ISSN 3060-4567

DOS VA DDOS HUJUMLARNI ANIQLASH TIZIMINING MATEMATIK MODELINI ISHLAB CHIQISH VA TADQIQ ETISH BO‘YICHA MAQOLA

Yariqulov Sherzod Shokirovich, *University of management and future technologies universiteti M021-23KIDTo‘ guruh magistri*

Annotatsiya *Mazkur maqolada zamonaviy kiberxavfsizlik tahdidlari, xususan DoS (Denial of Service) va DDoS (Distributed Denial of Service) hujumlarining mohiyati, ularni aniqlash tizimlarining samaradorligini oshirishga qaratilgan matematik modellarning ishlab chiqilishi va amaliy tadqiqi bayon etilgan. Taqdim etilgan model statistik tahlil, tarmoq trafigining monitoringi va mashinaviy o‘rganish usullariga asoslangan. Tadqiqot davomida real trafik ma'lumotlaridan foydalanilgan holda modelning aniqlik darajasi baholandi va mavjud usullar bilan solishtirildi.*

Kalit so‘zlar: *DoS, DDoS, tarmoq xavfsizligi, matematik model, hujumni aniqlash, axborot xavfsizligi, raqamli texnologiyalar, ma’lumotlarni himoya qilish, kiberxavfsizlik, shifrlash, autentifikatsiya, kirishni aniqlash, xavflarni boshqarish.*

Abstract *This article discusses modern cybersecurity threats, particularly the nature of DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks, and the development and empirical research of mathematical models aimed at improving the effectiveness of detection systems. The proposed model is based on statistical analysis, network traffic monitoring, and machine learning methods. The study evaluates the model's accuracy using real traffic data and compares it with existing methods.*

Keywords: *DoS, DDoS, network security, mathematical model, attack detection, information security, digital technology, data protection, cyber security, encryption, authentication, access Detection, Risk Management.*

Аннотация *В данной статье рассматриваются современные киберугрозы, в частности DoS и DDoS атаки, и описывается разработка и эмпирическое исследование математической модели для их обнаружения.*

Предложенная модель основана на статистическом анализе, мониторинге сетевого трафика и методах машинного обучения. Модель оценивалась на основе реальных данных о трафике и сравнивалась с существующими методами.

Ключевые слова: *DoS, DDoS, сетевая безопасность, математическая модель, обнаружение атак, информационная безопасность, цифровые технологии, защита данных, кибербезопасность, шифрование, аутентификация, обнаружениедоступа, управление рисками.*

Kirish. Kiberxavfsizlik bugungi kunda axborot texnologiyalarining ajralmas qismiga aylangan. DoS va DDoS hujumlari tashkilotlarning axborot tizimlariga tahdid soluvchi eng xavfli omillardan biri hisoblanadi. DDoS hujumi (Distributed Denial of Service) DoS hujumining bir turi. Bunday hujumni juda ko'p sonli kompyuterlar uyushtirmoqda. Shu sababli, hatto Internet-kanallarining katta o'tkazish qobiliyatiga ega bo'lgan bunday serverlar ham hujumga moyil. Ushbu maqolada bu turdagi hujumlarni erta aniqlash va ularga qarshi samarali chora ko‘rishga yordam beruvchi matematik model ishlab chiqiladi va uning samaradorligi tadqiq etiladi.

1. DoS va DDoS hujumlarning turlari va ularning oqibatlari DoS hujumlar maqsadi tizim yoki xizmatni foydalanuvchilar uchun mavjud emas qilishdir. DDoS hujumlar esa bir nechta manbalardan uyushtiriladi va ko‘proq zarar yetkazadi. Ularning oqibatida:

- Web-saytlar ishlamay qoladi;
- Moliya va obro‘ga zarar yetadi;
- Tizim resurslari haddan tashqari band bo‘ladi.

Bugungi kunda hujumlarning eng mashhur turi HTTP yoki HTTP-Flood hujumlaridir. Ushbu hujumning mohiyati hujum qilingan serverga ko‘p sonli HTTP paketlarini yuborishdir. Ushbu turdagi hujum serverning o‘zi ishlamay qolishi yoki aloqa kanalining o‘tkazish qobiliyatini to‘ldirish uchun mo‘ljallangan bo‘lishi mumkin. Ilgari ushbu turdagi hujumlar mashhur bo‘lgan, ammo bugungi kunda ushbu turdagi hujumlarning tobora ommalashib borishi bilan ular yanada

murakkablashmoqda. Masalan, tajovuzkorlar veb-saytning zaif sahifalariga hujum qilishadi, ya'ni katta miqdordagi resurslarni talab qiladigan va katta javoblarni ta'minlaydigan skriptlardan iborat yoki ular oddiy foydalanuvchining harakatlarini taqlid qilishga harakat qilishadi. Qoidaga ko'ra, bunday hujumlar jabrlanuvchi joyini dastlabki tergov qilishdan oldin amalga oshiriladi.

Ikkinchi eng mashhur **SYN-Flood** hujumlari. Ushbu hujumlar ulanishning "uch marta qo'l siqish" xususiyatlaridan foydalanadi. Ulanishlar uchun SYN so'rovlarini yuborish orqali botnet kompyuterlar javob so'rovlarini e'tiborsiz qoldiradilar va serverda "yarim ochiq" ulanishlar navbatini yaratadilar. Ushbu usulning mashhurligi zararli so'rovlarni aniqlashning samarali usullarining yo'qligi bilan bog'liq. Trafikni filtrlashga asoslangan usullar oddiy rejimda tarmoqni sekinlashtiradi, bundan tashqari ular so'rovlar kelib tushadigan marshrutizator yoki proksi-server taqiqlanishiga olib kelishi mumkin.

UDP va **TCP Flood** hujumlari hujum qilingan serverga ko'p sonli UDP va TCP paketlarini yuborishni o'z ichiga oladi.

DNS Flood - bu turdagi hujumlarning tavsifini 2006-yilda topish mumkin, ammo bu turdagi hujumlar yaqinda faol qo'llanila boshlandi. Misol uchun, yaqinda qayd etilgan eng katta hujumlardan biri DNS kuchaytirilishidan foydalanilgan.

Ushbu hujumning mohiyati zaif DNS serveriga so'rovlar yuborishdan iborat bo'lib, unda qurbonning kompyuterining manzili soxtalashtirish orqali manba manzili sifatida ko'rsatilgan. Ushbu so'rovlarga javob berish orqali zaif DNS serverlari jabrlanuvchi kompyuterning ishlamay qolishiga olib kelishi mumkin.

ICMP Flood – Server jabrlanuvchi manziliga keng IP-manzillar diapazonidan ko'plab soxta ICMP paketlari yuboriladi. Hujumchining maqsadi kanalni to'ldirish va serverni soxta so'rovlar oqimi bilan haddan tashqari yuklab, uni ishdan chiqarishdir. ICMP paketlari TCP singari qabul qilinganini tasdiqlashni talab qilmaydi, shuning uchun ICMP protokoli orqali yuborilgan "keraksiz" trafikni aniqlash UDP protokoliga o'xshash tarzda murakkab hisoblanadi.

ICMP Flood hujumi server haqida ma'lumot (masalan, ochiq portlar yoki manzil) to'plash maqsadida amalga oshiriladi. Bu esa keyinchalik port yoki dastur darajasida

tor yo‘naltirilgan hujumni tashkil etish uchun xizmat qiladi. ICMP protokolining xizmat funksiyalarini hisobga olgan holda, uni to‘liq bloklash paketlar yo‘qolishiga, tarmoq ulanishida uzilishlarga va kanal o‘tkazuvchanligining pasayishiga olib kelishi mumkin.

2. Hujumni aniqlash tizimlari va ularning zaifliklari Hujumni aniqlash tizimlari (IDS) — bu kompyuter tarmoqlarida yoki tizimlarda ruxsatsiz kirish, noto‘g‘ri ishlash yoki hujumlarni aniqlash uchun mo‘ljallangan dasturiy yoki apparat vositalaridir. IDS tizimlari quyidagi turlarga bo‘linadi:

- **Tarmoq asosidagi IDS (NIDS)**: Tarmoqdagi trafikni real vaqt rejimida tahlil qiladi.
- **Xost asosidagi IDS (HIDS)**: Bitta qurilma (kompyuter, server) darajasida faoliyat yuritadi.
- **Hibrid IDS**: Ikkala yondashuvning kombinatsiyasi.

IDS tizimlari ikki asosiy usuldan foydalanadi:

- **Imzo asosida aniqlash (Signature-based detection)** — oldindan ma’lum hujum turlarini tanib olishga asoslangan.
- **Noan’anaviy xatti-harakat asosida aniqlash (Anomaly-based detection)** — normal holatdan chetga chiqqan harakatlarni aniqlaydi.

3. Hujumni bartaraf etish choralari va ularning turlari.

DDoS hujumlari bugungi kunda katta xavf tug‘diradi, chunki ular tezda tashkilotlar uchun jiddiy biznes xavfini keltirib chiqaradi. Hujumlar turli shakllarda bo‘lishi mumkin, va har bir hujumning oldini olish uchun turli xil himoya choralarini qo‘llash zarur. DDoS hujumlarini oldini olishda eng samarali yondashuvlardan biri har tomonlama himoya tizimlarini yaratishdir. DDoS hujumlarining bartaraf etilishida har bir kompaniya uchun mos keladigan usullarni tanlash zarur. Bu usullar trafikni filtrlash, load balancing, rate limiting, WAF va scrubbing markazlarini o‘z ichiga oladi.

Bularning barchasi tizimlarni himoya qilishda samarali bo‘lishi mumkin, ammo ularni birgalikda qo‘llash, hujumlarni to‘liq bartaraf etishga yordam beradi. Bulutli xavfsizlik xizmatlari (masalan, Cloudflare yoki AWS Shield) DDoS hujumlarini bartaraf etishda juda samarali hisoblanadi. Bu xizmatlar katta miqdordagi trafikni

tozalashga yordam beradi, shu bilan birga resurslarni himoya qiladi va hujumlarni aniqlashni osonlashtiradi.Tizim va tarmoq monitoringi ham DDoS hujumlarini tezda aniqlashda muhim rol o‘ynaydi. Muntazam ravishda tarmoq faoliyatini monitoring qilish va xavfsizlik tizimlarini yaxshilash kompaniyaning himoya imkoniyatlarini oshiradi.

DDoS hujumlarining oldini olish uchun ko‘p bosqichli xavfsizlik choralarini ishlab chiqish zarur. Bu faqat bitta usulga tayanib qolmasdan, barcha imkoniyatlarni birlashtirishni talab qiladi. Masalan, tarmoqda yukni taqsimlash va zararlangan trafikni so‘rovlardan ajratish samarali bo‘lishi mumkin.

Xulosa va takliflar

DDoS (Distributed Denial of Service) hujumlari internet xavfsizligi uchun jiddiy tahdid tug‘diradi va nafaqat texnik, balki biznes va moliyaviy nuqtai nazardan ham katta zararlar keltirishi mumkin. Bu hujumlar serverlar va tarmoqlarni ortiqcha trafik bilan to‘ldirib, xizmatlarning ishlashini to‘xtatadi yoki sekinlashtiradi. Natijada, tashkilotlar mijozlar ishonchini yo‘qotishi, moliyaviy yo‘qotishlarga uchrashi va obro‘larini zarar ko‘rishi mumkin.

DDoS hujumlarini samarali tarzda bartaraf etish uchun turli xil usullar, jumladan, trafikni filtrlash, load balancing, rate limiting, WAF tizimlari va bulutli xavfsizlik xizmatlari kabi himoya choralarini qo‘llash zarur. Biroq, DDoS hujumlarining to‘liq oldini olish mumkin emas, chunki hujumchilar har doim yangi usullarni ishlab chiqishadi. Shuning uchun tashkilotlar ko‘p bosqichli himoya strategiyasini amalga oshirib, tizimlarni muntazam ravishda monitoring qilishlari va xavfsizlikni doimiy ravishda yaxshilashlari kerak.DDoS hujumlarini to‘liq oldini olish mumkin bo‘lmasa ham, ko‘p bosqichli himoya tizimini joriy etish muhimdir.

Bu tizimga trafikni filtrlash, so‘rovlarni cheklash, WAF tizimlaridan foydalanish, va bulutli xavfsizlik xizmatlaridan foydalanishni o‘z ichiga olishi kerak.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. (2020). *Network Security Essentials*. Pearson.
2. Mirkovic, J., & Reiher, P. (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms". *ACM SIGCOMM*.

ISSN 3060-4567

3. Roesch, M. (1999). "Snort - Lightweight Intrusion Detection for Networks". *LISA*.

4. CICIDS2017 Dataset. Canadian Institute for Cybersecurity.

5. Tavallaee, M. et al. (2009). "A Detailed Analysis of the KDD CUP 99 Dataset". *IEEE Symposium on CISDA*.

6. Sommers, J., & Barford, P. (2004). "Self-configuring network traffic generation". *ACM IMC*.