# GIBRID TARMOQ MUHITLARI UCHUN SUN’IY INTELLEKT ASOSIDAGI INTRUSION DETECTION FRAMEWORK

**Qo‘yliyev Behro‘z Sherzod o‘g‘li**
**Xayriddinov Shaxboz Shavkatovich**
**Normamatov Xusan Baxodir o‘g‘li**
**Seytmamatov Sohibjon Muzaffar o‘g‘li**
*TATU, Kiberxavfsizlik fakulteti talabalari*

**Annotatsiya:** *Raqamli texnologiyalar va tarmoq infratuzilmalarining rivojlanishi natijasida kiberhujumlar soni va murakkabligi ortib bormoqda. An’anaviy xavfsizlik tizimlari zamonaviy tahdidlarni aniqlashda yetarli samaradorlikka ega emasligi sababli sun’iy intellekt asosidagi intrusion detection tizimlariga ehtiyoj ortmoqda. Mazkur maqolada gibrid tarmoq muhitlari uchun sun’iy intellekt asosidagi intrusion detection framework modeli taklif etiladi. Tadqiqot davomida mashinaviy o‘qitish algoritmlari yordamida zararli trafiklarni aniqlash usullari tahlil qilinadi hamda Random Forest, Support Vector Machine va Deep Neural Network algoritmlarining samaradorligi o‘rganiladi.*

**Kalit so‘zlar:** *intrusion detection, sun’iy intellekt, mashinaviy o‘qitish, kiberxavfsizlik, gibrid tarmoq, IDS, deep learning, network security.*

So‘nggi yillarda korporativ tarmoqlar, bulutli hisoblash tizimlari va IoT qurilmalarining keng qo‘llanilishi natijasida tarmoq infratuzilmalari murakkablashib bormoqda. Gibrid tarmoq muhitlari lokal tarmoqlar, bulutli platformalar va simsiz qurilmalarni birlashtirgan holda ishlaydi. Bunday murakkab arxitektura kiberjinoyatchilar uchun yangi imkoniyatlarni yaratmoqda.

Kiberhujumlar orasida DDoS, ransomware, phishing, botnet va zero-day ekspluatatsiya kabi tahdidlar alohida xavf tug‘diradi. An’anaviy intrusion detection tizimlari asosan signature-based yoki rule-based mexanizmlarga asoslanadi. Ushbu yondashuvlar oldindan ma’lum bo‘lgan hujumlarni aniqlashda samarali bo‘lsa-da, yangi va noma’lum tahdidlarni aniqlashda yetarli emas.

Sun’iy intellekt va mashinaviy o‘qitish texnologiyalari esa katta hajmdagi tarmoq trafiklarini tahlil qilish, anomal holatlarni aniqlash va real vaqt rejimida tahdidlarni bashorat qilish imkonini beradi. Mazkur maqolada gibrid tarmoq muhitlari uchun AI-based intrusion detection framework ishlab chiqiladi hamda uning samaradorligi tahlil qilinadi.

Intrusion Detection tizimlari tushunchasi

Intrusion Detection System (IDS) bu tarmoq yoki axborot tizimlarida ruxsatsiz kirishlarni aniqlash uchun mo‘ljallangan xavfsizlik tizimidir. IDS tizimlari tarmoq faoliyatini monitoring qiladi va shubhali harakatlarni aniqlaydi.

IDS tizimlari quyidagi turlarga bo‘linadi:

| IDS turi | Tavsifi |
|---|---|

| | |
|---|---|
| Network-based IDS | Tarmoq trafiklarini monitoring qiladi |
| Host-based IDS | Qurilma ichidagi faoliyatni nazorat qiladi |
| Signature-based IDS | Ma’lum hujum signaturalari asosida ishlaydi |
| Anomaly-based IDS | G‘ayritabiiy faoliyatni aniqlaydi |
| Hybrid IDS | Bir nechta metodlarni birlashtiradi |

Gibrid IDS tizimlari zamonaviy xavfsizlik muhitlarida eng samarali yondashuvlardan biri hisoblanadi.

Gibrid tarmoq muhitlarining xavfsizlik muammolari

Gibrid tarmoqlar turli texnologiyalarni birlashtirgani sababli xavfsizlik jihatdan murakkab hisoblanadi. Ushbu muhitlarda quyidagi tahdidlar ko‘p uchraydi:

- DDoS hujumlari;
- ichki tahdidlar;
- malware va ransomware;
- phishing hujumlari;
- zero-day ekspluatatsiyalar;
- IoT qurilmalariga hujumlar.

Bulutli tizimlar va IoT qurilmalarining integratsiyasi xavfsizlik monitoringini yanada qiyinlashtiradi. An’anaviy xavfsizlik vositalari katta hajmdagi trafikni real vaqt rejimida tahlil qilishda cheklangan imkoniyatlarga ega

Sun’iy intellekt asosidagi intrusion detection

Sun’iy intellekt asosidagi IDS tizimlari tarmoqdagi normal va anomal faoliyatlarni o‘rganadi. Ushbu tizimlar tarixiy ma’lumotlar asosida model yaratadi va yangi trafiklarni avtomatik tahlil qiladi.

AI-based IDS ishlash bosqichlari:

1. Ma’lumotlarni yig‘ish
2. Trafikni oldindan qayta ishlash
3. Belgilarni ajratib olish
4. Modelni o‘qitish
5. Anomaliyalarni aniqlash
6. Ogohlantirish va javob qaytarish

Mashinaviy o‘qitish algoritmlari

Random Forest algoritmi

Random Forest intrusion detection tizimlarida eng samarali algoritmlardan biri hisoblanadi. Ushbu algoritm bir nechta qaror daraxtlari asosida ishlaydi.

Afzalliklari:

- yuqori aniqlik;
- katta ma’lumotlarni qayta ishlash;
- overfitting muammosining kamayishi.

Kamchiliklari:

- hisoblash resurslari talabi yuqori;
- model hajmi katta.

### Support Vector Machine algoritmi

SVM algoritmi tarmoq trafiklarini ikki sinfga ajratadi: normal va zararli trafik.

$$f(x) = w^T x + b$$

Bu yerda:

- $w$ — vazn vektori;
- $x$ — kiruvchi ma‘lumotlar;
- $b$ — siljish parametri.

SVM algoritmi intrusion detection tizimlarida yuqori aniqlik bilan ishlaydi.

*Support Vector Machine algoritmi*

SVM algoritmi tarmoq trafiklarini ikki sinfga ajratadi: normal va zararli trafik.

f(x)=wTx+bf(x)=w^Tx+bf(x)=wTx+b

Bu yerda:

- www — vazn vektori;
- xxx — kiruvchi ma’lumotlar;
- bbb — siljish parametri.

SVM algoritmi intrusion detection tizimlarida yuqori aniqlik bilan ishlaydi.

Deep Neural Network

Deep Learning asosidagi intrusion detection tizimlari murakkab tarmoq hujumlarini aniqlash imkonini beradi. Neyron tarmoqlar katta hajmdagi ma’lumotlardan yashirin naqshlarni aniqlaydi.

Deep Neural Network afzalliklari:

- yuqori aniqlik;
- avtomatik feature extraction;
- noma’lum hujumlarni aniqlash.

Kamchiliklari:

- katta GPU resurslari talab etadi;
- modelni o‘qitish murakkab.

Taklif etilayotgan AI-based framework

Mazkur tadqiqotda quyidagi arxitekturaga ega intrusion detection framework taklif etiladi:

| Modul | Vazifasi |
|---|---|
| Data Collection Layer | Tarmoq trafiklarini yig‘ish |
| Preprocessing Layer | Ma’lumotlarni tozalash |
| Feature Extraction Layer | Muhim belgilarni ajratish |
| AI Analysis Engine | ML/DL algoritmlari yordamida tahlil |
| Threat Detection Module | Tahdidlarni aniqlash |
| Alert & Response System | Ogohlantirish va himoya |

Framework real vaqt monitoringini amalga oshiradi hamda zararli trafik aniqlanganda avtomatik javob qaytaradi.

Framework ishlash prinsipi

Taklif etilgan model quyidagi bosqichlarda ishlaydi:

1. Tarmoq trafiklari sensorlar orqali yig‘iladi.
2. Trafik ma’lumotlari preprocessing moduliga uzatiladi.
3. Feature extraction bosqichida IP manzil, port, paket hajmi va protokol xususiyatlari ajratiladi.
4. AI engine trafikni tahlil qiladi.
5. Shubhali faoliyat aniqlansa alert yaratiladi.
6. Firewall yoki IPS tizimiga avtomatik buyruq yuboriladi.

Algoritmlar samaradorligini taqqoslash

| Algoritm | Aniqlik (%) | False Positive | Tezlik |
|---|---|---|---|
| Decision Tree | 88 | Yuqori | Yuqori |
| Random Forest | 97 | Past | O‘rta |
| SVM | 95 | Past | O‘rta |
| Deep Neural Network | 99 | Juda past | Past |
| Naive Bayes | 84 | O‘rta | Yuqori |

Jadvaldan ko‘rinib turibdiki, Deep Neural Network va Random Forest algoritmlari eng samarali natijalarni ko‘rsatgan.

Taklif etilgan framework afzalliklari

Taklif etilgan framework quyidagi ustunliklarga ega:

- real vaqt monitoringi;
- yuqori aniqlik;
- yangi tahdidlarni aniqlash;
- avtomatik javob mexanizmi;
- katta hajmdagi trafik bilan ishlash;
- bulutli va IoT muhitlariga moslashuvchanlik.
-

**Xulosa**

Gibrid tarmoq muhitlarida kiberxavfsizlikni ta’minlash zamonaviy axborot tizimlari uchun muhim masalalardan biri hisoblanadi. An’anaviy intrusion detection tizimlari murakkab va yangi turdagi hujumlarni aniqlashda yetarli samaradorlikka ega emas. Sun’iy intellekt asosidagi intrusion detection framework esa katta hajmdagi trafikni tahlil qilish, anomal faoliyatlarni aniqlash va real vaqt rejimida tahdidlarni aniqlash imkonini beradi.

Tadqiqot natijalari Random Forest va Deep Neural Network algoritmlari intrusion detection vazifalarida yuqori aniqlik ko‘rsatishini tasdiqladi. Kelgusida federated learning, explainable AI va edge computing texnologiyalarini intrusion detection tizimlariga integratsiya qilish yanada samarali himoya mexanizmlarini yaratishga yordam beradi.

**FOYDALANILGAN ADABIYOTLAR:**

1. William Stallings. Network Security Essentials. Pearson Education, 2017.
2. Ian Goodfellow. Deep Learning. MIT Press, 2016.
3. Bishop C. Pattern Recognition and Machine Learning. Springer, 2006.
4. S. Axelsson. Intrusion Detection Systems: A Survey and Taxonomy. IEEE, 2000.
5. Tavallaee M. A Detailed Analysis of the KDD CUP 99 Dataset. IEEE, 2009.
6. Garcia-Teodoro P. Anomaly-Based Network Intrusion Detection. Elsevier, 2009.
7. Kim G. A Survey of Intrusion Detection Systems Using Deep Learning. IEEE Access, 2020.
8. OWASP Cybersecurity Reports.