

DEEP LEARNING ASOSIDA TARMOQ TRAFIGINI TAHLIL QILISH

Usmanbayev Doniyorbek Shuxratovich¹, Raymqulova Gulzoda Ne'matjon qizi²

¹*Muhammad al-Xorazmiy nomidagi TATU katta o'qituvchisi*

²*Toshkent Axborot Texnologiyalari Universiteti talabasi*

Annotatsiya. Ushbu ishda kompyuter tarmoqlarida trafikni tahlil qilishda deep learning (chuqur o'rganish) texnologiyalaridan foydalanish masalalari yoritilgan. Zamonaviy tarmoqlarda ma'lumotlar oqimining keskin ortishi va kiberxavfsizlikka bo'lgan talabning kuchayishi an'anaviy tahlil usullarining samaradorligini cheklab qo'ymoqda. Deep learning modellari, jumladan, neyron tarmoqlar asosida trafikni real vaqt rejimida tahlil qilish, anomal holatlarni aniqlash va hujumlarni bashorat qilish imkoniyati ko'rib chiqilgan. Tadqiqot natijalari tarmoq xavfsizligini oshirish va aqlli monitoring tizimlarini yaratishda muhim ahamiyatga ega.

Kalit so'zlar: deep learning, tarmoq trafigi, kiberxavfsizlik, neyron tarmoqlar, anomaliyalarni aniqlash.

Abstract: This paper discusses the analysis of network traffic using deep learning techniques. The rapid growth of network data and increasing cybersecurity threats have reduced the effectiveness of traditional traffic analysis methods. Deep learning models, particularly neural networks, enable efficient real-time traffic analysis, anomaly detection, and cyberattack prediction. The study highlights the advantages of deep learning-based approaches in improving network security and developing intelligent traffic monitoring systems.

Keywords: deep learning, network traffic, cybersecurity, neural networks, anomaly detection.

Аннотация. В данной работе рассматриваются вопросы анализа сетевого трафика на основе технологий глубокого обучения (deep learning). Стремительный рост объемов сетевых данных и усиление киберугроз значительно снижают эффективность традиционных методов анализа. Модели глубокого обучения, основанные на нейронных сетях, позволяют осуществлять анализ трафика в реальном времени, выявлять аномалии и прогнозировать кибератаки. Результаты исследования имеют важное значение для повышения уровня сетевой безопасности и создания интеллектуальных систем мониторинга.

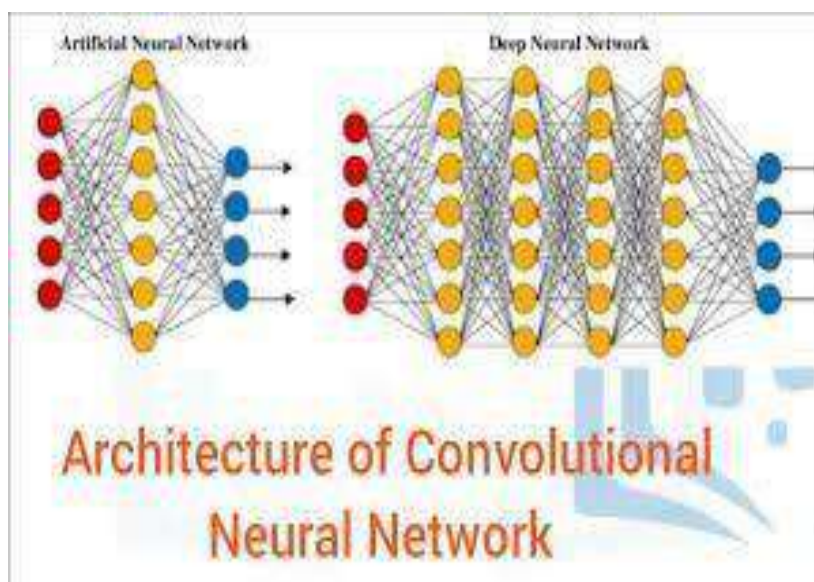
Ключевые слова: глубокое обучение, сетевой трафик, кибербезопасность, нейронные сети, обнаружение аномалий.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kompyuter tarmoqlari orqali uzatilayotgan ma'lumotlar hajmi yildan-yilga keskin ortib bormoqda. Bulutli hisoblash, IoT (Internet of Things), mobil tarmoqlar va raqamli xizmatlarning kengayishi tarmoq trafigining murakkabligini yanada oshirmoqda. Shu bilan birga, kiberhujumlar, zararli dasturlar va tarmoqdagi anomal holatlar sonining ko'payishi tarmoq xavfsizligini ta'minlash masalasini dolzarb muammoga aylantirmoqda. An'anaviy tarmoq trafigini tahlil qilish usullari, asosan, qo'lda belgilangan qoidalar va statistik modellarga tayanadi. Bunday yondashuvlar katta hajmdagi ma'lumotlarni real vaqt rejimida qayta ishlashda, shuningdek, yangi va murakkab hujum turlarini aniqlashda yetarli darajada samarali emas. Shu sababli, zamonaviy sun'iy intellekt texnologiyalariga asoslangan yondashuvlarga ehtiyoj ortib bormoqda. Deep learning (chuqur o'rganish) usullari ko'p qatlamli neyron tarmoqlar orqali murakkab va nolinear bog'lanishlarni avtomatik aniqlash imkonini beradi.

Ushbu texnologiyalar tarmoq trafigini tahlil qilish, normal va anomal trafikni farqlash, kiberxavfsizlik tahdidlarini oldindan aniqlashda yuqori aniqlikni ta'minlaydi. Ayniqsa, konvolyutsion va rekurrent neyron tarmoqlar (CNN, RNN, LSTM) tarmoq trafigi ma'lumotlarini chuqur tahlil qilishda keng qo'llanilmoqda.

Mazkur ishda deep learning asosida tarmoq trafigini tahlil qilishning nazariy asoslari, afzalliklari hamda amaliy qo'llanilish imkoniyatlari yoritiladi. Tadqiqot natijalari zamonaviy tarmoq monitoringi va kiberxavfsizlik tizimlarini takomillashtirishga xizmat qiladi.



ASOSIY QISM

Tarmoq trafigini tahlil qilishning nazariy asoslari

Tarmoq trafigi – bu kompyuter tarmoqlari orqali uzatilayotgan ma'lumotlar paketlarining

umumiy oqimidir. Trafikni tahlil qilish tarmoq faoliyatini monitoring qilish, ishlash samaradorligini baholash hamda kiberxavfsizlikni ta'minlashda muhim ahamiyatga ega. An'anaviy trafik tahlili usullari statistik ko'rsatkichlar, signatura asosidagi aniqlash va qoidaviy filtratsiyaga asoslangan bo'lib, ular oldindan ma'lum bo'lgan hujumlarni aniqlashda samarali hisoblanadi. Biroq ushbu usullar yangi va murakkab hujum turlarini aniqlashda cheklangan imkoniyatlarga ega. Zamonaviy tarmoqlarda trafikning hajmi va xilma-xilligi oshgani sari moslashuvchan va avtomatik o'rganishga qodir yondashuvlarga ehtiyoj kuchaymoqda. Shu nuqtai nazardan, sun'iy intellekt va mashinaviy o'rganish texnologiyalari tarmoq trafigini tahlil qilishda muhim vositaga aylanmoqda.

Deep learning texnologiyalarining o'rni va afzalliklari

Deep learning – bu mashinaviy o'rganishning rivojlangan yo'nalishi bo'lib, ko'p qatlamli sun'iy neyron tarmoqlar asosida ishlaydi. Ushbu yondashuv katta hajmdagi ma'lumotlardan murakkab va yashirin bog'lanishlarni avtomatik ravishda aniqlash imkonini beradi.

Deep learning modellarining asosiy afzalligi shundaki, ular qo'lda xususiyat tanlashni talab qilmaydi va to'g'ridan-to'g'ri xom ma'lumotlar bilan ishlay oladi. Tarmoq trafigini tahlil qilishda deep learning usullari normal va anomal trafikni farqlash, hujumlarni aniqlash va tarmoq holatini bashorat qilishda yuqori aniqlikni ta'minlaydi. Ayniqsa, katta hajmdagi real vaqt ma'lumotlarini qayta ishlashda ushbu texnologiyalar samaradorligi yuqori hisoblanadi.

Neyron tarmoqlar asosidagi modellarning qo'llanilishi

Deep learning asosida tarmoq trafigini tahlil qilishda turli xil neyron tarmoq arxitekturalari qo'llaniladi. Konvolyutsion neyron tarmoqlar (CNN) trafik ma'lumotlaridagi fazoviy bog'lanishlarni aniqlashda samarali bo'lsa, rekurrent neyron tarmoqlar (RNN) va ularning takomillashtirilgan turi bo'lgan LSTM modellar vaqtga bog'liq ketma-ketliklarni tahlil qilishda keng qo'llaniladi. Ushbu modellar yordamida paketlar oqimi, protokollar xatti-harakati va trafik intensivligi chuqur o'rganiladi. Natijada, tarmoqdagi g'ayrioddiy holatlar, hujum belgilari va xavfsizlik tahdidlari yuqori aniqlik bilan aniqlanadi. Bundan tashqari, avtoenkoderlar asosidagi modellar noma'lum hujum turlarini aniqlashda samarali natijalar beradi.

Deep learning asosida anomal trafikni aniqlash

Anomal trafikni aniqlash tarmoq xavfsizligini ta'minlashda asosiy vazifalardan biri hisoblanadi. Deep learning yondashuvlari an'anaviy usullarga nisbatan moslashuvchanligi va o'z-o'zini o'rganish qobiliyati bilan ajralib turadi. Model normal trafik xususiyatlarini o'rganib, undan keskin farqlanuvchi holatlarni avtomatik ravishda anomaliya sifatida belgilaydi. Bu yondashuv zero-day hujumlar, noma'lum zararli faoliyatlar va murakkab kiberxavfsizlik tahdidlarini aniqlashda muhim ahamiyat kasb etadi. Shu sababli, deep learning asosidagi tizimlar zamonaviy tarmoq monitoringi va xavfsizlik infratuzilmasining ajralmas qismiga aylanib bormoqda.

TAHLIL VA NATIJALAR

Natija va Tahlil Elementlari	Tavsif
Umumiy samaradorlik	Deep learning yondashuvlari an'anaviy usullarga nisbatan yuqori samaradorlikka ega.
Neyron tarmoqlarning roli	Katta hajmdagi trafik ma'lumotlari chuqur o'rganilib, normal va anomal holatlar o'rtasidagi murakkab bog'lanishlar aniqlandi.
LSTM va CNN modellarining afzalligi	Vaqtga bog'liq trafik o'zgarishlarini aniqlashda yuqori aniqlikni ta'minladi.
Yashirin naqshlarni aniqlash	Trafikdagi yashirin naqshlarni aniqlash imkonini berdi.
Noma'lum va zero-day hujumlarni aniqlash	Noma'lum va zero-day hujumlarni aniqlash samaradorligini oshirdi.
Noto'g'ri aniqlashni kamaytirish	Noto'g'ri aniqlash (false positive) holatlarini sezilarli darajada kamaytirdi.
Real vaqt monitoring	Real vaqt rejimida monitoring olib borish imkoniyatini ta'minladi.
Tarmoq xavfsizligi va resurslar	Modellar tarmoq xavfsizligi darajasini oshirish va resurslarni optimallashtirishga xizmat qiladi.
Umumiy xulosa	Deep learning texnologiyalarining tarmoq monitoringi va kiberxavfsizlik tizimlarida keng qo'llanishi ilmiy va amaliy jihatdan maqsadga muvofiq.

Xulosa qilib aytganda, deep learning asosida tarmoq trafigin tahlil qilish zamonaviy axborot-kommunikatsiya tizimlarida muhim ahamiyat kasb etadi. Ushbu texnologiya katta hajmdagi va murakkab trafik ma'lumotlarini avtomatik tahlil qilish, anomal holatlarni aniqlash va kiberxavfsizlik tahdidlarini oldindan bashorat qilish imkonini beradi. Tadqiqot natijalari shuni ko'rsatadiki, deep learning modellari tarmoq xavfsizligini ta'minlashda yuqori aniqlik va moslashuvchanlikni ta'minlaydi.

Mazkur ish natijalari kelajakda aqlli tarmoq monitoring tizimlarini yaratish, kiberxavfsizlikni mustahkamlash va raqamli infratuzilmani himoyalashda ilmiy- amaliy asos bo'lib xizmat qilishi mumkin.

ADABIYOTLAR

- [1]. Karimov Sh.X., To'rayev B.B. Axborot xavfsizligi va kiberxavfsizlik asoslari. – Toshkent: Fan va texnologiya, 2020.
- [2]. Islomov D.Sh. Kompyuter tarmoqlari va ularning xavfsizligi. – Toshkent: Innovatsion

rivojlanish nashriyoti, 2021.

- [3]. Abdullayev A.R. Mashinali o'rganish va deep learning texnologiyalari. – Toshkent: Oliy ta'lim nashriyoti, 2022.
- [4]. Jo'rayev M.M., Rahmonov S.A. Axborot tizimlarida ma'lumotlarni tahlil qilish. – Toshkent: Fan, 2018.
- [5]. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Kiberxavfsizlikni rivojlantirish konsepsiyasi. – Toshkent, 2022.
- [6]. Xudoyberdiyev N.N. Kompyuter tarmoqlarida trafikni tahlil qilish usullari. – Toshkent: Texnika oliy ta'lim muassasalari uchun o'quv qo'llanma, 2020.
- [7]. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.
- [8]. Bishop C.M. Pattern Recognition and Machine Learning. – Springer, 2006.
- [9]. Kim G., Lee S., Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. – Expert Systems with Applications, 2014.
- [10]. Zhang Y., Chen X., Jin L. Network intrusion detection using deep learning. – IEEE Communications Letters, 2018.
- [11]. Wang W., Zhu M., Wang J. Deep learning for network traffic classification. – IEEE Access, 2017.