OPTIK TARMOQ XAVFSIZLIGIDA TAHDIDLARNI ANIQLASHNING MASHINALI O‘QITISH MODELLARI

Jabbarov Nuriddin Akbarovich
Muhammad al-Alxorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, o‘qituvchi
nuriddinjabbarov2696@gmail.com

Odiljonov Boburbek Abduvaxob o‘g‘li
Muhammad al-Alxorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, magistrant
boburbek068@gmail.com

ANNOTATSIYA

Biz ushbu tadqiqot ishida optik tarmoq xavfsizligini ta’minlash va ish jarayonlarini tizimlashtirish uchun mashinali o‘qitish (ML) modellarini qo‘llashni taklif etdik. ML modellari optik tarmoq xavfsizligi uchun turli xil algoritmlar va turli ma’lumotlar to‘plamlarida ishlatilishi mumkin. Ushbu modellar oldindan belgilangan xususiyatlarning kombinatsiyasidan foydalangan holda normal va g‘ayritabiiy xatti-harakatlarni aniqlashga o‘rgatiladi.

Kalit so‘zlar: *Sun’iy intellekt (AI), mashinali o‘qitish (ML), Optik ishlash monitoringi (OPM), raqamli signalni qayta ishlash (DSP), OSM arxitekturasi, Transport-SDN.*

ABSTRACT

In this research paper, we proposed the application of machine learning (ML) models to ensure optical network security and systematize work processes. ML models can be used on different algorithms and different datasets for optical network security. These models are trained to identify normal and abnormal behavior using a combination of predefined features.

Keywords: *Artificial Intelligence (AI), Machine Learning (ML), Optical Performance Monitoring (OPM), Digital Signal Processing (DSP), OSM Architecture, Transport-SDN.*

KIRISH

Doimiy rivojlanib borayotgan aqlli raqibga dosh berish uchun kiberxavfsizlik sohasi barcha tarmoq domenlari va ilovalari bo‘ylab Sun’iy intellekt (AI) tomonidan boshqariladigan avtomatlashtirishdan samarali natijalarga erishmoqda [1]. Umuman olganda, sun’iy intellektga asoslangan yondashuvlar kognitiv va avtomatlashtirilgan optik tarmoqni boshqarish va nazorat qilish bilan bog‘liq turli xil vazifalarda keng qo‘llanilmoqda.

Jismoniy darajadagi hujumlar turli xil hujum texnikalarida keskin farq qiluvchi optik signal parametrlarida murakkab o‘zgarishlarga olib kelganligi sababli, aniq analitik modellarni yoki qarshi choralarni qo‘llash uchun chegaralarni belgilash jismoniy darajadagi xavfsizlikni kognitiv boshqarish uchun yaroqliligi isbotlanmagan. Buning o‘rniga, ushbu jarayonni qo‘llab-quvvatlash uchun ML texnikasining kuchli salohiyati bir necha yo‘llar bilan namoyish etilgan. [2] da, optik spektrni tekshirish orqali ruxsatsiz optik signallarning mavjudligini aniqlash uchun qo‘llab-quvvatlovchi vektor mashinalari (SVMs) qo‘llanildi. Yuqori quvvatli jamming hujumlarini aniqlash uchun sun’iy neyron tarmoqlari (ANN)ga asoslangan yondashuv [3] da taklif qilingan. Ichida va tarmoqdan tashqarida tiqilib qolish, shuningdek, polarizatsion shifrlash hujumlarini bog‘lanish darajasida amalga oshirish orqali olingan eksperimental ma’lumotlardan foydalangan holda hujumlarni aniqlash va identifikatsiyalash [4] da turli nazorat ostida o‘qitish (SL) texnikasi yordamida amalga oshirildi. SL dan tashqari, [5] dagi ish hujumlarni tarmoq darajasida aniqlash uchun Unsupervised Learning (UL) va Semi-Supervised Learning (SSL) usullarini qo‘llashga qaratilgan. UL va SSL ilgari to‘plangan, Optik ishlash monitoringi (OPM) yorlig‘i bo‘yicha o‘rganilmaganligi sababli, ular hatto yangi, ilgari ko‘rilmagan hujum usullarini ham aniqlay oladi va bu ularni rivojlanayotgan tahdid landshaftiga qarshi kurashishda munosib raqibga aylantiradi.

MUHOKAMA

Tarmoq xavfsizligini boshqarish umuman uchta asosiy ustunga tayanadi, 1-rasmda ko‘rsatilgan. Xatarlarni boshqarish turli xil hujum vektorlarining ko‘p qirrali ta’sirini aks ettiruvchi va ushbu ta’sirlarning tarmoqqa ta’sirini o‘lchaydigan aniq xavf modellarini ishlab chiqishni o‘z ichiga oladi.

1-rasm. Tarmoq xavfsizligini boshqarish siklining yuqori darajadagi ko‘rinishi.

Bunday modellarga asoslanib, ushbu ustun shuningdek, hujumlarga duchor bo‘lgan tarmoq sirtini minimallashtirishni ham o‘z ichiga oladi. Ma’lum va paydo bo‘layotgan xavfsizlik tahdidlariga nisbatan ma’lum darajadagi mustahkamlikni ta’minlash xavf modellarini va xavfsizlikni kuchaytiruvchi tarmoq dizaynini doimiy yangilashni talab qiladi. Optik tarmoqqa maqsadli tolali kesish hujumlarining ta’sirini o‘lchash uchun namunalarni [6] da, statik, davriy va dinamik trafik ostida hujumdan xabardor optik tarmoqni rejalashtirish misollarini [7], [8] va [9] da ko‘rish mumkin.

Hujumni aniqlash tarmoq faoliyatining va indikativ ma’lumotlarini to‘plashni, ularni chuqur tahlil qilishni va hujumni aniqlash va buzilish joyini aniqlash uchun kuzatilgan tendensiyalarni har xil turdagi xavfsizlik buzilishlariga to‘g‘ri bog‘lashni o‘z ichiga oladi. Bu hujumning mumkin bo‘lgan kirish nuqtalari va turli xil hujum usullarining imzolari, ya’ni ularning alohida OPM parametrlariga ta’siri haqida batafsil ma’lumotni talab qiladi. Qimmatbaho OPM uskunasining siyrak joylashuvi tufayli optik tarmoqlarda OPM ma’lumotlarini hamma joyda, real vaqt rejimida yig‘ish qiyin. Biroq, raqamli signalni qayta ishlash (DSP) funktsiyalariga ega bo‘lgan so‘nggi avlod kogerent qabul qiluvchilar bu muammoni har bir ulanish manzilida (masalan, daqiqada) OPM ma’lumotlar to‘plamini to‘plash va uni NMS standartlashtirilgan interfeyslariga ta’sir qilish orqali bu muammoni yengillashtiradi.

Xavfsizlik diagnostikasi asosida ***hodisaga javob berish*** ustuni ta’sirlangan tarmoq elementlari va ulanishlarini tiklashni, buzilishni zararsizlantirishni va shunga o‘xshash hujumlarning kelajakda yuzaga kelishiga chidamliligini oshirish uchun tarmoq moslashuvini o‘z ichiga oladi. Tarmoq moslashuvi, masalan, hujumdan xabardor zahiraviy resurslarni oldindan rejalashtirish, tez chastota sakrash, ulanish yo‘nalishini o‘zgartirish, modulyatsiya formati va spektrni qayta tayinlash (masalan, [10] da tavsiflangan protsedura yordamida) yoki davriy faol resurslarni qayta taqsimlash.

Optik tarmoq boshqaruvi arxitekturasida xavfsizlik kafolati

Optik xavfsizlik kafolati (OSA) kognitiv tarmoqlarni boshqarish tizimi (C-NMS) rivojlanayotgan arxitekturalar doirasida hal qilinishi kerak [4]. Transport-SDN

kontseptsiyasining paydo bo‘lishi va ochiq manbali ko‘p sotuvchili tarmoq kontrollerlarining rivojlanishi optik tarmoqlarni boshqarish nuqtai nazarini chuqur o‘zgartirdi [31]. Yangi C-NMS paradigmasining muhim jihatlarini quyidagicha umumlashtirish mumkin.

- Tarmoqni boshqarish va nazorat qilish - bu bir nechta tarmoq kontrollerlari (har biri ma’lum bir tarmoq qatlami yoki operatsion domeniga bag‘ishlangan) va bir yoki bir nechta arxitektirlar tomonidan tuzilgan qatlamlararo keng qamrovli arxitektura;

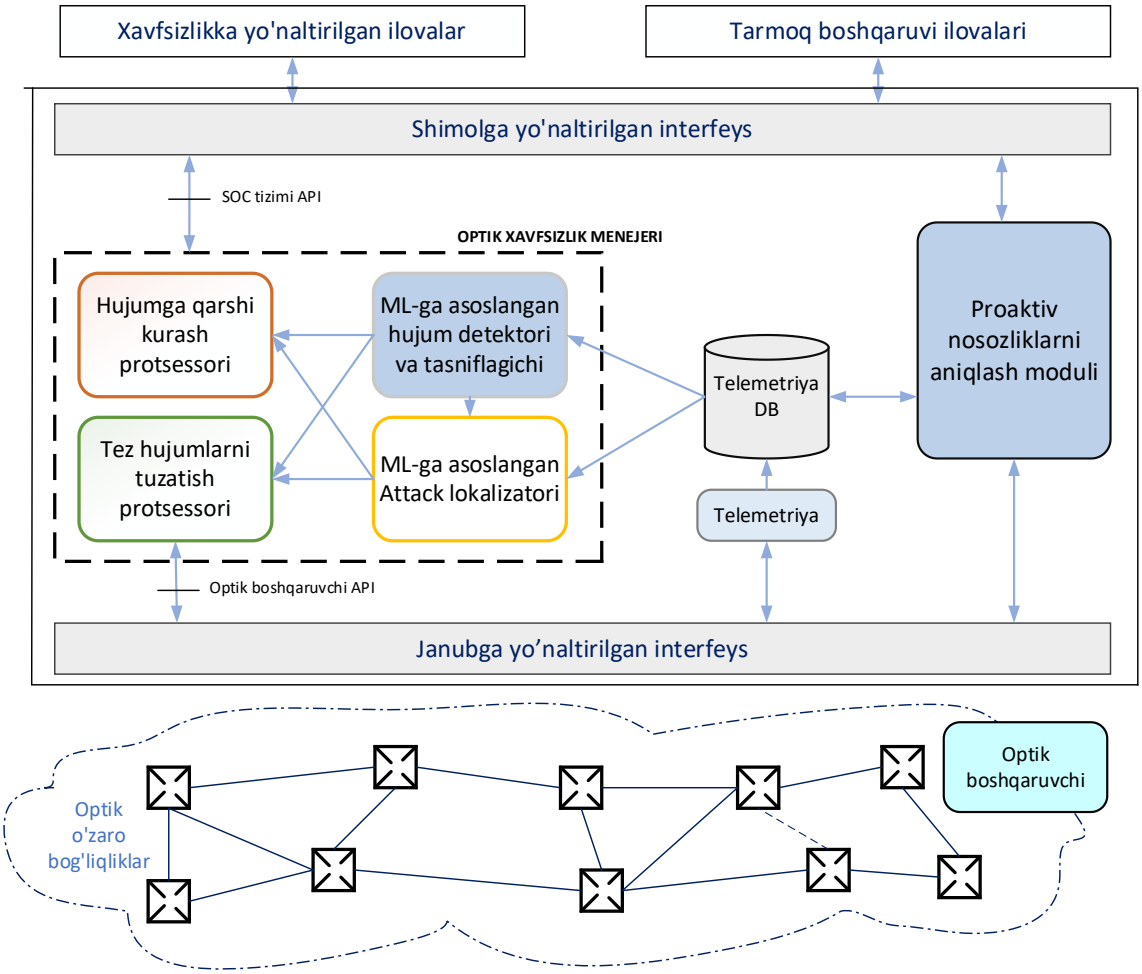
- Har bir kontroller yuqori qatlam orkestratori tomonidan talab bo‘yicha o‘rnatiladigan oxirigacha xizmatlarni taqdim etadi;

- Standart amaliy dasturlash interfeyslari (API) foydalanuvchilar va tashqi tizimlar (masalan, Data Center Hypervisors) uchun tarmoq xizmatlaridan oson foydalanish imkonini beradi;

- Analitika tarmoq holatini samarali diagnostika qilish va har qanday nosozlik uchun tegishli chora-tadbirlarni amalga oshirish uchun keng qo‘llaniladi.

Xavfsizlik kafolati optik transport xizmatlarining yangi muhim xususiyati bo‘lib, u hozirgi Transport-SDN boshqaruv arxitekturasida muammosiz joriy etilishi kerak. Optik xavfsizlikni boshqarishning yana bir muhim jihati uning ko‘plab yirik kompaniyalarda butun tarmoq va axborot texnologiyalari xavfsizligi uchun mas’ul bo‘lgan SOC jarayonlariga qattiq integratsiyalashuvi zaruratidir. Boshqacha qilib aytganda, OSA tarmoq va xavfsizlikni boshqarish o‘rtasidagi chegarada yotadi. Shu sababli, Tarmoq Operatsion Markazi (NOC) va SOC o‘rtasidagi har qanday ziddiyat yoki rollar va mas’uliyatlarning superpozitsiyasiga mutlaqo yo‘l qo‘ymaslik kerak. Shu sabablarga ko‘ra, optik tarmoqlarda xavfsizlikni ta’minlashni joriy etish quyidagi muhim funktsiyalar va talablarga ega bo‘lgan ahamiyatsiz vazifadir:

- telemetriya (agar optik boshqaruvchi tomonidan ta’minlanmagan bo‘lsa);
- hujumni aniqlash va tasniflash;
- xizmatning uzilish vaqtini minimallashtirish uchun tezkor hujum reaktsiyasi;
- hujumning lokalizatsiyasi;
- doimiy hujumni bartaraf etish.



2-rasm. Kognitiv Transport dasturiy ta'minoti aniqlangan tarmoq (T-SDN) boshqaruvchisi doirasida tavsiya etilgan OSM arxitekturasi.

2-rasmda ko‘rsatilgan OSM arxitekturasi barcha optik xavfsizlik funktsiyalarini o‘z ichiga oladi va printsipial jihatdan har qanday optik kontroller bilan mos keladi. Shuningdek, u SOC tizimlariga mos interfeysni taqdim etadi.

OSM *telemetriya* va *telemetriya ma'lumotlar bazasi (DB)* bloklaridan iborat bo‘lib, ular kogerent qabul qiluvchi OPM ma'lumotlarini (va, ehtimol, boshqa tegishli tarmoq holati ma'lumotlarini) oladi va saqlaydi [15]. OPM ma'lumotlari ikkita ML moduli tomonidan qo‘llaniladi: ***hujumlarni aniqlovchi, tasniflagich*** va funktsiyalari o‘z-o‘zidan tushunarli bo‘lgan ***hujum lokalizatori.*** ML bloklari tomonidan bildirilgan hujum holati haqidagi ma'lumotlarga asoslanib, tezkor hujumga javob berish ***Tezkor hujumlarni aniqlash protsessori*** tomonidan belgilanadi**.** Ushbu blokning maqsadi xizmatning to‘xtab qolish vaqtini minimallashtirishga qaratilgan tezkor qarshi chora tanlashdir (masalan, oddiy trafik yo‘nalishini o‘zgartirish orqali). Qarshi chorani amalga oshirish tegishli API orqali optik kontrollerga so‘raladi. To‘liq hujumga qarshi vositaning vazifasi boshqacha bo‘lib, uni boshqa blok bajaradi: ***Hujumga qarshi***

kurash protsessori. Ushbu blok hujumni tuzatishning yakuniy strategiyasini ishlab chiqish uchun hujum tasnifi va lokalizatsiya ma'lumotlaridan foydalanadi. Optik qatlam hujumlarining tabiati tarmoq infratuzilmasi firibgarlik yo'li bilan o'zgartirilganligini anglatadi va shuning uchun hujumni trafikni himoya qilish yoki yo'nalishni o'zgartirish kabi elementar tarmoq funktsiyalari bilan doimiy ravishda tuzatish mumkin emas. Ushbu aralashuv hujum ostidagi havolani izolyatsiya qilish uchun optik kuchaytirgichlarni o'chirish, so'ngra maydondagi hujum qurilmalarini jismoniy olib tashlash kabi tezkor harakatlardan iborat bo'lishi mumkin [11].

Hujumni aniqlash uchun aniqlik choralari

Hujumni aniqlash usullarining aniqligi to'rtta asosiy ko'rsatkich bo'yicha o'lchanishi mumkin:

- Haqiqiy salbiy stavka [$T_n \in (0,1)$]: normal namunalar sifatida aniqlangan normal ish holati namunalarining qismi;
- Noto'g'ri ijobiy ko'rsatkich [$F_p \in (0,1)$]: hujum sifatida aniqlangan normal ish holati namunalarining qismi;
- Haqiqiy ijobiy ko'rsatkich [$T_p \in (0,1)$]: hujum sifatida aniqlangan hujum namunalarining qismi;
- Noto'g'ri salbiy ko'rsatkich [$F_n \in (0,1)$]: oddiy namunalar sifatida aniqlangan hujum namunalarining qismi.

Haqiqiy manfiy va noto'g'ri musbat stavkalar yig'indisi bittaga teng bo'lishi kerak, ya'ni $T_n + F_p = 1$, xuddi haqiqiy ijobiy va noto'g'ri manfiy stavkalar yig'indisi, ya'ni $T_p + F_n = 1$ bo'lishi kerak.

$$P = \frac{T_p}{T_p + F_p} \quad (1)$$

$$R = \frac{T_p}{T_p + F_n} \quad (2)$$

$$F1 = 2\frac{p \times R}{p + R} \quad (3)$$

Bizning ishimiz doirasida normal ish holati namunalari soni hujumga qaraganda ancha ko'p bo'lishi kutilmoqda, bu juda zaif ma'lumotlar to'plamini sozlaydi. Bunday hollarda modelning aniqligini umumlashtirish uchun *aniqlik* va *eslab qolishdan* foydalanish mumkin. Tenglik (1) da aniqlangan aniqlik [$P \in (0, 1)$] baholanayotgan modelning noto'g'ri musbatlarga nisbatan sezgirligini o'lchaydi.

XULOSA

Esda tuting [$R \in (0, 1)$] Tenglik (2) da aniqlangan, baholanayotgan modelning noto'g'ri negativlarga nisbatan sezgirligini o'lchaydi. Nihoyat, Tenglik (3) da aniqlangan f1 ball [$F1 \in (0, 1)$] aniqlik va eslab qolishning garmonik o'rtacha qiymatini

hisoblab, bitta metrikada modelning aniqligini umumlashtiradi. f1 balli eng samarali hisoblanadi, chunki yaxshi natijaga erishish uchun model yuqori aniqlik va yuqori eslab qolishga erishishi kerak.

Xulosa qilib aytganda, optik tarmoq xavfsizligi bugungi kunda juda muhim masala bo‘lib, ML texnologiyasi bu sohada sezilarli ta’sir ko‘rsatadi. Optik tarmoq xavfsizligi uchun ML modellari optik tarmoq trafigidagi potentsial tahdidlarni aniqlash uchun ishlatiladi va optik tarmoq xavfsizligini ta’minlashga yordam beradi.

FOYDALANILGAN ADABIYOTLAR

[1] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” IEEE Access 8, 23817–23837 (2020). DOI: 10.1109/ACCESS.2020.2968045.

[2] Y. Li, N. Hua, Y. Yu, Q. Luo, and X. Zheng, “Light source and trail recognition via optical spectrum feature analysis for optical network security,” IEEE Commun. Lett. 22, 982–985 (2018).

[3] M. Bensalem, S. K. Singh, and A. Jukan, “On detecting and preventing jamming attacks with machine learning in optical networks,” in 2019 IEEE Global Communications Conference (GLOBECOM), (2019), pp. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9013238.

[4] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, “Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks,” IEEE/OSA J. Light. Technol. 37, 4173–4182 (2019). DOI: 10.1109/JLT.2019.2923558.

[5] M. Furdek, C. Natalino, F. Lipp, D. Hock, A. D. Giglio, and M. Schiano, “Machine learning for optical network security monitoring: A practical perspective,” J. Light. Technol. 38, 2860–2871 (2020). DOI: 10.1109/JLT.2020.2987032.

[6] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek, “Infrastructure upgrade framework for content delivery networks robust to targeted attacks,” Opt. Switch. Netw. 31, 202 – 210 (2019). DOI: 10.1016/j.osn.2018.10.006.

[7] N. Skorin-Kapov, J. Chen, and L. Wosinska, “A new approach to optical networks security: Attack-aware routing and wavelength assignment,” IEEE Trans. Netw. 18, 750–760 (2010). DOI:10.1109/TNET.2009.2031555.

[8] K. Manousakis, P. Kollios, and G. Ellinas, “Multi-period attack-aware optical network planning under demand uncertainty,” in Optical Fiber and Wireless Communications, R. Roka, ed. (2017). DOI: 10.5772/in- techopen.68491.

[9] J. Zhu, B. Zhao, and Z. Zhu, “Leveraging game theory to achieve efficient attack-aware service provisioning in EONs,” IEEE/OSA J. Ligh. Techn. 35, 1785–1796 (2017). DOI: 10.1109/JLT.2017.2656892.

[10] N. Sambo, K. Christodoulopoulos, N. Argyris, P. Giardina, C. Delezoide, D. Roccato, A. Percelsi, R. Morro, A. Sgambelluri, A. Kretsis, G. Kanakis, G. Bernini, E. Varvarigos, and P. Castoldi, “Field trial: Demonstrating automatic reconfiguration of optical networks based on finite state machine,” J. Light. Technol. 37, 4090–4097 (2019). DOI: 10.1109/JLT.2019.2922841.

[11] Adhikari, M., Choi, B.-G., & Kim, J.-H. (2020). Detection of threats in optical network security using machine learning algorithms. Journal of Optical Communications, 41(2), 131–137. https://doi.org/10.1515/joc-2020-0062.