Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

FORTIGATE VA PFSENSE/SURICATA ASOSIDAGI IKKI QATLAMLI GIBRID HIMOYA MODELIDA TARMOQ HUJUMLARIGA AVTOMA «CSE-CIC-IDS2018 VA BOT-IOT MA'LUMOTLAR TO'PLAMLARIDA DDOS HUJUMLARINI ANIQLASHDA RANDOM FOREST, SVM VA LSTM ALGORITMLARINING QIYOSIY TAHLILI

Komilov Abrorjon Maxamatsoli o'g'li
Vatan universiteti Raqamli texnologiyalar fakulteti,
Telekommunikatsiya injineringi mutaxasisligi magistranti
Kuvandikov J.T.
PhD., O'ZMU Jizzax filiali
"Kompyuter ilmlari va dasturlashtirish'
' kafedrasi mudiri
https://doi.org/10.5281/zenodo.24399113

Annotatsiya. Mazkur tezisda zamonaviy kompyuter tarmoqlarida keng tarqalgan DDoS (Distributed Denial of Service) hujumlarini aniqlash va ulardan himoyalanishning gibrid modeli ko'rib chiqiladi. Unda FortiGate tarmoq xavfsizligi qurilmasi hamda pfSense/Suricata ochiq kodli xavfsizlik vositalarini ikki qatlamli himoya tizimiga birlashtirish imkoniyatlari tahlil qilinadi. Shuningdek, CSE-CIC-IDS2018 va BoT-IoT ma'lumotlar to'plamlari asosida DDoS hujumlarini aniqlashda Random Forest, Support Vector Machine (SVM) va Long Short-Term Memory (LSTM) algoritmlarining qo'llanilishi, afzalliklari va cheklovlari yoritiladi. Mashinaviy o'qitish algoritmlarini tarmoq xavfsizligi infratuzilmasiga integratsiya qilish orqali hujumlarni aniqlash samaradorligini oshirish masalalariga alohida e'tibor qaratiladi.

Kalit so'zlar: kiberxavfsizlik, DDoS, FortiGate, pfSense, Suricata, gibrid himoya, Random Forest, SVM, LSTM, mashinaviy o'qitish, CSE-CIC-IDS2018, BoT-IoT, IDS, IPS.

KIRISH

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, internet xizmatlari va raqamli infratuzilmalarning kengayishi tarmoq xavfsizligini ta'minlash masalasini dolzarb vazifalardan biriga aylantirmoqda. Ayniqsa, DDoS hujumlari serverlar, veb-resurslar va korporativ tarmoqlarning ishlash qobiliyatini izdan chiqarishi, xizmatlardan foydalanish imkoniyatini cheklashi hamda katta iqtisodiy zarar keltirib chiqarishi mumkin. An'anaviy xavfsizlik vositalari ko'pincha oldindan belgilangan qoidalar va imzolar asosida ishlaydi. Biroq murakkab, tez o'zgaruvchan va yangi ko'rinishdagi hujumlarni aniqlashda bunday yondashuv har doim ham yetarli natija bermaydi. Shu sababli tarmoq trafigini tahlil qilishda sun'iy intellekt va mashinaviy o'qitish algoritmlaridan foydalanish muhim ahamiyat kasb etmoqda. Mazkur tadqiqotning asosiy maqsadi FortiGate hamda pfSense/Suricata vositalariga asoslangan ikki qatlamli gibrid himoya modelini taklif etish va CSE-CIC-IDS2018 hamda BoT-IoT ma'lumotlar to'plamlari yordamida DDoS hujumlarini aniqlashda Random Forest, SVM va LSTM algoritmlarining imkoniyatlarini qiyosiy tahlil qilishdan iborat.

ASOSIY QISM

DDoS hujumi bir vaqtning o'zida ko'plab manbalardan maqsadli server yoki tarmoq resursiga ortiqcha so'rovlar yuborish orqali uning xizmat ko'rsatish imkoniyatini cheklashga qaratilgan kiberhujum turidir. Bunday hujumlarda odatda botnetlar, zararlangan kompyuterlar, IoT qurilmalari yoki boshqa boshqariladigan tarmoq tugunlaridan foydalaniladi.

DDoS hujumlari ta'sir mexanizmiga ko'ra bir necha asosiy guruhlarga ajratiladi:

- **Volumetrik hujumlar** – tarmoq kanalini katta hajmdagi trafik bilan band qilishga qaratiladi. UDP Flood va ICMP Flood bunga misol bo'ladi.

➢ **Protokol darajasidagi hujumlar** – tarmoq protokollarining ishlash mexanizmlaridagi zaifliklardan foydalanadi. SYN Flood shunday hujumlardan biridir.

➢ **Ilova darajasidagi hujumlar** – HTTP so‘rovlari kabi amaliy darajadagi murojaatlarni ko‘paytirish orqali server resurslarini band qiladi.

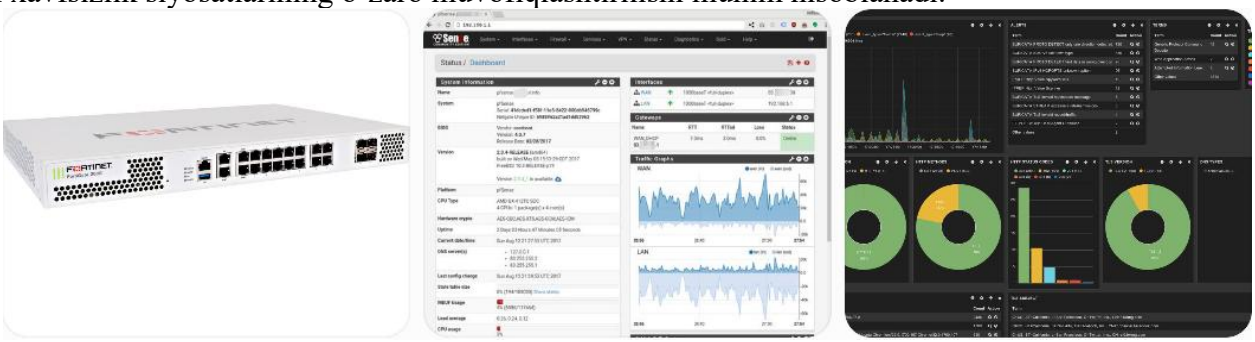
DDoS hujumlarini aniqlashda trafik hajmi, paketlar soni, manba va qabul qiluvchi IP-manzillar, protokollar, ulanishlar davomiyligi hamda so‘rovlar chastotasi kabi ko‘rsatkichlardan foydalaniladi. Biroq faqat bitta parametrga asoslangan aniqlash usuli yetarli bo‘lmasligi mumkin. Masalan, katta hajmdagi trafik har doim ham hujumni anglatmaydi, chunki qonuniy foydalanuvchilar faolligi ham trafikning keskin oshishiga sabab bo‘lishi mumkin. Shu bois bir nechta parametrni kompleks tahlil qilish talab etiladi.

FortiGate va pfSense/Suricata asosidagi ikki qatlamli gibrid himoya modeli. Tarmoq xavfsizligini kuchaytirishning samarali yo‘llaridan biri turli funksional imkoniyatlarga ega xavfsizlik vositalarini yagona infratuzilmaga birlashtirishdir. Bunda FortiGate va pfSense/Suricata vositalaridan foydalanish ikki qatlamli himoya modelini shakllantirish imkonini beradi.

Birinchi qatlamda FortiGate qurilmasi perimetr xavfsizligini ta’minlaydi. U tarmoqqa kiruvchi va undan chiquvchi trafikni nazorat qilish, xavfsizlik siyosatlarini qo‘llash, IP-manzillarni filtrlash, NAT, VPN, ilovalarni nazorat qilish va mavjud litsenziya hamda konfiguratsiyaga qarab qo‘shimcha tahdidlarni aniqlash funksiyalarini bajaradi. Ushbu qatlamda shubhali trafikning dastlabki filtrlash jarayoni amalga oshiriladi.

Ikkinchi qatlamda pfSense platformasi va uning tarkibiga integratsiya qilinadigan Suricata IDS/IPS tizimi ishlaydi. pfSense tarmoq oqimini boshqarish, marshrutlash va xavfsizlik qoidalarini tashkil etish imkonini bersa, Suricata paketlarni chuqur tahlil qilish, hujum imzolarini aniqlash va belgilangan qoidalar asosida zararli trafikni bloklash vazifalarini bajaradi.

Mazkur modelda har ikkala qatlamning vazifalari bir-birini to‘ldiradi. FortiGate umumiy perimetr himoyasini amalga oshiradi, pfSense/Suricata esa trafikni chuqurroq tahlil qilish va hujum belgilarini aniqlashga xizmat qiladi. Bunda ikki qurilmaning bir xil vazifalarni takroran bajarishi emas, balki xavfsizlik siyosatlarining o‘zaro muvofiqlashtirilishi muhim hisoblanadi.



1-rasm. FortiGate, pfSense va Suricata vositalari asosida tarmoq xavfsizligini ta’minlash texnologiyalari.

CSE-CIC-IDS2018 va BoT-IoT ma’lumotlar to‘plamlarining tahlili. Mashinaviy o‘qitish algoritmlarining samaradorligini baholashda real tarmoq muhitlariga yaqin bo‘lgan ma’lumotlar to‘plamlaridan foydalanish muhim hisoblanadi. Ushbu tadqiqotda CSE-CIC-IDS2018 va BoT-IoT ma’lumotlar to‘plamlari tanlanishi ularning turli tarmoq muhitlari va hujum ssenariylarini qamrab olishi bilan izohlanadi.

CSE-CIC-IDS2018 – Kanada kiberxavfsizlik instituti (CIC) va Communications Security Establishment hamkorligida ishlab chiqilgan tarmoq hujumlarini aniqlashga mo‘ljallangan ma’lumotlar to‘plamidir. Unda o‘n kun davomida shakllantirilgan tarmoq trafigi, normal faoliyat namunalari va turli kiberhujumlar aks ettirilgan. Ma’lumotlar to‘plamida 80 dan ortiq trafik xususiyatlari mavjud bo‘lib,

DDoS hujumlarining LOIC-HTTP, HOIC va LOIC-UDP kabi ko‘rinishlari ham qayd etilgan. Ushbu xususiyatlar trafikning statistik va xulq-atvor ko‘rsatkichlarini o‘rganish imkonini beradi.

BoT-IoT ma’lumotlar to‘plami esa buyumlar interneti (IoT) muhitidagi kiberhujumlarni tadqiq qilish uchun ishlab chiqilgan. Unda IoT qurilmalarining normal va zararli faoliyati, DoS va DDoS hujumlari, xizmatlarni skanerlash hamda boshqa zararli harakatlar namunalari mavjud. Ushbu to‘plamning muhim jihati shundaki, u ko‘plab IoT qurilmalari ishtirokidagi botnet faoliyatini va tarmoq trafigidagi anomal holatlarni tahlil qilishga imkon beradi.

Har ikkala ma’lumotlar to‘plamidan foydalanish algoritmlarning turli sharoitlardagi ishlash xususiyatlarini aniqlashga xizmat qiladi. CSE-CIC-IDS2018 korporativ tarmoq muhitidagi hujumlarni, BoT-IoT esa IoT infratuzilmasiga xos zararli trafikni o‘rganish imkoniyatini beradi. Bunda ma’lumotlar to‘plamlarining belgilari va formatlari turlicha bo‘lgani sababli ularni yagona modelga kiritishdan oldin moslashtirish talab etiladi.

Random Forest, SVM va LSTM algoritmlarining qiyosiy tahlili. DDoS hujumlarini aniqlashda mashinaviy o‘qitish algoritmlarining tanlanishi aniqlik, hisoblash tezligi, xotira sarfi, katta hajmdagi ma’lumotlarni qayta ishlash imkoniyati va yangi hujumlarni aniqlash qobiliyatiga bog‘liq. Ushbu jihatdan Random Forest, SVM va LSTM algoritmlari o‘ziga xos xususiyatlarga ega.

Random Forest algoritmi. Random Forest bir nechta qaror daraxtlaridan tashkil topgan ansambl algoritmi bo‘lib, yakuniy tasniflash natijasi daraxtlarning ovoz berish mexanizmi orqali aniqlanadi. Algoritm tarmoq trafigining turli xususiyatlarini birgalikda tahlil qilish, normal va zararli trafikni farqlash hamda murakkab bog‘liqliklarni aniqlash imkoniyatiga ega.

Ushbu algoritmning asosiy afzalliklari quyidagilardan iborat:

- ✓ katta hajmdagi strukturaviy ma’lumotlar bilan ishlash imkoniyati;
- ✓ murakkab va chiziqli bo‘lmagan bog‘liqliklarni aniqlash;
- ✓ xususiyatlarning ahamiyatlilik darajasini baholash;
- ✓ parametrlarni nisbatan sodda sozlash;
- ✓ tasniflash jarayonida barqaror natijalar olish imkoniyati.

Random Forest CSE-CIC-IDS2018 va BoT-IoT kabi ma’lumotlar to‘plamlarida DDoS trafikning statistik belgilarini aniqlash uchun qulay hisoblanadi. Biroq daraxtlar soni va chuqurligining ortishi model hajmi hamda hisoblash xarajatlarini oshirishi mumkin. Shuningdek, o‘qitish jarayonida ma’lumotlardagi nomutanosiblikni hisobga olish zarur.

Support Vector Machine (SVM) algoritmi. SVM ma’lumotlarni turli sinflarga ajratish uchun optimal ajratuvchi gipertekislikni aniqlashga asoslangan algoritmdir. U chiziqli va chiziqli bo‘lmagan tasniflash vazifalarida qo‘llaniladi. Kernel funksiyalari yordamida murakkab ma’lumotlar fazosida ham sinflar o‘rtasidagi chegaralarni aniqlash imkonini beradi. SVM algoritmining DDoS hujumlarini aniqlashdagi afzalligi trafik xususiyatlari o‘rtasidagi murakkab chegaralarni o‘rganish imkoniyatidir. Ayniqsa, normal trafik va hujum trafiklari o‘rtasidagi farqlar aniq ajratilgan hollarda yaxshi natija berishi mumkin. Shu bilan birga, SVM katta hajmdagi ma’lumotlar bilan ishlashda hisoblash jihatidan qimmatga tushishi, parametrlarni tanlashga sezgirligi va ma’lumotlarni oldindan normallashtirish zarurati bilan tavsiflanadi. Shu sababli CSE-CIC-IDS2018 ma’lumotlar to‘plamining katta hajmli namunalarini qayta ishlashda tanlab olish yoki xususiyatlar sonini kamaytirish kabi usullardan foydalanish maqsadga muvofiq.

Long Short-Term Memory (LSTM) algoritmi. LSTM takrorlanuvchi neyron tarmoqlarning rivojlantirilgan turi bo‘lib, ketma-ket ma’lumotlardagi uzoq muddatli bog‘liqliklarni o‘rganishga mo‘ljallangan. Uning asosiy xususiyati axborotni xotira bloklarida saqlash va kerakli vaqtda undan foydalanish imkoniyatidir. DDoS hujumlari ko‘pincha vaqt davomida trafik intensivligining o‘zgarishi, so‘rovlar chastotasining keskin oshishi va ko‘plab manbalardan bir xil xizmatga murojaat qilish kabi belgilar orqali namoyon bo‘ladi. LSTM aynan shu kabi vaqtga bog‘liq xususiyatlarni aniqlashda muhim imkoniyatlarga ega.

LSTM algoritmining afzalliklari:

- vaqt bo‘yicha ketma-ket trafik o‘zgarishlarini tahlil qilish;
- uzoq muddatli bog‘liqliklarni o‘rganish;
- murakkab va dinamik hujum ssenariylarini modellashtirish;
- turli trafik holatlari o‘rtasidagi yashirin munosabatlarni aniqlash.

Biroq LSTM modelini o‘qitish uchun ko‘proq hisoblash resurslari va vaqt talab etiladi. Bundan tashqari, ma’lumotlarni vaqt ketma-ketligiga mos ravishda shakllantirish, normallashtirish va o‘qitish parametrlarini to‘g‘ri tanlash zarur.

Algoritmlarning qiyosiy baholanishi va taklif etilayotgan metodologiya. Uchta algoritmning samaradorligini aniqlashda faqat umumiy aniqlik ko‘rsatkichiga tayanish yetarli emas. Chunki DDoS hujumlarini aniqlashda normal trafik va zararli trafik namunalari o‘rtasidagi nomutanosiblik noto‘g‘ri baholashga olib kelishi mumkin. Shu sababli quyidagi mezonlardan foydalanish tavsiya etiladi:

- **Accuracy** – model tomonidan to‘g‘ri tasniflangan barcha namunalar ulushi.
- **Precision** – hujum deb aniqlangan namunalar ichida haqiqatan hujumga tegishlilar ulushi.
- **Recall** – mavjud hujum namunalarining model tomonidan aniqlangan ulushi.
- **F1-score** – Precision va Recall ko‘rsatkichlarining garmonik o‘rtachasi.
- **False Positive Rate (FPR)** – normal trafikning noto‘g‘ri ravishda hujum sifatida aniqlanish darajasi.
- **Detection Time** – hujumni aniqlash uchun sarflangan vaqt.

Algoritmlarning asosiy xususiyatlarini quyidagicha umumlashtirish mumkin.

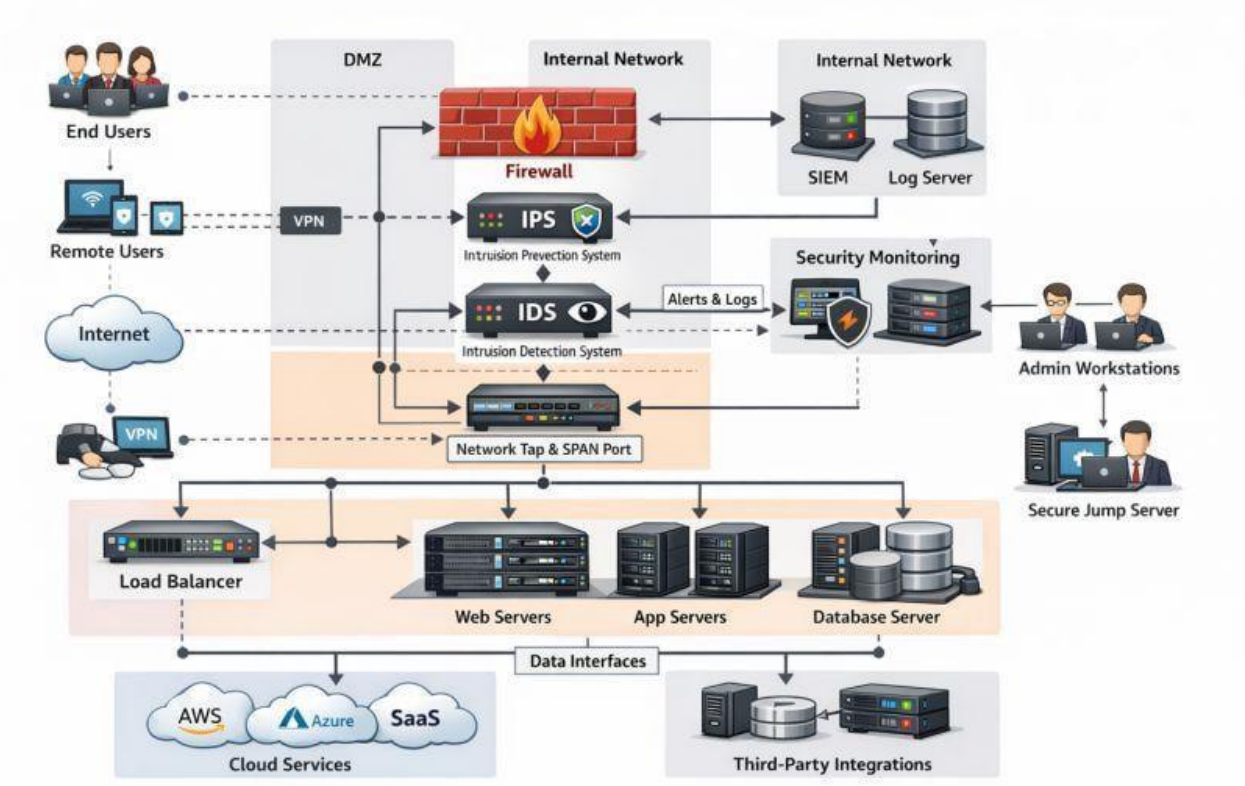
1-jadval. DDoS hujumlarini aniqlashda Random Forest, SVM va LSTM algoritmlarining qiyosiy tavsifi.

Baholash mezoni	Random Forest	SVM	LSTM
Tasniflash imkoniyati	Yuqori	Yuqori	Yuqori
Vaqt ketma-ketligini tahlil qilish	Cheklangan	Cheklangan	Yuqori
O‘qitish murakkabligi	O‘rtacha	O‘rtacha–yuqori	Yuqori
Katta ma’lumotlar bilan ishlash	Qulay	Resurs talab qiladi	Resurs talab qiladi
Normallashtirish zarurati	Odatda shart emas	Muhim	Muhim
Asosiy qo‘llanish sohasi	Statistik trafik tahlili	Sinflarni ajratish	Dinamik trafik tahlili

Tadqiqot doirasida quyidagi eksperimental metodologiyani qo‘llash taklif etiladi. Dastlab, CSE-CIC-IDS2018 va BoT-IoT ma’lumotlar to‘plamlari yuklab olinib, ulardagi takroriy yozuvlar, bo‘sh qiymatlar, cheksiz sonlar hamda noto‘g‘ri formatdagi ma’lumotlar tozalanadi. Bunda IP-manzillar va boshqa identifikatsiyalovchi belgilar modelning hujumlarni aniqlash qobiliyatiga sun’iy ta’sir ko‘rsatmaydigan tarzda qayta ishlanadi. Keyingi bosqichda ma’lumotlar xususiyatlari tanlanib, paketlar soni, baytlar miqdori, oqim davomiyligi, paketlar orasidagi vaqt, TCP bayroqlari va trafik chastotasi

kabi belgilar asosiy parametrlar sifatida belgilanadi. SVM va LSTM algoritmlari uchun ma’lumotlarni normallashtirish amalga oshiriladi, LSTM modeli uchun esa trafik vaqt bo‘yicha ketma-ket namunalar shaklida tashkil qilinadi. Shundan so‘ng har bir algoritm alohida o‘qitilib, ma’lumotlar o‘qitish, validatsiya va test qismlariga ajratiladi. Bunda vaqtga bog‘liq trafik yozuvlarini tasodifiy aralashtirish o‘rniga, ularni vaqt ketma-ketligi asosida ajratish maqsadga muvofiq hisoblanadi, chunki bu modelning kelajakdagi trafik ma’lumotlarini oldindan ko‘rib qolishi bilan bog‘liq xatolarning oldini oladi. Navbatdagi bosqichda algoritmlar natijalari belgilangan baholash mezonlari asosida tahlil qilinadi hamda CSE-CIC-IDS2018 ma’lumotlar to‘plamida o‘qitilgan modelning BoT-IoT ma’lumotlarida ishlash qobiliyati tekshiriladi. Bu orqali modelning turli tarmoq muhitlariga moslashuvchanligi va umumlashtirish imkoniyati baholanib, faqat bitta ma’lumotlar to‘plamiga moslashib qolishining oldi olinadi. Yakuniy bosqichda eng maqbul algoritm ikki qatlamli himoya infratuzilmasiga integratsiya qilinadi. Bunda Suricata tomonidan qayd etilgan trafik hodisalari va oqim statistikasi maxsus tahlil moduliga uzatiladi, mashinaviy o‘qitish modeli esa shubhali holatlarni baholab, belgilangan xavf darajasiga muvofiq tegishli qarorni shakllantiradi. Aniqlangan tahdidlar haqidagi ma’lumotlar FortiGate yoki pfSense xavfsizlik siyosatlariga mos ravishda uzatilishi mumkin. Mazkur avtomatlashtirish jarayonida tasdiqlangan qoidalar, hodisalar jurnallarini qayd etish, noto‘g‘ri bloklash holatlarini nazorat qilish va favqulodda tiklash mexanizmlarini ham nazarda tutish lozim. Ushbu yondashuvning muhim jihati shundaki, mashinaviy o‘qitish algoritmlari mavjud IDS/IPS vositalarining o‘rnini to‘liq egallamaydi, balki ularning tahdidlarni aniqlash imkoniyatlarini kengaytiradi. Natijada imzo asosidagi aniqlash va tarmoq xatti-harakatlarini tahlil qilish mexanizmlari birgalikda faoliyat yuritadigan gibrid axborot xavfsizligi tizimi shakllanadi.

Taklif etilayotgan gibrid modelning amaliy samaradorligi. Taklif etilayotgan modelda tarmoq xavfsizligini ta’minlash jarayoni uchta o‘zaro bog‘liq mexanizm asosida tashkil etiladi: perimetr himoyasi, chuqur trafik tahlili va intellektual aniqlash.



2-rasm. FortiGate va pfSense/Suricata vositalari hamda mashinaviy o‘qitish algoritmlari asosida DDoS hujumlarini aniqlashning ikki qatlamli gibrid himoya arxitekturasi.

Modelning ishlash ketma-ketligi quyidagicha tashkil etiladi:

- Tarmoqdan kelayotgan trafik dastlab FortiGate orqali tekshiriladi va belgilangan xavfsizlik siyosatlari asosida filtrlab boriladi.
- Keyingi qatlamda pfSense va Suricata yordamida tarmoq paketlari hamda ulanishlar chuqur tahlil qilinadi.
- Trafikdan ajratib olingan statistik va xulq-atvor xususiyatlari mashinaviy o‘qitish moduliga uzatiladi.
- Random Forest, SVM yoki LSTM algoritmi trafikni normal yoki zararli deb tasniflaydi.
- Aniqlangan xavf darajasiga qarab avtomatik ogohlantirish, trafikni cheklash yoki bloklash bo‘yicha qaror shakllantiriladi.

Bunda avtomatik bloklash mexanizmini to‘g‘ridan-to‘g‘ri algoritmning o‘ziga topshirish emas, balki uning qarorini xavfsizlik siyosati bilan muvofiqlashtirish maqsadga muvofiq. Masalan, yuqori xavfli trafik avtomatik bloklanishi, o‘rta xavfli trafik esa qo‘shimcha tekshiruvga yuborilishi mumkin. Qiyosiy tahlil asosida Random Forest algoritmi statistik xususiyatlar asosida tezkor tasniflash uchun, SVM chegaraviy ajratish vazifalari uchun, LSTM esa vaqt davomida o‘zgaruvchi trafik xususiyatlarini o‘rganish uchun istiqbolli yechim sifatida qaraladi. Shuning uchun amaliy infratuzilmada ushbu algoritmlardan birini tanlash tarmoqning yuklanishi, hisoblash resurslari va aniqlash talablariga bog‘liq bo‘ladi.

XULOSA

O‘tkazilgan nazariy va metodologik tahlil natijasida DDoS hujumlariga qarshi kurashishda FortiGate va pfSense/Suricata vositalariga asoslangan ikki qatlamli gibrid himoya modelidan foydalanish maqsadga muvofiqligi asoslandi. Random Forest, SVM va LSTM algoritmlari turli xususiyatlari bilan ajralib turishi aniqlandi: Random Forest statistik trafikni tasniflashda, SVM sinflar o‘rtasidagi chegaralarni aniqlashda, LSTM esa vaqtga bog‘liq trafik o‘zgarishlarini tahlil qilishda muhim imkoniyatlarga ega. CSE-CIC-IDS2018 va BoT-IoT ma’lumotlar to‘plamlaridan foydalanish taklif etilayotgan yondashuvni turli tarmoq muhitlarida baholash imkonini beradi. Mazkur modelni amaliy sinovdan o‘tkazish, aniqlik, Recall, F1-score va aniqlash vaqtini o‘lchash hamda avtomatik bloklash mexanizmini takomillashtirish tarmoq xavfsizligini oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. G‘aniyev S.K., Irgasheva D.Y., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. Darslik. – 2022. Elektron manba.
2. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – Toshkent, 2022.
3. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-sonli «Raqamli O‘zbekiston – 2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risidagi Farmoni. – Toshkent, 2020.
4. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – B. 108–116.
5. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset // Future Generation Computer Systems. – 2019. – Vol. 100. – B. 779–796.
6. Songma S., Sathuphan T., Pamutha T. Optimizing Intrusion Detection Systems in Three Phases on the CSE-CIC-IDS-2018 Dataset // Computers. – 2023. – Vol. 12, № 12. – 245.