Impact Factor: 9.9
ISSN-L: 2544-980X

IDS ORQALI TARMOQDA BO‘LADIGAN HUJUMLARNI AQINLASH USULLARI VA TAHLILI

X.X.Sadirova
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg’ona filiali, “Axborot xavfsizligi” kafedrasi assistenti Farg’ona, O’zbekiston
+998914372060
sadirovaxursanoy@gmail.com

Annotatsiya: Ushbu maqolada hozirgi davrda kiberxavfsizlik texnologiyalarining ahamiyati oshib bormoqda, chunki korxonalar va tashkilotlar o’z ma’lumotlarini himoya qilish uchun yangi texnologiyalarga muhtoj. Kiber hujumlarni erta bosqichda aniqlash va ularning oldini olish muhim vazifalardan biridir. IDS (Intrusion Detection System - tizimga tajovuzni aniqlash tizimi) bunday hujumlarni real vaqt rejimida aniqlash va zarur choralarni ko‘rishga imkon beradi. Mazkur maqolada IDS texnologiyalarining asosiy turlari, ularning ishlash prinsiplari va samaradorlik omillari ko‘rib chiqiladi..

Kalit so’zlari: Sun’iy intellekt, ma’lumotlar xavfsizligi, hujumlar, IDS, tarmoq protokollari, tahdidlarni aniqlsh, anomaliyalar

Kirish

Bugungi kunda siyosiy va tijorat tuzilmalari tobora ko‘proq murakkablashmoqda kompyuter tarmoqlaridagi axborot mazmuniga zarar etkazish, buzish yoki senzura qilish uchun kiberurush [6]. Tarmoq protokollarini loyihalashda ishonchlilikni ta’minlash zarurati mavjud hattoki partiyalarning bir qismini nazorat qila oladigan kuchli hujumchilarning kirib kelishi tarmoqda kuzatlinishi munkin.

Boshqariladigan tomonlar ikkala passivni ham ishga tushirishlari mumkin (masalan, tinglash, ishtirok etmaslik) va faol hujumlar (masalan, tiqilib qolish, axborotlarni o‘chirib yuborish hamda axborotni soxtalashtirish) kabi ishlarni amalga oshirishi munkin. Hujumni aniqlashda sodir bo‘layotgan hodisalarni dinamik ravishda kuzatib turish jarayoni kompyuter tizimi yoki tarmog‘i, ularni mumkin bo‘lgan hodisalar belgilari uchun tahlil qilish hamda tez-tez ruxsatsiz kirishni taqiqlashdir [4]. Bu odatda, turli tizimlar va tarmoq manbalaridan ma’lumotlarni avtomatik ravishda yig’ish keyin amalga oshiriladi, mumkin bo‘lgan xavfsizlik muammolari uchun ma’lumotlarni tahlil qiladi [1].

An’anaviy hujumlarni aniqlash va oldini olish usullari, masalan, xavfsizlik devorlari, kirishni boshqarish mexanizmlari va shifrlashlar to‘liq himoya qilishda bir qator cheklovlarga ega tarmoqlar va tizimlar xizmat ko‘rsatishni rad etish kabi tobora murakkab hujumlardan. Bundan tashqari, bunday usullarga asoslangan tizimlarning aksariyati noto‘g‘ri pozitivlardan aziyat chekadi va noto‘g‘ri salbiy aniqlash darajalari va o‘zgarishlarga doimiy moslashishning yo‘qligi zararli xatti-harakatlardir [2].

Biroq so‘nggi to‘qqiz, o’n yil ichida bir nechta Machine Learning degan umidda hujmlarni aniqlash muammosiga texnikalar qo‘llanilgan aniqlash darajalari va moslashuvchanlikni yaxshilash hamda hujumlarni oldini olishda foydali hisoblanadi. Ushbu texnikalar ko‘pincha saqlash uchun ishlatiladi, hujumga oid bilim bazalari eng yangi va keng qamrovli. Machine Learning usullaridan foydalanadigan bir nechta maqolalarni o’rganib chiqilib, taqsimlangan kompyuter tizimlarida zararli xatti-harakatlarni aniqlash. An’anaviy sun’iy intellektga asoslangan hujumlarni aniqlashning bir necha usullarini ko‘rib chiqiladi. Hisoblash intellektining turli asosiy usullarini aniqlaymiz va adabiyotda taklif qilingan bir nechta sun’iy intellektga asoslangan algoritmlarni tavsiflaymiz. IDS tizimiga birinchi navbatda IDS nima ekanligiga to‘xatilib o‘tamiz. IDS bu suqilib kirishni oldini

Impact Factor: 9.9 ISSN-L: 2544-980X

oladigan tizim, odatda katta tarmoq trafigining hajmi, ma’lumotlarning notekis taqsimlanishi, normal va g‘ayritabiiy xatti-harakatlar o‘rtasidagi qaror chegaralarini amalga oshirishning qiyinligi va doimiy o‘zgaruvchan muhitga doimiy moslashish talabi kabi muammolarni hal qilishda yordam beradi[14].

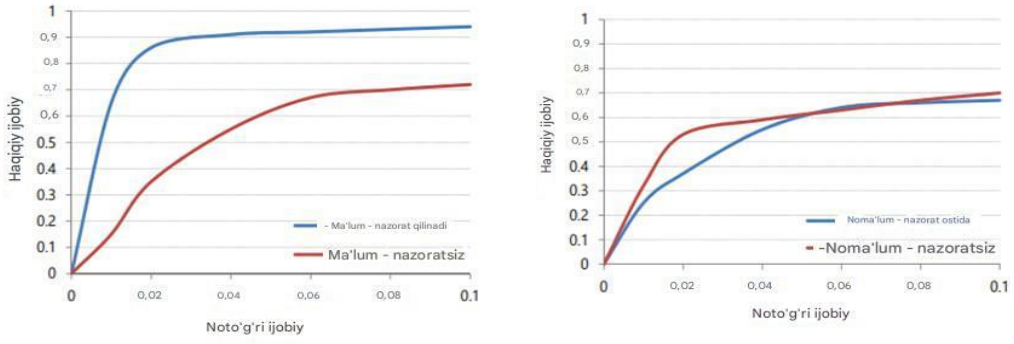
Umuman olganda, muammo samarali suratga olishdir va kompyuter tarmog‘idagi turli xatti-harakatlarni tasniflash. Tarmoq xatti-harakatlarini tasniflash strategiyalari odatda ikkita toifaga bo’linadi:

- ✓ foydalanuvchilar soni aniqlash;
- ✓ anomaliyalarni aniqlash [4].

Adabiyotlar sharhi va metodologiya (Literature Review and Methodology)

Noto‘g‘ri foydalanishni aniqlash usullari imzoni moslashtirish algoritmlari yordamida ma’lum noto‘g‘ri foydalanish holatlari uchun tarmoq va tizim faoliyatini tekshiradi. Ushbu usul allaqachon ma’lum bo’lgan hujumlarni aniqlashda samarali. Biroq, yangi hujumlar ko’pincha o’tkazib yuboriladi va bu noto’g’ri negativlarni keltirib chiqaradi. Ogohlantirishlar IDS tomonidan yaratilishi mumkin, ammo bunga reaktsiya har bir ogohlantirish tizimning beqarorligiga olib keladigan vaqt va resurslarni behuda sarflaydi. Ushbu muammoni bartaraf etish uchun IDS birinchi alomat aniqlangandan so’ng darhol yo’q qilish jarayonini boshlamasligi kerak, aksincha ogohlantirishlarni to’plash va ularning o’zaro bog’liqligi asosida qaror qabul qilish uchun etarlicha sabrli bo’lishi kerak. Biz buzg’unchilikni aniqlashga asoslangan ML-ga asoslangan yondashuvlarni ikki toifaga ajratamiz: Sun'iy intellekt (AI) texnikasiga asoslangan yondashuvlar va Hisoblash intellekt (CI) usullariga asoslangan yondashuvlar. AI texnikasi statistik modellashtirish kabi klassik AI sohasidagi usullarga tegishli bo’lsa, CI texnikasi esa klassik usullar hal qila olmaydigan murakkab muammolarni hal qilish uchun ishlatiladigan tabiatdan ilhomlangan usullarga ishora qiladi.

Muhim CI metodologiyalari evolyutsion hisoblash, loyqa mantiq, sun'iy neyron tarmoqlar va sun'iy immunitet tizimlaridir. CI AIning taniqli sohasidan farq qiladi. AI ramziy ma'lumotni taqdim etish bilan shug’ullanadi, CI esa ma'lumotlarning raqamli ko’rinishini boshqaradi. Garchi bu ikki toifa o’rtasidagi chegara har doim ham aniq bo’lmasa-da va adabiyotda ko’plab gibrid usullar taklif qilingan bo’lsa-da, avvalgi ishlarning aksariyati asosan toifalarning har biriga asoslangan holda ishlab chiqilgan. Bundan tashqari, klassik usullardan farqli o’laroq, tabiatga asoslangan usullar qanchalik yaxshi ishlashini tushunish juda foydali bo’lar edi. Laskov va boshqalar. [7] zararli faoliyatni aniqlash uchun nazorat ostidagi (tasniflash) va nazoratsiz o‘rganish (klasterlash) usullarini qiyosiy tahlil qilish uchun eksperimental asosni ishlab chiqish. Ushbu ishda baholangan nazorat qilinadigan usullar qarorni o’z ichiga oladi. Daraxtlar, k-Yaqin qo’shni (kNN), Ko’p qatlamli perseptron (MLP) va vektorli mashinalarni qo’llab-quvvatlash (SVM).



Rasm.1. Baholangan usullarni aniqlash tezligining o‘rtachasi

Test ma’lumotlari faqat ma’lum hujumlarni o‘z ichiga oladi (chapda) va test ma’lumotlari noma’lum hujumlarni o‘z ichiga oladi (o‘ngda). chunki bugungi murakkab dushmanlar qochish uchun bir nechta bosqin usullaridan foydalanadilar ya’ni zamonaviy IDS dan [8]. Natijalari shuni ko’rsatadiki, nazorat ostidagi algoritmlar umuman ma’lum hujumlar bilan ma’lumotlarga nisbatan yaxshiroq tasniflash aniqligini ko‘rsatadi (birinchi diogrammada). Ushbu algoritmlar orasida qarorlar

Impact Factor: 9.9 ISSN-L: 2544-980X

daraxti algoritmi eng yaxshi natijalarga erishdi (95% haqiqiy ijobiy ko'rsatkich, 1% noto'g'ri ijobiy ko'rsatkich). Keyingi ikkita eng yaxshi algoritm MLP va SVM, keyin esa keng yaqin yonma yon algoritmi. Biroq, agar test ma'lumotlarida ko'rinmaydigan hujumlar mavjud bo'lsa, u holda nazorat qilinadigan usullarni aniqlash tezligi sezilarli darajada kamayadi. Bu erda nazoratsiz texnikalar yaxshiroq ishlaydi, chunki ular ko'rinadigan va ko'rinmaydigan hujumlar uchun aniqlikda sezilarli farq ko'rsatmaydi. 1-rasmda baholangan barcha usullarning o'rtacha haqiqiy hamda noto'g'ri ijobiy stavkalari ko'rsatilgan. Rasmdan ko'rinib turibdiki, nazorat qilinadigan usullar odatda yaxshiroq ishlaydi, ammo nazoratsiz usullar ikkala senariyda ham kuchliroq natijalar beradi.

Natijalar va tahlillar (Results and analysis)

Nazoratsiz o'rganishga asoslangan TCP/IP tarmoqlarida IDS uchun ikki bosqichli anomaliyaga asoslangan arxitekturani joriy qiladi: birinchi daraja nazoratsiz klasterlash algoritmi bo'lib, u tarmoq paketlarining foydali yukidan kichik o'lchamli naqshlarni yaratadi [17].

Boshqacha qilib aytganda, TCP yoki UDP paketi normal va anormal trafikni ifodalovchi ikkita klasterga tayinlangan. Ikkinchi daraja optimallashtirilgan an'anaviy anomaliyalarni aniqlash algoritmi bo'lib, paketning foydali yuki tarkibidagi ma'lumotlarning mavjudligi bilan takomillashtiriladi. Ishning motivi shundaki, nazoratsiz o'rganish usullari odatda nazorat qilinadigan usullarga qaraganda hujum shakllarini umumlashtirishda kuchliroqdir, shuning uchun bunday arxitektura polimorf hujumlarga samaraliroq qarshilik ko'rsatishiga yordam beradi.

Ma'lumotlarni yig'ish usullaridan foydalangan holda tarmoqlardagi anomaliyalarni aniqlash uchun klassifikatorni quradi. Ular dastur yoki foydalanuvchining normal xatti-harakatlarini tavsiflashda muhim bo'lgan ikkita umumiy ma'lumot olish algoritmlarini amalga oshiradilar. Ular tajovuzlarni aniqlash tizimlari uchun agentga asoslangan arxitekturani taklif qiladilar, bu yerda agentlar doimiy ravishda o'rganishib boradi [9]. Hisoblash va agentlarga yangilangan aniqlash modellarini taqdim etish. Ular anomaliyalarni aniqlashda tasniflash modellarining samaradorligini ko'rsatish uchun Sendmail[1] tizimi qo'ng'iroqlari ma'lumotlari va tarmoq tcpdump ma'lumotlari bo'yicha tajribalar o'tkazadilar. Nihoyat, ular buzg'unchilikda ma'lumotlarni qidirish yondashuvlaridan foydalanishning eng muhim muammosi ekanligini ta'kidlaydilar.

Aniqlash shundan iboratki, ular profil qoidalari to'plamini hisoblash uchun katta miqdordagi audit ma'lumotlarini talab qiladi [13]. ML-ga asoslangan hujumlarni aniqlash bo'yicha olib borilgan keng ko'lamli tadqiqotlar va bunday tizimlarning operatsion joylashuvi yo'qligi o'rtasidagi nomutanosiblikni o'rganadilar. Ular tarmoqqa tajovuzni aniqlash bilan bog'liq muammolarni aniqlaydi va ML asosidagi hujumni aniqlash bo'yicha kelajakdagi tadqiqotlarni kuchaytirish uchun ko'rsatmalar to'plamini taqdim etadi. Aniqroq qilib aytganda, ular anomaliyaga asoslangan IDS chetni aniqlashni talab qiladi, ML ning klassik qo'llanilishi esa faoliyat o'rtasidagi o'xshashlikni topish bilan shug'ullanadigan tasniflash muammosidir [10].

To'g'ri, ba'zi hollarda chetni aniqlash muammosini tasniflash muammosi sifatida modellashtirish mumkin, unda ikkitasi sinf mavjud ular normal va g'ayritabiiy. Mashinani o'rganishda barcha sinflarning o'quv maqshlari bilan tizimni o'rgatish kerak, anomaliyalarni aniqlashda esa faqat oddiy ishlar bo'yicha mashq qilish mumkin. Bu shuni anglatadiki, anomaliyalarni aniqlash ilgari noma'lum bo'lgan zararli faoliyatdan ko'ra, ma'lum bo'lgan hujumlarning o'zgarishlarini topish uchun yaxshiroqdir. Shuning uchun ML usullari hujumni aniqlashdan ko'ra spamni aniqlashda samaraliroq qo'llanilgan.

CI-ga asoslangan texnikalar. Ushbu bo'limda biz hisoblash intellektining to'rtta asosiy texnikasiga asoslangan bir nechta algoritmlarni ko'rib chiqamiz: genetik algoritmlar, sun'iy neyron tarmoqlari, mantiq va sun'iy immunitet tizimlari. Genetik algoritmlar masalalarning optimal yechimlarini topishga qaratilgan. Muammoning har bir potentsial yechimi genom yoki xromosoma deb ataladigan bitlar (genlar) ketma-ketligi sifatida ifodalanadi. Genetik algoritm genomlar to'plamidan (aholi) va har bir genomning sifatini (yaxshiligini) o'lchaydigan funktsiyasi deb ataladigan baholash funktsiyasidan boshlanadi. Algoritm krossover va deb nomlangan ikkita takrorlash operatoridan foydalanadi. yangi avlodlarni (yechimlarni) yaratish uchun mutatsiya, keyinchalik ular baholanadi. Krossover populyatsiyadagi ota-onalarning turli xususiyatlari avlodlarga qanday meros bo'lib qolganligini aniqlaydi. Mutatsiya - bu bitta genning o'z-o'zidan o'zgarishi [12].

Impact Factor: 9.9 ISSN-L: 2544-980X

Anomal tarmoq faolligini oddiy tarmoq trafigidan farqlashda tahlilchi ishini qo‘llab-quvvatlaydigan tajovuzni aniqlash ekspert tizimi qoidalarini yaratish uchun genetik algoritmlar va qarorlar daraxtlaridan foydalaning. Ushbu ishda GA tarmoq trafigi uchun oddiy qoidalarni ishlab chiqish uchun ishlatiladi. Har bir qoida genom bilan ifodalanadi va genomlarning boshlang’ich populyatsiyasi tasodifiy qoidalar to’plamidir. Har bir genom 29 gendan iborat: IP manbasi uchun 8, maqsad IP uchun 8, manba porti uchun 6, maqsad porti uchun 6 va protokol uchun.

Funktsiyada oldindan tasniflangan ma’lumotlar to‘plamidagi har bir qoidaning haqiqiy ishlashiga asoslanadi. Tahlilchi ulanishlardan tashkil topgan ma’lumotlar to‘plamini normal yoki g‘ayritabiiy deb belgilaydi. Tizim qoidalarni ishlab chiqish va tahlilchilar qarorlarini qo‘llab-quvvatlash uchun tahlilchilar tomonidan yaratilgan o‘quv majmualaridan foydalanadi. Agar qoida g’ayritabiiy ulanishga to‘liq mos kelsa, u bonus bilan taqdirlanadi va agar u oddiy ulanishga to‘g‘ri kelsa, u jarimaga tortiladi. Shunday qilib, avlodlar faqat intruziv aloqalarga mos keladigan qoidalarga moyil. Genetik algoritm ma'lum bir avlod avlodiga yetgandan so’ng, u to’xtaydi va eng yaxshi genomlar (ya'ni, qoidalar) tanlanadi. Yaratilgan qoidalar to’plami bilim sifatida ishlatilishi mumkin**,** tarmoq ulanishi va tegishli xatti-harakatlar potentsial bosqinlar ekanligini aniqlash uchun IDS ichida. An’anaviy GA global maksimal deb ataladigan yagona eng yaxshi yechimga yaqinlashishga intiladi. Chunki [7] algoritmi eng yaxshi noyob qoidalar guruhini talab qiladi, bu mahalliy maksimallarga yaqinlashadigan kichik populyatsiyalarni yaratishga harakat qiladigan niching deb ataladigan tabiatdan ilhomlangan usul. Ular mahalliy tarmoq uchun intruziv xatti-harakatlarni aniqlash uchun oddiy va g’ayritabiiy xatti-harakatlarni aniqlash uchun tarmoq ulanishlaridan foydalanish kerakligini ta'kidlaydilar. Hujum ba’zan mavjudlarni skanerlash kabi oddiy bo‘lishi mumkin. Serverdagi portlar yoki parolni taxmin qilish sxemasi. Lekin, odatda, ular murakkab va avtomatlashtirilgan vositalar tomonidan ishlab chiqariladi. Shunday qilib, samarali genetik algoritm yordamida murakkab anomal harakatlarni tasniflashi mumkin bo’lgan IDS qoidalarini aniqlash uchun tarmoq ulanishlarining vaqtinchalik va fazoviy ma'lumotlaridan foydalanish kerak.

Sun’iy neyron tarmoqlari (ANN) Neyron tarmoq ma’lum bir topologiyaga ko‘ra bir-biri bilan yuqori darajada bog‘langan neyronlar deb ataladigan ishlov berish birliklari to’plamidan iborat. ANN misol orqali o’rganish va cheklangan, shovqinli va to‘liq bo’lmagan ma'lumotlardan umumlashtirish qobiliyatiga ega. Ular ma'lumotlarni ko’p talab qiladigan ilovalarning keng spektrida muvaffaqiyatli qo‘llanilgan [6]. Neyron tarmoqlari va yordam vektor mashinalari (SVM) yordamida hujumni aniqlash yondashuvlarini tavsiflaydi. Ularning maqsadi anomaliyalarni tanib olish uchun tasniflagichlarni yaratish uchun foydalanuvchi xatti-harakatlarini tavsiflovchi naqshlar yoki xususiyatlarni aniqlashdir. SVM 6 - bu yuqori o‘lchamli xususiyat maydonida o’quv vektorini ifodalovchi va har bir vektorni o’z sinfi bo’yicha belgilovchi nazorat qilinadigan o’quv mashinalari. SVM noma'lum vektorlarni tasniflashda xato miqdori bo’lgan umumlashtirish xatosini minimallashtirish uchun turli sinflar orasidagi chegara (ajralish) ning yuqori chegarasini belgilaydi. SVM xususiyat makonida giperplanga yaqinlashadigan qo’llab-quvvatlash vektorlari deb ataladigan o’quv ma'lumotlari to’plamini aniqlash orqali ma'lumotlarni tasniflaydi.

Xulosa (Conclusion)

Ushbu ishda “IDS orqali tarmoqda bo‘ladigan hujumlarni aniqlash usullari va tahlili” mavzusi yoritilib, zamonaviy axborot texnologiyalari muhitida tarmoq xavfsizligini ta’minlash masalalari ko‘rib chiqildi. IDS (Intrusion Detection System) tizimlari tarmoqdagi kiberhujumlarni erta aniqlash va ularga qarshi kurashishda muhim vosita hisoblanadi. Shuningdek, tarmoqda aniqlangan hujumlarni tahlil qilishning ahamiyati, ularni oldini olish va kelgusidagi xavfsizlik strategiyasini ishlab chiqish uchun zarur ekani ko‘rsatildi. IDS tizimlaridan foydalanishni avtomatlashtirish va sun’iy intellekt algoritmlarini qo‘llash yo‘nalishlari bo‘yicha tavsiyalar berildi. Tadqiqot natijalari IDS tizimlarini takomillashtirish va ulardan samarali foydalanish orqali tarmoq xavfsizligini oshirishga yordam beradi. Shu bilan birga, IDS tizimlarini boshqa xavfsizlik choralari bilan integratsiyalash orqali ko‘p qavatli xavfsizlik tizimini yaratish imkoniyati ta’kidlandi.

Foydalanilgan adabiyotlar.

Impact Factor: 9.9 ISSN-L: 2544-980X

1. Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta'minlashning zamonaviy usullari. *Engineering problems and innovations*.
2. Sadirova, X., & Ergasheva, A. (2023). AXBOROTNING MAXFIYLIGINI, YAXLITLIGINI VA FOYDALANUVCHANLIGINI BUZISH USULLARI. *Engineering problems and innovations*.
3. Sadirova, X. (2023). Axborot texnologiyalarida yangi o'qitish usullari tahlili. *Engineering problems and innovations*.
4. Sadirova, X., & Ganiyeva, S. (2023, October). Cloud-Based Security Solutions: Protecting Networks in the Era of Digital Transformation. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.
5. Mamadaliyeva, L., Xusanova, M., & Sadirova, X. (2023, October). Endpoint Protection in the Modern Network Landscape: Securing Devices Beyond the Perimeter. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.
6. Turdimatov, M., Xusanova, M., Sadirova, X., Abdurakhmonov, S., & Bilolov, I. (2024, November). On the method of approximation and quantization of information transmission through communication channels. In *E3S Web of Conferences* (Vol. 508, p. 03007). EDP Sciences.
7. Sadirova, X., & Ergasheva, A. (2023). TA'LIMDA INNOVATSION O 'QITISH TEXNOLOGIYALARI. *Engineering problems and innovations*.
8. Sadirova, X., Qadamova, Z., & Tojidinov, A. (2023). Qisman tarmoqli shovqin siqilish muhitida shifrlangan tarqalish kodlari bilan chastota sakrashining tarqalishi spektrining xavfsizligi. *Journal of technical research and development*, *1*(2), 69-74.
9. Садирова, Х., Хусанова, М., & Акбаров, Н. (2023, October). INTRUSION DETECTION AND PREVENTION SYSTEMS FOR NETWORK SECURITY. In *Conference on Digital Innovation:" Modern Problems and Solutions"*