshi choralar ko‘rishga yordam beradi. Zabbix va Nagios kabi monitoring tizimlari esa tarmoq va serverlarning holatini doimiy kuzatib boradi.

Zamonaviy tarmoqlarda Denial-of-Service attack hujumlarini erta aniqlash xizmat uzilishlarining oldini olishda muhim ahamiyatga ega. Ushbu bo‘limda tarmoq trafigidagi o‘zgarishlarga asoslangan sodda, lekin samarali algoritm taklif etiladi. Ushbu algoritm paketlar oqimi va trafik intensivligining keskin oshishini aniqlash orqali hujum ehtimolini baholaydi. Taklif etilayotgan algoritmning asosiy g‘oyasi tarmoqdagi normal trafik bilan anomaliyali trafikni solishtirishga asoslanadi. Oddiy holatda tarmoq trafigi ma’lum diapazonda o‘zgaradi va keskin sakrashlar kuzatilmaydi. Biroq DoS yoki DDoS hujumi sodir bo‘lganda, juda qisqa vaqt ichida paketlar soni keskin oshib ketadi. Shu sababli, agar ma’lum vaqt oralig‘ida trafik hajmi odatiy qiymatdan keskin farq qilsa, bu anomaliya sifatida baholanadi va hujum ehtimoli mavjud deb hisoblanadi. Algoritm aynan shu o‘zgarishlarni aniqlashga qaratilgan.

Threshold usuli — bu eng sodda va tezkor aniqlash mexanizmlaridan biri bo‘lib, unda tarmoq trafigi uchun maksimal ruxsat etilgan qiymat belgilanadi. Ushbu qiymat tarmoqning normal ishlash holatiga qarab aniqlanadi. Masalan, agar normal sharoitda tarmoqda 50–100 paket/sekund uzatilsa, threshold qiymati 200 paket/sekund qilib belgilanadi. Agar real vaqtda kuzatilayotgan trafik ushbu qiymatdan oshib ketsa, tizim bu holatni xavfli deb baholaydi. Bu usulning afzalligi — tezkorligi va soddaligidir. Biroq threshold qiymatini noto‘g‘ri tanlash noto‘g‘ri signal (false positive yoki false negative) berishiga olib kelishi mumkin.

Quyida taklif etilgan algoritmning soddalashtirilgan ishlash tartibi keltirilgan:

Mazkur algoritm sodda bo‘lishiga qaramay, real tizimlarda dastlabki himoya mexanizmi sifatida samarali ishlaydi. U resurslarni kam talab qiladi va real vaqt rejimida ishlay oladi. Shu bilan birga, uni yanada rivojlantirish orqali sun’iy intellekt yoki mashinaviy o‘rganish usullari bilan birlashtirish mumkin.

Dasturda ikki xil trafik ishlatildi:

- **Normal trafik**: 50–100 paket/sekund
- **Hujum trafigi**: 300–500 paket/sekund

Threshold qiymati 200 paket/sekund qilib belgilandi. Bu qiymatdan yuqori bo‘lgan holatlar hujum sifatida baholandi.

Vaqt(sekund)	Paketlar soni	Holat
1	65	Normal
10	88	Normal
21	320	Hujum aniqlandi
25	410	Hujum aniqlandi

Olingan natijalar shuni ko‘rsatadiki, threshold usuliga asoslangan algoritm oddiy DoS/DDoS hujumlarini aniqlashda samarali ishlaydi. Trafik keskin oshgan paytda tizim tezkor ravishda hujumni aniqlaydi va ogohlantirish beradi.Shu bilan birga, ushbu yondashuvning ayrim cheklovlari ham mavjud. Masalan, threshold qiymati noto‘g‘ri tanlansa, tizim noto‘g‘ri signal berishi mumkin.

Xulosa

Ushbu maqolada lokal kompyuter tarmoqlarida Denial-of-Service attack (DoS) va DDoS hujumlarini erta aniqlash masalasi ko‘rib chiqildi. Tarmoq trafigini tahlil qilish asosida ishlovchi oddiy va samarali algoritm taklif etildi hamda uning dasturiy realizatsiyasi amaliy misollar yordamida sinovdan o‘tkazildi. O‘tkazilgan tajribalar natijasida shuni ko‘rish mumkinki, tarmoq trafigidagi keskin o‘zgarishlar asosida hujumlarni aniqlash mumkin. Simulyatsiya qilingan trafik ma’lumotlari orqali threshold qiymatidan oshgan holatlar muvaffaqiyatli aniqlanib, tizim tomonidan hujum sifatida belgilandi. Bu esa algoritmning ishlash tamoyili to‘g‘ri tanlanganini ko‘rsatadi. Taklif etilgan algoritm soddaligi va tez ishlashi bilan ajralib turadi. U real vaqt rejimida ishlash imkoniyatiga ega bo‘lib, minimal hisoblash resurslarini talab qiladi. Ayniqsa, oddiy DoS va DDoS hujumlarini aniqlashda yuqori samaradorlik ko‘rsatadi. Biroq murakkab va past intensivlikdagi hujumlarni aniqlashda uning samaradorligi biroz pasayishi mumkin.

Foydalanilgan adabiyotlar:

1. **Mamarayimov A.** Kriptografiyaning zamonaviy ko‘rinishi.
2. **Bhuyan M. H., Bhattacharyya D. K., Kalita J. K.** Network Anomaly Detection: Methods, Systems and Tools // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, No. 1. – Pp. 303–342.
3. **Al-Haija Q. A., Al-Badawi A.** AI-based intrusion detection systems in IoT networks: A survey // Future Internet. – 2021. – Vol. 13, No. 11. – P. 266.
4. **Aldhaheri S., Alghazzawi D., Cheng L.** Artificial Intelligence and Machine Learning for Intrusion Detection Systems: A Survey // Applied Sciences. – 2022. – Vol. 12, No. 20. – P. 10216.
5. **Qodirov F. E.** DDoS hujumlari va ularni bartaraf etish usullari.
6. **Madrahimov Z. E., Olimboyev H. K.** Deep learning asosida DDoS hujumlarini aniqlash: optimallashtirilmagan va optimallashtirilgan ma'lumotlar bilan ishlash.

RAQAMLI IQTISOD VA INNOVATSION AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARINI JORIY ETISHNING DOLZARB MASALALARI

Abduxakimova Maftuna

G‘ofur qizi O‘zMu JF " Amaliy matematika" kafedrasi o‘qituvchisi

Abdulaziz Mirzaqobilov O'tkir o'g'li

O'zMU JF Iqtisodiyot yo'nalishi talabasi

abduhakimova1995@gmail.com

abdulazizmirzaqobilov0@gmail.com

Annotatsiya: Ushbu maqola raqamli iqtisodiyot va innovatsion axborot-kommunikatsiya texnologiyalarini joriy etishning dolzarb masalalarini o‘rganadi.