NEYRON TARMOQLAR ASOSIDA TAHDIDLARNI ANIQLASH USULI VA ALGORITMI TAHLILI

Mualliflar: Bekmirzayev Obidjon Nuraliyevich [1], Karimov Abdukarimjon Alisher o‘g‘li [2]
Affiliyatsiya: Xalqaro Nordik universiteti, Sanoatni boshqarish va raqamli texnologiyalar kafedrasi PhD., dotsenti [1], Xalqaro Nordik universiteti talabasi [2]
DOI: https://doi.org/10.5281/zenodo.17588577

ANNOTATSIYA

Mazkur tadqiqotda neyron tarmoqlar asosida tahdidlarni aniqlash usuli va algoritmi tahlil qilindi. Tadqiqotda SVM (tayanch vektor mashinasi) va entropiya usullari birlashtirilgan holda tarmoq hujumlarini aniqlash samaradorligi oshirildi. Metodologiya sifatida ma’lumotlar intellektual tahlili, entropiyani normallashtirish va SVM orqali sinflashtirish bosqichlari qo‘llanildi. Natijalar mujassamlangan algoritmda 97,25% aniqlik bilan tahdidlarni to‘g‘ri saralash imkonini berdi. Taklif etilgan yechim axborot xavfsizligi tizimlarida hujumlarni erta aniqlash va ularni samarali tahlil qilish imkonini yaratadi.

Kalit so‘zlar: neyron tarmoqlar, SVM, entropiya, tarmoq hujumlari, axborot xavfsizligi, tahdidlarni aniqlash algoritmi.

KIRISH

Hozirgi kunda global tarmoqlarda axborot xavfsizligini ta’minlash dolzarb masalalardan biri hisoblanadi. Tarmoq orqali uzatilayotgan ma’lumotlar hajmining ortishi, foydalanuvchilar sonining ko‘payishi va tarmoq xizmatlarining murakkablashuvi turli xil kiberxavflarning paydo bo‘lishiga sabab bo‘lmoqda. Shu boisdan, hujumlarni aniqlash va ularni erta ogohlantirish tizimlarini ishlab chiqish axborot xavfsizligini mustahkamlashda muhim ahamiyat kasb etadi.

So‘nggi yillarda tahdidlarni aniqlashda intellektual texnologiyalar, xususan, neyron tarmoqlar, tayanch vektor mashinasi (SVM) va entropiya asosidagi yondashuvlar samarali natijalar bermoqda. Mazkur tadqiqotda neyron tarmoqlar asosida tahdidlarni aniqlash algoritmi ishlab chiqilib, SVM va entropiya metodlari integratsiyalashgan holda sinovdan o‘tkazildi. Tadqiqot natijalari mujassamlangan algoritmning an’anaviy usullarga nisbatan yuqori aniqlikka ega ekanligini ko‘rsatdi. Ushbu yondashuv axborot xavfsizligi tizimlarida tahdidlarni erta aniqlashni avtomatlashtirish va himoya samaradorligini oshirish imkonini beradi.

ASOSIY QISM

Tayanch vektor mashinasi (SVM - Support Vector Machine) - bu ma’lumotlar to‘plamidagi elementlarni ikkita sinfdan biriga ajratishni ta’minlaydigan chiziqli tasniflovchi modelni aniqlashga qaratilgan metoddir. Ushbu usulning asosiy g‘oyasi - ma’lumotlar orasidagi eng optimal chiziqli chegarani topish, ya’ni har bir sinf elementlari uchun nol qiymatdan kichik yoki katta bo‘lgan chiziqli funksiya f(x) ni aniqlashdan iboratdir.

SVM algoritmi aniqlik va moslashuvchanlikni oshirish maqsadida ma'lumotlardagi aniqmaslik (noaniqlik) elementlarini qo'shish orqali yaxshilangan. Bu yondashuv sinflar chegarasiga yaqin joylashgan qaydlarni moslashuvchan tarzda tasniflash imkonini beradi va natijada birinchi hamda ikkinchi turdagi xatolar soni kamayadi. Shuning uchun SVM hujumlarni aniqlash tizimlarida samarali vosita sifatida keng qo'llanilmoqda.

Shuningdek, tarmoq hujumlarini aniqlashda Data Mining (ma'lumotlarni intellektual tahlil qilish) usullarining ahamiyati ham katta. Turli Data Mining yondashuvlari yordamida tarmoq trafigida mavjud bo'lgan tahdidlarni aniqlash, hujum turlarini farqlash va ularning chastotasini aniqlash imkoniyati yaratiladi. Tadqiqot natijalari shuni ko'rsatadiki, Data Mining usullarini qo'llash orqali tarmoqdagi zararsizlantirishlar (anomaliyalar)ni aniqlash samaradorligini sezilarli darajada oshirish mumkin.

Tadqiqot jarayonida tarmoq hujumlarini aniqlash uchun bir nechta usullar sinovdan o'tkazildi va ularning samaradorlik ko'rsatkichlari tahlil qilindi (1-jadvalda keltirilgan). Ayniqsa, SVM asosida yaratilgan model tarmoqdagi tahdidlarni aniqlashda yuqori natijalarni ko'rsatdi.

Shu asosda, tadqiqotda tahdidlarni aniqlashning yangi algoritmi ishlab chiqish taklif etilgan. Ushbu algoritm intellektual tizimlar asosida yaratilgan bo'lib, tarmoqdagi o'zgarishlarni avtomatik ravishda kuzatish, g'ayritabiiy xatti-harakatlarni aniqlash va ularga javob choralari ko'rish imkonini beradi. Ishlab chiqilgan yechimning samaradorligini baholash uchun uni an'anaviy algoritmlar bilan taqqoslash zarur bo'lib, bu yondashuv real tarmoq muhitlarida tahdidlarni aniqlash darajasini yanada oshirishga xizmat qiladi.

1-jadval

Turli xil metodlarning hujumlarni aniqlash ko'rsatkichi

Malumotlarni intellektual taxlili metodlari	Hujumni aniqlash ko'rsatkichi (%)	Yolg'on axborot berish (%)
Tayanch vektor usuli (SVM)	95,5	1
k-means klasteri	65	1
Y-means klasteri	89,89	1
SVM + Genetik algoritm	99	-
SVM + Noaniq mantiq	99,56	0,44
Neyron tarmoqlari + MGK	97,22	-
G yenetik algoritmlar	97,47	0,69

E*ntropiya asosida tahdidlarni aniqlash algoritmi*: Entropiya – belgi yoki sonlarning tasodifiylik yoki ketma-ketlik o'lchovidir. Tarmoqda turli paketlar qabul qilinadi va qayta ishlanadi. Ular nol va birlardan tashkil topadi. Hujumga uchragan IP manzillarining qancha qismini tashkil topishini aniqlash uchun ham, aynan tasodifiy IP larning entropiyasidan foydalaniladi.

Tarmoqda turli paketlar qo'llaniladi, shuningdek, xujumchi o'z maqsadiga yetishish uchun maxsus usullardan foydalaniladi. Uning maqsadi entropiyani kamaytirish. Masalan: ICMP uchun ICMP flood attack, UDP uchun UDP flood attack paketlarini qo'llaydi.

Entropiya asosida tahdidlarni aniqlash algoritmi quyidagi bosqichlardan tashkil topgan:

– Paket o'lchamining entropiyasini normallashtirish;

– Manba IP manzili entropiyasini normallashtirish;
– Manba port raqami entropiyasini normallashtirish;
– Masofadagi IP manzili entropiyasini normallashtirish;
– Masofadagi port raqami entropiyasini normallashtirish;
– Paket turi (ICMP, TCP va UDP) entropiyasini normallashtirish.

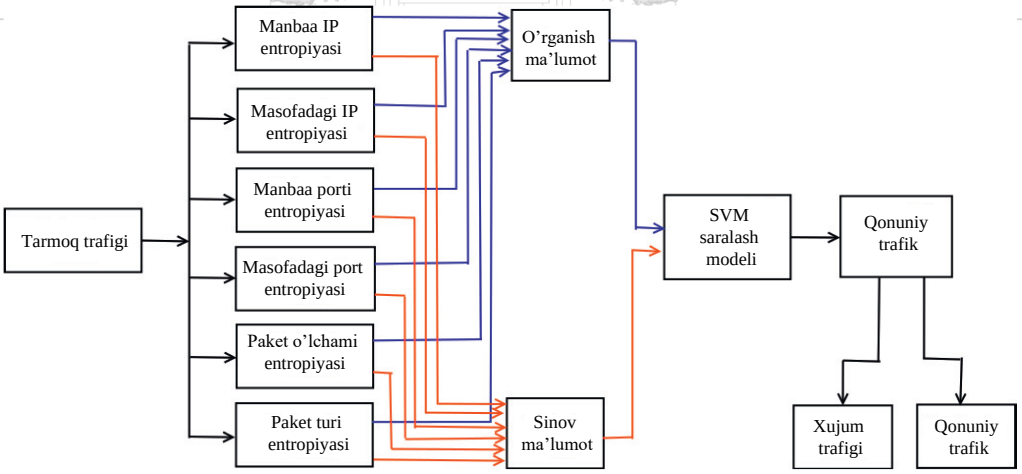
Xujum vaqtida ushbu algoritm, paket entropiyasi normallashtiriladi va odatiy qiymatlari bilan taqqoslanadi, agar farq mavjud bo‘lsa, foydalanuvchiga xabar chiqaradi, yoki keyingi tekshirishni amalga oshiradi.

Neyron tarmoqlar yordamida tahdidlarni aniqlash algoritmi. Keltirilgan neyron tarmoq asosida qurilgan tahdidlarni aniqlash usulining ichida tahdidlarni va tahdid mavjud paketlarni sinflashtirish funksiyasi mavjud edi. Shunga muvofiq tahdidlarni aniqlashda SVM (Support Vector Machine) sinflashtirishdan foydalanish amalga oshirildi. SVM – sinflashtirish usullarining eng yaxshisi hisoblanadi. SVM algoritmlarini tarmoqda qo‘llash natijasida, paketlarni oson saralash va u haqida xulosalalar qabul qilish imkoniyatlariga ega bo‘linadi. Unda ham neyron tarmoqlar kabi, paketni o‘rganish, tahlil qilish va qaror qabul qilish bosqichlari mavjud.

Tarmoq hususiyatlarini ajratish quyidagi bosqichlardan tashkil topgan:
– farq qiladigan manbaning IP manzillar soni;
– farq qiladigan manbaning port manzillar soni;
– masofadagi farq qiladigan manbaning IP manzillar soni;
– masofadagi farq qiladigan manbaning port manzillar soni;
– farq qiladigan paket turlari soni (ICMP, TCP yoki UDP);
– bir hil paket o‘lchamdagi turli paketlarning soni.

Ushbu tarmoq hususiyatlari LIBSAP kutubxonasini qo‘llagan holda, har 60 sekundda tarmoqdan ajratib olinadi. Bundan keyin ushbu qiymatlar normallashtiriladi. Normallashtirilgan tarmoq hususiyatlari SVM asosida o‘rganiladi va SVM model tarmoqdagi o‘zgarishlarni aniqlashi mumkin.

Ushbu tadqiq ishida neyron tarmoqlarning ichida SVM va entropiya asosida tarmoq tahdidlarini aniqlash algoritmini taklifi berildi. Ular asosida entropiyadan chiqqan natija yana bir bor SVM da o‘rganiladi va ikkita algoritmdan chiqqan qaror tahlil qilinadi (1-rasmda berilgan).



1-rasm. Tahdidlarni aniqlash algoritmining sxemasi

Tahdidlarni aniqlashda SVM tahdidlarni saralashning yaxshi usuli bo‘lsa, entropiya natijani chop etishda qulay hisoblanadi. SVM yo‘naltirilgan tarmoq trafiklari

uchun yaxshi natija bermaydi. Chunki unda paketlar bir turda etib belgilanadi. Ushbu algoritmda tarmoq hususiyatlari algoritmda berilgan ketma-ketlikda hisoblanadi va normallashtirilgan entropiyalar SVM ga tarmoq hususiyatlarini o‘rganish uchun jo‘natiladi.

Tahlil qilingan algoritm dasturiy vositada amalga oshirilgan natijalar 2-jadvalda berildi.

2-jadval
Algoritmlarning sifat ko‘rsatkichlarini tahlillash

	Entropiyaga asoslangan	SVM ga asoslangan	Mujassamlashgan
Saralash to‘g‘ri	85.71%	77.71%	97.25%
Saralash noto‘g‘ri	14.29%	22.29%	2.75%

2-jadvalda keltirilgan natijalar tahliliga ko‘ra, entropiya va SVM asosida ishlab chiqilgan mujassamlangan algoritm tahdidlarni aniqlashda eng yuqori aniqlik - 97,25% natijani ko‘rsatdi. Bu ko‘rsatkich entropiya asosidagi modelga nisbatan 11,54%, SVM asosidagi modelga nisbatan esa 19,54% yuqori ekanligi aniqlangan. Tadqiqot shuni ko‘rsatadiki, bir nechta metodlarning kombinatsiyasi tarmoq hujumlarini aniqroq tasniflash imkonini beradi. Shuningdek, mujassamlangan yondashuv xatolik ehtimolini kamaytirib, noto‘g‘ri saralash foizini atigi 2,75% gacha tushirdi. Natijalar taklif etilgan algoritmning samaradorligi va barqarorligini amaliy qo‘llash uchun yetarli darajada yuqori ekanligini tasdiqlaydi. Ushbu yondashuv axborot xavfsizligi tizimlarida tahdidlarni aniqlashning ilg‘or usuli sifatida tavsiya etilishi mumkin.

XULOSA

Tadqiqot natijalariga ko‘ra, tarmoq tahdidlarini aniqlashda neyron tarmoqlar, entropiya va SVM (tayanch vektor mashinasi) asosida ishlab chiqilgan mujassamlangan algoritm yuqori samaradorlikni namoyon etdi. Entropiya va SVM usullarining birgalikda qo‘llanilishi tahdidlarni aniqlash aniqligini 97,25% gacha oshirdi hamda noto‘g‘ri saralash darajasini 2,75% gacha kamaytirdi. Ushbu natijalar mujassamlangan yondashuv tarmoqdagi anomaliyalarni tez va ishonchli tarzda aniqlash imkonini berishini ko‘rsatadi. Shuningdek, SVM sinflashtirishning kuchli tomoni — aniqlik, entropiya usulining ustunligi esa tezkorlik va o‘zgaruvchan muhitga moslashuvchanlikdir. Natijada, ularning integratsiyasi axborot xavfsizligi tizimlarida real vaqt rejimida tahdidlarni erta aniqlash uchun samarali yechim hisoblanadi. Taklif etilgan algoritmni amaliy tizimlarga joriy etish orqali kiberhujumlarni aniqlash va ularga qarshi kurashish sifatini sezilarli darajada yaxshilash mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Samarov, H. K., & Bekmirzayev, O. N. (2023). Masofaviy o‘qitish tizimlarida mavjud risklar va ularni minimallashtirish istiqbollari. Research and Education, 2(4), 146-155.

2. Bekmirzayeva, M. (2024). Vizuallashtirish tizimlarida yomg‘ir va qor muammolarini tasvirga dastlabgi ishlov berish yordamida bartaraf etish. Digital Transformation and Artificial Intelligence, 2(1), 120-124.

3. Bekmirzayev, O., & Sabirov, X. (2023). “Kompyuter arxitekturasi” fanini o ‘qitish samaradorligini oshirishda zamonaviy pedagogik texnologiyalarning interfaol usullaridan foydalanish. Science and Innovation, 2 (Special Issue 14), 549-551.

4. Muminov, B., Bekmirzaev, O., & Al-Khwarizmi, M. (2022). Classification and analysis of network attacks in the category of “denial of service” information system. central asian journal of education and computer sciences (CAJECS), 1, 7-15.

5. Бекмирзаев О., Турсунов Ж. Алгоритмы системы одностороннего межсетевого взаимодействия и система обнаружения вторжений //Digital Transformation and Artificial Intelligence. – 2023. – Т. 1. – №. 4. – С. 135-145.

6. Axmedova, N., & Bekmirzaev, O. (2022). Analysis of methods of fighting against network attacks of the “denial of service” category on information systems. central asian journal of education and computer sciences (CAJECS), 1, 5.

7. Bekmirzayev, O., & Muminov, B. (2024). The Role and Application of Artificial Intelligence in Identifying Threats to Information Systems. DTAI–2024, 1(DTAI), 85-90.