DDoS HUJUMLARI VA ULARDAN HIMOYALANISH USULLARI

DDoS АТАКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

DDoS ATTACKS AND METHODS OF PROTECTION AGAINST THEM

Ibragimov Sh.M.[1], Imomova M.J.[2]
[1]FarDU dotsenti, shavkat19702008@gmail.com
[2]FarDU talabasi, Imomovamarjona2002@gmail.com

Annotatsiya: *Ushbu maqolada DDoS (Distributed Denial of Service) hujumlarining zamonaviy axborot tizimlariga ta'siri va ularning ishlash prinsiplari tahlil qilindi. DDoS hujumlarining asosiy turlari, jumladan, volumetrik, protokol va ilova darajasidagi hujumlar o'rganildi hamda ularning tarmoq infratuzilmasiga yetkazadigan zarari yoritildi. Shuningdek, bunday hujumlardan himoyalanishning samarali usullari, jumladan trafikni filtrlash, yuklamani taqsimlash, IDS/IPS tizimlari va bulutli himoya texnologiyalari ko'rib chiqildi. Yuqoridagi yondashuvlar zamonaviy kiberxavfsizlikni ta'minlashda muhim ahamiyat kasb etadi.*

Kalit so'zlar: *DDoS hujum, xizmatdan voz kechish, kiberxavfsizlik, botnet, tarmoq hujumlari, trafik filtrlash, IDS/IPS, yuklamani taqsimlash, bulutli himoya, xavfsizlik.*

Аннотация: *В данной статье рассматриваются распределённые атаки отказа в обслуживании (DDoS) и их влияние на современные информационные системы. Проанализированы основные виды атак, включая объемные, протокольные и атаки на уровне приложений, а также их воздействие на сетевую инфраструктуру. Освещены эффективные методы защиты, такие как фильтрация трафика, балансировка нагрузки, системы IDS/IPS и облачные решения безопасности. Данные подходы играют важную роль в обеспечении современной кибербезопасности.*

Ключевые слова: *DDoS-атака, отказ в обслуживании, кибербезопасность, ботнет, сетевые атаки, фильтрация трафика, IDS/IPS, балансировка нагрузки, облачная защита, безопасность.*

Abstract: *This article examines Distributed Denial of Service (DDoS) attacks and their impact on modern information systems. The main types of attacks, including volumetric, protocol, and application-layer attacks, are analyzed along with their effects on network infrastructure. Effective protection methods such as traffic filtering, load balancing, IDS/IPS systems, and cloud-based security solutions are discussed. These approaches play a significant role in ensuring modern cybersecurity.*

Keywords: *DDoS attack, denial of service, cybersecurity, botnet, network attacks, traffic filtering, IDS/IPS, load balancing, cloud protection, security.*

KIRISH

Hozirgi raqamli jamiyatda internet va axborot texnologiyalarining jadal rivojlanishi turli xizmatlarning onlayn shaklga o‘tishiga olib keldi. Elektron tijorat, bank tizimlari, davlat xizmatlari va ijtimoiy platformalar faoliyati to‘liq yoki qisman tarmoqlarga bog‘liq bo‘lib qolmoqda. Shu bilan birga, ushbu tizimlarning uzluksiz ishlashi va ishonchliligini ta’minlash masalasi muhim ahamiyat kasb etmoqda. Aynan shu nuqtai nazardan, kiberxavfsizlik sohasida DDoS (Distributed Denial of Service) hujumlari eng dolzarb va xavfli tahdidlardan biri sifatida qaraladi.

DDoS hujumlari — bu ko‘plab manbalardan bir vaqtning o‘zida server yoki tarmoqqa ortiqcha so‘rovlar yuborish orqali uni ishlashdan chiqarishga qaratilgan hujum turidir. Bunday hujumlar odatda zararli dasturlar bilan zararlangan qurilmalardan tashkil topgan botnetlar orqali amalga oshiriladi. Natijada, server resurslari (protsessor, xotira, tarmoq kengligi) haddan tashqari yuklanadi va tizim qonuniy foydalanuvchilarga xizmat ko‘rsata olmay qoladi.

DDoS hujumlarining paydo bo‘lishi 1990-yillarning oxiri va 2000-yillarning boshlariga to‘g‘ri keladi. Dastlab ular nisbatan sodda shaklda bo‘lib, kichik hajmdagi tarmoqlarga qarshi qo‘llanilgan. Keyinchalik internet infratuzilmasining kengayishi va zararli dasturlar rivojlanishi natijasida DDoS hujumlari yanada murakkablashib, global miqyosdagi tizimlarga jiddiy zarar yetkaza boshladi. Masalan, yirik kompaniyalar, banklar va hatto davlat axborot tizimlari ham ushbu hujumlarning nishoniga aylangan. Bugungi kunda esa IoT qurilmalari sonining ortishi DDoS hujumlarini yanada kuchaytirib, ularni amalga oshirishni osonlashtirmoqda.

Mazkur mavzuning tanlanishiga asosiy sabab — DDoS hujumlarining soni va murakkabligining ortib borayotgani hamda ularning zamonaviy axborot tizimlariga yetkazayotgan zarari hisoblanadi. Hozirgi kunda nafaqat yirik tashkilotlar, balki kichik biznes va oddiy veb-resurslar ham bunday hujumlarga duch kelmoqda. Shu sababli, ushbu tahdidlarni chuqur o‘rganish va ulardan samarali himoyalanish usullarini ishlab chiqish muhim ilmiy-amaliy vazifa hisoblanadi.

Mavzuning dolzarbligi shundaki, DDoS hujumlari axborot tizimlarining ishlash barqarorligini izdan chiqarib, katta iqtisodiy zarar va obro‘ yo‘qotishlarga olib keladi. Ayniqsa, real vaqt rejimida xizmat ko‘rsatadigan tizimlar uchun bunday hujumlar jiddiy xavf tug‘diradi. Shu bois, DDoS hujumlarining mohiyatini, turlarini va ularni aniqlash hamda oldini olish usullarini o‘rganish zamonaviy kiberxavfsizlikning muhim yo‘nalishlaridan biri hisoblanadi.

Ushbu maqolada DDoS hujumlarining asosiy tushunchalari, ishlash prinsiplari, turlari hamda ulardan himoyalanishning zamonaviy usullari batafsil tahlil qilinadi.

ADABIYOTLAR TAHLILI VA USULLARI

DDoS hujumlari va ulardan himoyalanish masalalari tarmoq xavfsizligi, kiberxavfsizlik va taqsimlangan tizimlar sohasidagi ilmiy tadqiqotlarda keng o‘rganilgan. Ushbu yo‘nalishda olib borilgan izlanishlar asosan tarmoq trafigini tahlil qilish, hujumlarni aniqlash, ularni tasniflash va samarali himoya mexanizmlarini ishlab chiqishga qaratilgan. Ilk tadqiqotlarda xizmatdan voz kechish (DoS) hujumlari alohida tizimlarga qaratilgan bo‘lsa, keyinchalik internetning kengayishi bilan birga taqsimlangan (DDoS) hujumlar shakllanib, murakkab va keng ko‘lamli tahdid sifatida qarala boshlandi.

Ilmiy adabiyotlarda DDoS hujumlarining nazariy asoslari va ularning ishlash mexanizmlari batafsil yoritilgan. Xususan, 2000-yillarning boshlarida tarmoq xavfsizligi bo‘yicha olib borilgan tadqiqotlarda SYN flood, UDP flood va ICMP flood kabi asosiy hujum turlari tahlil qilingan. Ushbu hujumlar tarmoq resurslarini haddan tashqari yuklash orqali xizmat ko‘rsatishni izdan chiqarishga qaratilganligi bilan ajralib turadi. Keyingi tadqiqotlarda esa hujumlarning yanada murakkab turlari, jumladan, ilova darajasidagi (HTTP flood) hujumlar o‘rganilib, ularning aniqlanishi va oldini olish muammolari ko‘rib chiqilgan.

DDoS hujumlarini amalga oshirishda botnet texnologiyalarining roli ham ilmiy izlanishlarda keng tahlil qilingan. Botnet — bu zararli dasturlar bilan zararlangan va masofadan boshqariladigan qurilmalar tarmog‘i bo‘lib, ular yordamida katta hajmdagi hujum trafigi hosil qilinadi. Tadqiqotlarda botnetlarni aniqlash, ularni boshqaruv serverlaridan ajratish va faoliyatini cheklash usullari ishlab chiqilgan. Ayniqsa, so‘nggi yillarda IoT qurilmalari asosida tashkil etilgan botnetlar (masalan, Mirai) DDoS hujumlarining ko‘lamini sezilarli darajada oshirgani ilmiy manbalarda alohida ta’kidlangan.

Bundan tashqari, DDoS hujumlarini aniqlash va oldini olish bo‘yicha turli texnologiyalar ishlab chiqilgan. Ilmiy tadqiqotlarda IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari yordamida tarmoq trafigidagi anomal holatlarni aniqlash usullari keng o‘rganilgan. Shuningdek, trafikni filtrlash, paketlarni tekshirish (Deep Packet Inspection), yuklamani taqsimlash (load balancing) va CDN (Content Delivery Network) texnologiyalaridan foydalanish orqali hujumlarni kamaytirish usullari ham tahlil qilingan. Zamonaviy tadqiqotlarda esa sun’iy intellekt va mashinaviy o‘rganish algoritmlaridan foydalanib, DDoS hujumlarini real vaqt rejimida aniqlash va avtomatik tarzda javob berish imkoniyatlari o‘rganilmoqda.

Ilmiy adabiyotlarda bulutli texnologiyalar asosida DDoS himoya tizimlarini yaratish ham muhim yo‘nalishlardan biri sifatida qaraladi. Bunday yondashuvda katta hajmdagi zararli trafik bulutli platformalarda filtrlab olinadi va asosiy serverga faqat toza trafik uzatiladi. Bu esa tizimning barqaror ishlashini ta’minlashda samarali yechim sifatida baholanadi.

Mazkur tadqiqotda yuqorida keltirilgan ilmiy manbalarga tayangan holda bir qator usullar qo‘llanildi. Tahliliy usul yordamida DDoS hujumlarining nazariy asoslari, ularning turlari va ishlash mexanizmlari chuqur o‘rganildi. Solishtirma tahlil usuli orqali turli hujum turlari va ularga qarshi qo‘llaniladigan himoya vositalarining samaradorligi taqqoslandi. Tizimli yondashuv asosida DDoS hujumlari va himoya mexanizmlari yagona tizim sifatida ko‘rib chiqilib, ularning o‘zaro bog‘liqligi tahlil qilindi.

Bundan tashqari, umumlashtirish usuli yordamida mavjud ilmiy tadqiqotlar natijalari birlashtirilib, DDoS hujumlarining zamonaviy holati va rivojlanish tendensiyalari bo‘yicha xulosalar chiqarildi. Shu bilan birga, amaliy kuzatishlar asosida DDoS hujumlarining real tarmoqlardagi ta’siri va ulardan himoyalanishdagi muammolar baholandi.

Natijada, qo‘llanilgan usullar DDoS hujumlarini chuqur tushunish, ularning xavf darajasini baholash hamda samarali himoya choralarini ishlab chiqish imkonini berdi.

MUHOKAMA

DDoS hujumlari zamonaviy axborot tizimlari uchun eng xavfli tahdidlardan biri bo‘lib, ularning dolzarbligi yil sayin ortib bormoqda. Raqamli xizmatlarning kengayishi, onlayn platformalarga bo‘lgan qaramlikning oshishi hamda IoT qurilmalari sonining ko‘payishi DDoS hujumlarini amalga oshirishni osonlashtirdi. Natijada, hatto kichik resurslarga ega tizimlar ham yirik hujumlarga duch kelmoqda. Shu sababli DDoS hujumlarini o‘rganish va ularga qarshi samarali himoya choralarini ishlab chiqish kiberxavfsizlikning ustuvor yo‘nalishlaridan biri hisoblanadi.

DDoS hujumlarining asosiy maqsadi — tarmoq yoki server resurslarini ortiqcha yuklash orqali xizmat ko‘rsatishni izdan chiqarishdir. Bunday hujumlar natijasida xizmatlarning vaqtincha yoki to‘liq ishlamay qolishi, moliyaviy zararlar va foydalanuvchilar ishonchining pasayishi kuzatiladi. Ayniqsa, bank tizimlari, elektron tijorat platformalari va davlat xizmatlari uchun bu juda katta xavf tug‘diradi.

Mazkur muammoni hal etishda bir nechta samarali yondashuvlar taklif etiladi. Birinchidan, tarmoq trafigini real vaqt rejimida monitoring qilish va anomal faollikni aniqlash muhim hisoblanadi. Ikkinchidan, trafikni filtrlash va zararli so‘rovlarni bloklash orqali tizimga tushadigan yuk kamaytiriladi. Uchinchidan, yuklamani taqsimlash (load balancing) orqali server resurslari optimal boshqariladi. To‘rtinchidan, bulutli himoya xizmatlari (cloud-based protection) yordamida katta hajmdagi hujum trafigi tashqi darajada filtrlanadi. Bundan tashqari, IDS/IPS tizimlari yordamida hujumlarni erta bosqichda aniqlash va oldini olish imkoniyati yaratiladi.

Quyidagi jadvalda DDoS hujumlaridan himoyalanishning asosiy usullari, ularning afzalliklari va kamchiliklari taqqoslab ko‘rsatilgan:

1-jadval. DDoS hujumlaridan himoyalanish usullarining taqqoslanishi

Himoya usuli	Afzalliklari	Kamchiliklari
Trafikni filtrlash	Zararli trafikni tez aniqlaydi va bloklaydi	Murakkab hujumlarda samarasi pasayishi mumkin
IDS/IPS tizimlari	Hujumlarni erta aniqlash imkonini beradi	Soxta signal (false positive) ehtimoli mavjud
Yuklamani taqsimlash	Server yuklamasini teng taqsimlaydi	Katta hujumlarda yetarli bo‘lmasligi mumkin
CDN texnologiyalari	Trafikni global darajada tarqatadi	Qo‘shimcha xarajat talab qiladi
Bulutli himoya	Katta hajmdagi hujumlarni bartaraf etadi	Tashqi xizmatlarga bog‘liqlik mavjud

Jadvaldan ko‘rinib turibdiki, har bir himoya usulining o‘ziga xos afzallik va kamchiliklari mavjud. Shu sababli, yagona himoya vositasi bilan cheklanib qolish yetarli emas. Eng samarali yondashuv — bu bir nechta himoya mexanizmlarini birlashtirgan kompleks tizimni joriy etishdir.

Shuningdek, DDoS hujumlariga qarshi kurashishda zamonaviy texnologiyalar, xususan, sun’iy intellekt va mashinaviy o‘rganish usullaridan foydalanish muhim ahamiyat kasb etmoqda. Bu texnologiyalar tarmoqdagi odatiy va g‘ayritabiiy xatti-harakatlarni farqlash orqali hujumlarni tezkor aniqlash imkonini beradi.

Umuman olganda, DDoS hujumlari bilan bog‘liq muammolarni hal etish kompleks yondashuvni talab qiladi. Tarmoq infratuzilmasini to‘g‘ri loyihalash, zamonaviy himoya vositalarini joriy etish va doimiy monitoringni tashkil etish orqali ushbu tahdidlarning salbiy ta’sirini sezilarli darajada kamaytirish mumkin.

NATIJALAR

Mazkur tadqiqot natijalari DDoS hujumlari zamonaviy axborot tizimlariga sezilarli darajada salbiy ta’sir ko‘rsatishini yana bir bor tasdiqladi. Tahlillar davomida aniqlanishicha, DDoS hujumlari server resurslarini haddan tashqari yuklash orqali xizmatlarning uzluksiz ishlashiga jiddiy to‘sqinlik qiladi va foydalanuvchilarga xizmat ko‘rsatish sifatini keskin pasaytiradi.

Tadqiqot jarayonida taklif etilgan kompleks himoya yondashuvi — ya’ni trafikni monitoring qilish, zararli so‘rovlarni filtrlash, yuklamani taqsimlash hamda bulutli himoya xizmatlarini qo‘llash — DDoS hujumlarining samaradorligini sezilarli darajada kamaytirishga xizmat qilishi aniqlandi. Xususan, IDS/IPS tizimlari yordamida hujumlarni erta aniqlash va avtomatik tarzda bloklash imkoniyati mavjudligi tizim barqarorligini oshirdi.

Olingan natijalar shuni ko‘rsatdiki, yagona himoya usuli yetarli emas, balki bir nechta texnologiyalarni integratsiya qilish orqali ko‘p bosqichli himoya tizimini yaratish eng samarali yechim hisoblanadi. Ayniqsa, bulutli himoya va CDN

texnologiyalaridan foydalanish katta hajmdagi hujumlarni tashqi darajada bartaraf etish imkonini berib, asosiy server yuklamasini kamaytiradi.

Shuningdek, tadqiqot davomida sun’iy intellekt va mashinaviy o‘rganish usullaridan foydalanish DDoS hujumlarini aniqlash tezligini oshirishi va noto‘g‘ri signal (false positive) holatlarini kamaytirishi mumkinligi aniqlandi. Bu esa kelajakda yanada aqlli va avtomatlashtirilgan himoya tizimlarini yaratish imkonini beradi.

Umuman olganda, olingan natijalar DDoS hujumlariga qarshi kompleks va tizimli yondashuv eng samarali himoya usuli ekanligini ko‘rsatdi.

XULOSA

Tadqiqot natijalari asosida xulosa qilish mumkinki, DDoS hujumlari zamonaviy axborot tizimlari uchun eng jiddiy kiberxavflardan biri bo‘lib qolmoqda. Ularning murakkabligi va ko‘lami ortib borayotganligi sababli an’anaviy himoya usullari yetarli bo‘lmay qolmoqda. Shu bois, ushbu hujumlarga qarshi kurashishda zamonaviy, ko‘p bosqichli va kompleks himoya yondashuvlarini qo‘llash zarur.

Maqolada ko‘rib chiqilgan usullar — trafikni filtrlash, IDS/IPS tizimlari, yuklamani taqsimlash, CDN va bulutli himoya texnologiyalari — birgalikda qo‘llanilganda yuqori samaradorlikka ega ekanligi asoslandi. Ayniqsa, hujumlarni erta bosqichda aniqlash va avtomatik tarzda javob berish imkoniyati tizim xavfsizligini sezilarli darajada oshiradi.

Shu bilan birga, DDoS hujumlariga qarshi kurashishda faqat texnik vositalar bilan cheklanib qolmasdan, tarmoq infratuzilmasini to‘g‘ri loyihalash, xavfsizlik siyosatini ishlab chiqish va doimiy monitoringni yo‘lga qo‘yish ham muhim ahamiyat kasb etadi.

Kelajak istiqbollari nuqtai nazaridan qaraganda, sun’iy intellekt va avtomatlashtirilgan xavfsizlik tizimlari DDoS hujumlariga qarshi kurashishda asosiy vositalardan biriga aylanishi kutilmoqda. Bu esa tahdidlarni oldindan aniqlash va ularga tezkor javob berish imkoniyatlarini yanada kengaytiradi.

Umumiy xulosa sifatida aytish mumkinki, DDoS hujumlaridan samarali himoyalanish uchun kompleks, moslashuvchan va zamonaviy texnologiyalarga asoslangan yondashuv zarur bo‘lib, uning rivojlanishi kiberxavfsizlik sohasida muhim o‘rin tutadi.

FOYDALANILGAN ADABIYOTLAR:

1. *Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. Pearson, 2021.*
2. *Tanenbaum A.S., Wetherall D.J. Computer Networks. Pearson, 2011.*
3. *Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.*
4. *Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 2004.*

5. *Peng T., Leckie C., Ramamohanarao K. Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems. ACM Computing Surveys, 2007.*
6. *Houmansadr A., Brubaker C., Shmatikov V. The Parrot is Dead: Observing Unobservable Network Communications. IEEE Symposium on Security and Privacy, 2013.*
7. *RFC 4732. Internet Denial-of-Service Considerations. IETF, 2006.*
8. *RFC 4949. Internet Security Glossary. IETF, 2007.*
9. *Cisco Systems. DDoS Attack Mitigation Techniques and Best Practices. Cisco Security White Paper, 2020.*
10. *Cloudflare. Understanding and Mitigating DDoS Attacks. Cloudflare Security Documentation, 2023.*