ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

SUN'IY INTELLEKT ASOSIDA ISHLOVCHI IDS/IPS ALGORITMLARINING TARMOQ TAHDIDLARINI ANIQLASHDAGI SAMARADORLIGINI BAHOLASH

Mo'ydinov Mirjalol Zokirovich
University of Management and Future Technologies Telekommunikatsiya injiniringi magistranti

https://doi.org/10.5281/zenodo.15549997

Annotatsiya. *Ushbu maqolada sun'iy intellekt (SI) asosida ishlovchi tarmoq xavfsizligi tizimlari – Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) algoritmlarining tarmoq tahdidlarini aniqlashdagi samaradorligi ko'rib chiqiladi. IDS/IPS tizimlarining an'anaviy metodlardan farqli jihatlari, sun'iy neyron tarmoqlar, mashinaviy o'rganish (ML), chuqur o'rganish (DL) va tabiiy tilni qayta ishlash (NLP) kabi SI uslublarini qo'llash orqali tahdidlarni aniqlash aniqligi va tezligi tahlil qilinadi. Shuningdek, real vaqt rejimida ishlovchi zamonaviy SI-IDS/IPS tizimlarining afzalliklari va cheklovlari tahlil qilinadi.*

Kalit so'zlar: *IDS, IPS, Sun'iy intellekt, tarmoq xavfsizligi, mashinaviy o'rganish, tahdidni aniqlash, kiberxavfsizlik.*

ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМОВ IDS/IPS НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОБНАРУЖЕНИИ СЕТЕВЫХ УГРОЗ

Аннотация. *В статье рассматривается эффективность систем сетевой безопасности на основе искусственного интеллекта (ИИ) — алгоритмов систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) — при обнаружении сетевых угроз. Анализируются различия между системами IDS/IPS и традиционными методами, а также точность и скорость обнаружения угроз с использованием методов ИИ, таких как искусственные нейронные сети, машинное обучение (МО), глубокое обучение (ГО) и обработка естественного языка (НЯ). Также анализируются преимущества и ограничения современных систем SI-IDS/IPS реального времени.*

Ключевые слова: *IDS, IPS, искусственный интеллект, сетевая безопасность, машинное обучение, обнаружение угроз, кибербезопасность.*

EVALUATING THE EFFECTIVENESS OF AI-BASED IDS/IPS ALGORITHMS IN DETECTING NETWORK THREATS

Abstract. *This article reviews the effectiveness of AI-based network security systems – Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) algorithms in detecting network threats. The differences between IDS/IPS systems and traditional methods, the accuracy and speed of threat detection using AI techniques such as artificial neural networks, machine learning (ML), deep learning (DL), and natural language processing (NLP) are analyzed. The advantages and limitations of modern AI-IDS/IPS systems operating in real time are also analyzed.*

Keywords: *IDS, IPS, Artificial Intelligence, network security, machine learning, threat detection, cybersecurity.*

Kirish

So'nggi yillarda axborot texnologiyalarining jadal rivojlanishi inson hayotining deyarli barcha jabhalarida raqamlashtirish jarayonining keng ko'lamda amalga oshirilishiga olib keldi.

Internet tarmoqlariga ulanayotgan qurilmalar sonining keskin oshishi, bulutli texnologiyalar, Internet of Things (IoT) va sanoat avtomatizatsiyasi kabi sohalarning rivojlanishi bilan bir qatorda, tarmoq xavfsizligiga tahdid soluvchi omillar ham ortib bormoqda.

Kiberhujumlar murakkablashib, ularning aniqlanishi va oldini olish jarayonlari an’anaviy xavfsizlik yondashuvlari uchun yetarlicha samarali bo‘lmay qolmoqda. Hozirgi tahdidlar – bu oddiy viruslar yoki zararli fayllar emas, balki o‘z-o‘zini yashira oladigan, noto‘g‘ri trafik oqimlariga "yopishib" oladigan, ma’lumotlarni yashirin tarzda o‘g‘irlaydigan va bir vaqtning o‘zida turli hujum shakllarini uyg‘unlashtiradigan murakkab kiberhujumlardir.

Bunday muammolarga qarshi kurashishda **IDS (Intrusion Detection System)** va **IPS (Intrusion Prevention System)** kabi xavfsizlik tizimlari muhim o‘rin tutadi. IDS/IPS texnologiyalari ma’lumotlar oqimini real vaqt rejimida tahlil qiladi va tahdidlarni aniqlash yoki ularning oldini olish vazifasini bajaradi. Biroq, an’anaviy IDS/IPS tizimlarining asosiy kamchiligi – ularning ko‘pchiligi signaturaga asoslanganligi sababli faqat oldindan ma’lum bo‘lgan tahdidlarni aniqlash imkoniyatiga ega. Bu esa yangi turdagi noma’lum (zero-day) hujumlar oldida ularni ojiz holga keltiradi.

Shu bois, **sun’iy intellekt (SI)** va uning tarkibiy qismlari – mashinaviy o‘rganish (Machine Learning), chuqur o‘rganish (Deep Learning), mustahkamlovchi o‘rganish (Reinforcement Learning) – asosida yaratilgan IDS/IPS tizimlari kiberxavfsizlikda yangi paradigma sifatida namoyon bo‘lmoqda. Ushbu maqolaning asosiy maqsadi SI asosidagi IDS/IPS tizimlarining tarmoq tahdidlarini aniqlashdagi samaradorligini chuqur tahlil qilish, amaliy jihatlarini ko‘rsatish va ularni baholash mezonlarini yoritishdan iborat.

IDS/IPS TIZIMLARINING UMUMIY TAVSIFI

IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) – bu axborot tarmoqlari orqali ro‘y berayotgan tahdidlarni aniqlash va bartaraf etishga qaratilgan maxsus xavfsizlik tizimlaridir. Ular tarmoqda harakatlanayotgan trafikni yoki kompyuter tizimi ichidagi faoliyatni tahlil qilib, xavfsizlik siyosatiga zid holatlarni aniqlashga mo‘ljallangan.

1. IDS (Intrusion Detection System)

IDS – bu passiv xavfsizlik tizimi bo‘lib, u tahdidlarni aniqlaydi va bu haqda administratorga xabar beradi. IDS hujumni to‘xtatmaydi, lekin uning mavjudligini ko‘rsatadi. IDS quyidagi turlarga bo‘linadi:

- **Network-based IDS (NIDS)** – tarmoqdagi trafikni kuzatadi.
- **Host-based IDS (HIDS)** – biror tizim yoki qurilmadagi log fayllar, fayl tizimi va boshqa ichki faoliyatni nazorat qiladi.

2. IPS (Intrusion Prevention System)

IPS – bu faol xavfsizlik tizimi bo‘lib, u nafaqat hujumni aniqlaydi, balki unga qarshi chora ham ko‘radi. IPS real vaqt rejimida ishlaydi va quyidagi choralarni ko‘rishi mumkin:

- Tarmoq trafikini to‘sish yoki bloklash
- Zararli paketlarni yo‘q qilish
- Seanslarni tugatish
- Tizim siyosatini avtomatik ravishda yangilash

3. An’anaviy IDS/IPS yondashuvlari

An’anaviy IDS/IPS tizimlari quyidagi ikki asosiy metodga tayanadi:

- **Signatura asosidagi aniqlash (Signature-based detection):** Oldindan ma’lum bo‘lgan hujumlar signaturalari bilan taqqoslash orqali aniqlash. Bu metod tez va samarali, lekin yangi hujumlarni aniqlay olmaydi.
- **Anomaliya asosidagi aniqlash (Anomaly-based detection):** Normal faoliyatni o‘rganib, undan chetga chiqqan har qanday xatti-harakatni tahdid sifatida aniqlaydi. Bu metod yangi hujumlarni aniqlashda foydalidir, ammo ko‘p hollarda soxta ijobiylar (False Positives) yuqori bo‘ladi.

SUN’IY INTELLEKTNING IDS/IPS TIZIMLARIDA QO‘LLANILISHI

Sun’iy intellekt asosida ishlovchi IDS/IPS tizimlari o‘zining o‘zgaruvchanlik, moslashuvchanlik va yuqori aniqlikdagi tahlil qobiliyatlari bilan tahdidlarni an’anaviy usullardan ancha samarali aniqlay oladi. Quyida SI asosida qo‘llaniladigan asosiy yondashuvlar keltiriladi:

1. Mashinaviy o‘rganish (Machine Learning – ML)

ML algoritmlari ma’lumotlar asosida tahdidlarni avtomatik ravishda o‘rganib, ularni tasniflash imkonini beradi. IDS/IPS tizimlarida eng ko‘p qo‘llaniladigan ML algoritmlari:

- **Decision Tree (DT):** Qaror daraxti asosida trafikni xavfli yoki xavfsiz deb tasniflaydi.
- **Random Forest (RF):** Bir nechta qaror daraxtlarini uyg‘unlashtirib, yuqori aniqlikka ega bo‘lgan model yaratadi.
- **Support Vector Machines (SVM):** Belgilangan ikki sinf orasidagi eng yaxshi farqlovchi chiziqni topadi.
- **K-Nearest Neighbors (KNN):** Har qanday yangi trafikni unga eng yaqin bo‘lgan o‘quv namunalariga qarab baholaydi.

ML asosida ishlovchi IDS/IPS tizimlari **anomaliya aniqlash**da eng yuqori samaradorlikka ega hisoblanadi.

2. Chuqur o‘rganish (Deep Learning – DL)

DL – bu sun’iy neyron tarmoqlarga asoslangan ilg‘or o‘rganish metodi bo‘lib, katta hajmdagi murakkab ma’lumotlar ustida ishlay oladi. IDS/IPS tizimlarida DL algoritmlarining qo‘llanishi quyidagicha:

- **Convolutional Neural Networks (CNN):** Tarmoq trafik ma’lumotlarini tasvir sifatida ko‘rib chiqadi, bu orqali vizual anomaliyalarni aniqlash mumkin.
- **Recurrent Neural Networks (RNN):** Vaqtga bog‘liq bo‘lgan trafik o‘zgarishlarini o‘rganadi, masalan, DDoS hujumlar.
- **Autoencoders:** Trafikdagi normal holatni o‘rganadi va bu normalikdan chetga chiqqan harakatlarni anomaliya sifatida aniqlaydi.

3. Mustahkamlovchi o‘rganish (Reinforcement Learning – RL)

RL – bu agent atrof-muhit bilan o‘zaro ta’sirda bo‘lib, harakatlariga qarab mukofot oladigan o‘rganish modeli. IDS/IPS tizimlarida RL orqali quyidagilar amalga oshiriladi:

- Tarmoqda real vaqt rejimida optimal qaror qabul qilish
- O‘z-o‘zini sozlash
- Davriy tahdidlar va strategik hujumlarga moslashish

4. Hibrid yondashuvlar

So‘nggi yillarda **hibrid yondashuvlar** – ya’ni ML, DL va RL uslublarining birgalikda qo‘llanilishi orqali yanada yuqori aniqlikdagi, kam soxta ijobiy ko‘rsatkichga ega bo‘lgan, moslashuvchan IDS/IPS tizimlari yaratilmoqda.

3. Sun’iy intellekt asosida ishlovchi IDS/IPS tizimlarining samaradorligini baholash mezonlari

Sun’iy intellekt yordamida ishlaydigan IDS/IPS tizimlarining samaradorligini baholashda klassik statistik, hisoblash va funksiya asosidagi metrikalar qo‘llaniladi. Ular tizimning tahdidlarni aniqlash aniqligi, noto‘g‘ri aniqlash darajasi, ishlash tezligi va resurs iste’molini baholash imkonini beradi.

Mezon	Tavsif
Aniqlik (Accuracy)	To‘g‘ri tasniflangan trafik ulushi.
Senzitivlik (Recall)	Aniqlangan haqiqiy tahdidlar ulushi.
F1-mezon	Precision va Recall ko‘rsatkichlarining garmoniyasi.
Soxta ijobiylar (FP)	Xavfsiz trafikni tahdid deb noto‘g‘ri aniqlash holatlari.
Soxta salbiylar (FN)	Tahdidli trafikni xavfsiz deb noto‘g‘ri aniqlash holatlari.
Tezlik (Latency)	Tahdidni aniqlash va javob berishdagi kechikish vaqti.
Moslashuvchanlik	Yangi, ilgari noma’lum bo‘lgan hujumlarni aniqlash qobiliyati.

REAL HOLATLAR VA EKSPERIMENTAL TAHLIL

Sun’iy intellekt asosidagi IDS/IPS tizimlari samaradorligi bir nechta mashhur ma’lumotlar to‘plamlari asosida sinovdan o‘tkaziladi. Ular orasida:

- **KDD Cup 1999**
- **NSL-KDD**
- **CICIDS2017**
- **UNSW-NB15**

1. NSL-KDD to‘plami asosidagi tahlil

Ko‘plab tadqiqotlarda ushbu to‘plam asosida SVM, Random Forest, CNN kabi algoritmlar sinovdan o‘tkazilgan.

Algoritm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Random Forest	95.4	94.8	93.5	94.1
SVM	91.2	90.3	88.9	89.6
CNN	96.8	96.5	95.7	96.1

2. Real holatdagi tadbiq misoli

Bir yirik bank tizimida chuqur o‘rganishga asoslangan IDS joriy etildi. An’anaviy signaturali tizim soatiga o‘rtacha 50 dan ortiq soxta ijobiy holat qayd etgan bo‘lsa, SI asosida ishlaydigan yangi tizim ushbu ko‘rsatkichni 5 taga kamaytirishga erishdi, bu esa xavfsizlik xodimlarining yukini sezilarli darajada kamaytirdi.

AFZALLIKLAR VA CHEKLOVLAR

Afzalliklar:

1. **Yuqori aniqlik:** SI algoritmlari tarmoqdagi eng noaniq va murakkab tahdidlarni aniqlay oladi.
2. **O‘rganish qobiliyati:** Model vaqt o‘tishi bilan yangi ma’lumotlar asosida o‘zini yangilay oladi.
3. **Zero-day hujumlarni aniqlash:** Anomaliya asosidagi yondashuvlar yangi, noma’lum hujumlarni aniqlash imkonini beradi.
4. **Moslashuvchanlik:** Har xil tarmoq muhitlari va tahdid turlariga tez moslasha oladi.

Cheklovlar:

1. **Ma’lumotlarga bog‘liqlik:** O‘rganish uchun katta hajmdagi to‘g‘ri belgilangan ma’lumotlar to‘plamlari zarur.
2. **Resurs talabi:** SI modellari, ayniqsa DL algoritmlari, kuchli protsessorlar va katta xotira talab qiladi.
3. **Soxta ijobiylar:** Har doim ham SI modeli mukammal ishlamaydi; noto‘g‘ri ogohlantirishlar xavfi bor.
4. **Tushunarlilik (Interpretability):** Ayniqsa chuqur o‘rganish modellari “qora quti” bo‘lib, nega aynan shu qarorni qabul qilgani tushunarsiz bo‘lishi mumkin.

XULOSA

Sun’iy intellekt asosida ishlab chiqilgan IDS/IPS tizimlari zamonaviy kiberxavfsizlik infratuzilmasining ajralmas qismiga aylanmoqda. An’anaviy signatura va qoidaga asoslangan tizimlar hozirgi murakkab kiberhujumlarga qarshi samarali bo‘lmay qolgan bir paytda, mashinaviy o‘rganish, chuqur o‘rganish va mustahkamlovchi o‘rganishga asoslangan yondashuvlar tahdidlarni aniqlashda yuqori sezuvchanlik va aniqlikka erishmoqda.

Shunga qaramay, bunday tizimlar muvaffaqiyatli ishlashi uchun katta hajmdagi sifatli ma’lumotlar, kuchli hisoblash resurslari va optimallashtirilgan algoritmlar zarur. Hozirgi paytda ilmiy va sanoat doiralarida SI asosidagi IDS/IPS tizimlarni amaliyotga tadbiq etish bo‘yicha jadal izlanishlar olib borilmoqda.

Kelajakda **AI asosidagi IDS/IPS tizimlari** o‘z-o‘zini boshqaruvchi, kontekstga moslashuvchi, xavflarni prognoz qila oluvchi va foydalanuvchi xatti-harakatlaridan kelib chiqib oldindan tahdidlarni aniqlovchi avtonom xavfsizlik tizimlariga aylanishi kutilmoqda.

REFERENCES

1. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection.
2. Zhang, J., & Zulkernine, M. (2006). Anomaly based network intrusion detection with unsupervised outlier detection.
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection.
4. Javaid, A., et al. (2016). A deep learning approach for network intrusion detection system.
5. Garcia-Teodoro, P., et al. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges.