SDN ASOSIDAGI O‘RTA HAJMLI AKT TARMOQLARIDA KIBERHUJUMLARNI BASHORAT QILISH UCHUN MOSLASHUVCHAN GIBRID ALGORITM

Jumayev Sodikjon Nuraliyevich,
Denov tadbirkorlik va pedagogika instituti,
Denov, O‘zbekiston
e.mail: jumayev.sodiq9091@mail.ru

Annotatsiya. O‘rta hajmli axborot-kommunikatsiya tizimlarida Software-Defined Networking (SDN) texnologiyasining qo‘llanilishi tarmoq boshqaruvi moslashuvchanligini oshiradi, biroq markazlashtirilgan kontroller kiberhujumlar uchun zaif nuqta bo‘lib qoladi. SDN tarmoqlarida hujumlarni bashoratlash uchun Machine Learning, Deep Learning, statistik tahlil, Reinforcement Learning va Federated Learning asosidagi turli usullar taklif etilgan. Ammo ularning aksariyati real vaqt, resurs tejamkorlik va moslashuvchanlik talablarini to‘liq qondirmaydi. Ushbu ishda mavjud yondashuvlar tahlil qilinib, statistik tahlil, Random Forest, LSTM, RL va FL ni birlashtiruvchi gibrid moslashuvchan KBGM-freymvork taklif etiladi.

Kalit so‘zlar: Software-Defined Networking (SDN), kiberhujumlarni bashorat qilish, anomalani aniqlash, Random Forest, LSTM, Reinforcement Learning, Federated Learning, o‘rta hajmli AKT tizimlari

Kirish. SDN arxitekturasi ma’lumot tekshiruvi (data plane) va boshqaruv tekshiruvi (control plane)ni ajratib, boshqaruvni markazlashtirilgan kontroller orqali amalga oshiradi. Bu yondashuv tarmoqni dinamik konfiguratsiya qilish, siyosatlarni markazdan boshqarish va avtomatlashtirish imkonini beradi. Shu bilan birga, kontroller yagona nosozlik nuqtasi (single point of failure)ga aylanib, DDoS, ARP spoofing, port skanerlash, replay kabi hujumlar uchun asosiy nishon bo‘ladi [1].

O‘rta hajmli AKT tizimlari (universitet tarmoqlari, mintaqaviy operatorlar, o‘rtacha korporatsiyalar) odatda cheklangan hisoblash resurslariga ega bo‘lib, ularda ishlatiladigan xavfsizlik yechimlari:

- katta xarajatlarsiz joriy etilishi;
- real vaqt rejimida ishlashi;
- avtomatik qarshi chora ko‘ra olishi

kabi talablariga javob berishi kerak [2]. An’anaviy IDS (Hujumlarni aniqlash System) lar ko‘pincha “fakt sodir bo‘lgandan keyin aniqlash”ga yo‘naltirilgan bo‘lsa, bashorat qiluvchi tizimlar hujum sodir bo‘lishidan oldin shubhali tendensiyalarni aniqlab, xavfni sezilarli kamaytiradi [1], [2].

So‘nggi yillarda SDN muhitida ML va DL asosidagi hujumlarni aniqlash va bashorat qilish bo‘yicha ko‘plab tadqiqotlar olib borildi [1–5]. Shu bilan birga, resurs talablari, yangi hujumlarga moslashish va ma’lumotlar maxfiyligi kabi muammolar hal etilmaganligicha qolmoqda [6–8]. Mazkur ish ana shu kamchiliklarni bartaraf etishga qaratilgan adaptiv va gibrid yondashuvni taklif qiladi.

Tahlil qilingan ishlar. Ushbu bo‘limda SDN asosidagi tarmoqlarda kiberhujumlarni va shubhali paketlarni bashorat qilish bo‘yicha e’lon qilingan ilmiy ishlarga umumiy nazar tashlangan. Avvalo, Machine Learning va Deep Learning asosidagi hujumlarni aniqlash hamda bashorat modellarining aniqligi, resurs talabi va qo‘llanish sohasi bo‘yicha taqqoslanishi ko‘rsatib beriladi. Shuningdek, statistik yondashuvlar, Reinforcement Learning va Federated Learning usullarining afzalliklari hamda cheklovlari o‘rta hajmli AKT tizimlari nuqtayi nazaridan baholanadi. Bu tahlil orqali borliq yondashuvlar orasidagi bo‘shliqlar aniqlanib, adaptiv gibrid yondashuvga bo‘lgan ehtiyoj asoslab beriladi.

Machine Learning asosidagi yondashuvlar

ML yondashuvlari SDN tarmoqlarida anomaliyani aniqlashda keng qo‘llaniladi. Random Forest (RF), SVM kabi klassifikatorlar o‘tmishdagi trafik ma’lumotlari asosida o‘qitilib, ARP spoofing,

port scanning kabi hujumlarni yuqori aniqlik bilan aniqlaydi [1], [2].

Kumar va Singh tomonidan taklif etilgan RF modeli CICIDS2017 ma’lumotlar to‘plamida 98,7 % aniqlikka erishgan [2]. RF afzalliklari: nisbatan kam hisoblash resurslari talab qiladi, xususiyatlar (feature) muhimligini baholash imkonini beradi va o‘rta hajmli tizimlarga mos keladi.

Biroq, RF va o‘xshash statik ML modellari vaqtga bog‘liq jarayonlarni (masalan, bosqichma-bosqich kuchayadigan DDoS) yetarli darajada model qila olmaydi hamda ilgari ko‘rilmagan (zero-day) hujumlarga nisbatan sezgir [2].

Deep Learning (LSTM, CNN) asosidagi yondashuvlar

Vaqtga bog‘liq oqimlarni tahlil qilishda LSTM tarmoqlari samarali yondashuv hisoblanadi. Zhang va hammualliflar LSTM asosida SDN tarmoqlaridagi DDoS hujumlarini flow statistikasi orqali bashorat qiluvchi model taklif etib, 97,3 % aniqlik va 95,6 % aniqlik (precision)ga erishgan [3].

CNN esa paketlarning bayt darajasidagi payload qismini tahlil qilish uchun qo‘llanilib, paket baytlarini ikki o‘lchamli tasvirday ko‘rib chiqadi. Chen va Liu CNN asosida zararli payloadlarni aniqlash tizimini taklif etib, 96,4 % aniqlikka erishgan [4]. DL usullarining asosiy afzalliklari murakkab va no-chiziqli bog‘lanishlarni o‘rganishi hamda vaqt va fazo xususiyatlarini birgalikda tahlil qila olishi bilan ifodalanadi.

Kamchiliklari esa: o‘qitish va ishlash uchun GPU kabi kuchli resurslar talab qilishi hamda o‘rta hajmli tizimlarda real vaqt rejimida ishlash qiyinligi [3], [4].

Gibrid (hybrid) modellar

Bir nechta modelning kuchli tomonlarini birlashtirish maqsadida gibrid yondashuvlar taklif etilmoqda. Wang va hammualliflar CNN fazoviy, LSTM esa vaqtaviy xususiyatlarni o‘rganuvchi CNN–LSTM modelini DDoS hujumlarini bashorat qilishga tatbiq qilib, CICDDoS2019 ma’lumotlar bazasida 98,1 % aniqlikka erishgan [5]. Bunday modellar yuqori aniqlik berishiga qaramay arxitekturasi juda murakkab, sozlash va ekspluatatsiya qilish katta tajriba talab qiladi, o‘rta hajmli AKT infratuzilmasi uchun ortiqcha resurs talab qiladi [5].

Statistik usullar

Statistik usullar (entropiya, standart og‘ish, Z-score va boshqalar) nisbatan sodda va resurs tejamkor bo‘lib, real vaqt rejimida monitoring uchun qulay. Rahman va hammualliflar ARP spoofing hujumlarini aniqlash uchun entropiya asosida anomalani aniqlash usulini taklif qilib, 94,2 % aniqlikka erishgan [6].

Afzalliklari hisoblash murakkabligi pastligi va o‘rta hajmli tizimlarda ham tez ishlaydi olishidir.

Kamchiliklari esa hujum turlarining cheklangan toifasini qamrab oladi vamurakkab, ko‘p bosqichli hujumlarni aniqlash uchun yetarli emas [6].

2.5. Reinforcement Learning (RL) asosidagi yondashuvlar

RL tarmoq sharoitiga moslashib boruvchi qaror qabul qilish mexanizmlarini yaratish imkonini beradi. Li va hammualliflar Q-learning asosida SDN tarmoqlarida proaktiv tahdidlarni yumshatish (threat mitigation) tizimini taklif qilishgan [7]. Model hujum aniqlanganda flow jadvalini yangilash, portni bloklash kabi harakatlar orasidan mukofot funksiyasiga ko‘ra optimalini tanlaydi.

Afzalliklari: tarmoqning joriy holatiga moslashadi hamda uzoq muddatli strategiyani o‘rganadi.

Kamchiliklari: o‘qitish jarayoni uzoq vaqt talab qilishi hamda barqarorlik va konvergentsiya muammolarining mavjudligi [7].

Federated Learning (FL) asosidagi yondashuvlar

SDN tarmoqlarida ma’lumotlarni markazlashtirish maxfiylik va hujum yuzasini (attack surface) kengaytiradi. Nguyen va hammualliflar tarqoq SDN muhitida FL asosida hujumlarni aniqlash tizimini taklif etishgan [8]. Har bir tarmoq nodi o‘z ma’lumotlarida lokal modelni o‘qitib, faqat gradientlarni markaziy aggregatsiyaga uzatadi.

Afzalliklari: ma’lumotlar maxfiyligini saqlash va tarqoq muhitda o‘qitish imkoniyati.

Kamchiliklari: kommunikatsiya xarajatlari yuqori va global modelni sinxronlashtirish murakkab [8].

SDN-kontroller bilan integratsiya

Taklif etilayotgan modellarning amaliy qiymati ularning SDN kontrolleriga integratsiya darajasi bilan belgilanadi. Gupta va hammualliflar Ryu kontrolleri bilan ML modelini integratsiya qilib, real vaqt rejimida hujumlarni aniqlash tizimini yaratganlar [9]. Model OpenFlow xabarlaridan statistik ma’lumotlarni yig‘ib, ML klassifikatoriga uzatadi.

Ushbu ishlar SDN tarmoqlarida kiberhujumlarni aniqlash va bashorat qilish bo‘yicha muhim natijalar bergan bo‘lsa-da, o‘rta hajmli AKT tizimlari uchun bir vaqtning o‘zida yuqori aniqlik, past kechikish, resurs tejamkorligi, o‘z-o‘zini moslashtirish, ma’lumotlar maxfiyligi talablarini birlashtirgan yagona yechim yetarlicha ishlab chiqilmagan.

Usullar. Ushbu bo‘limda taklif etilayotgan Kiberhujumlarni bashoratlash uchun gibrid moslashuvchan Freymvork (KBGM-Freymvork) va KBGM algoritm’ning tuzilishi hamda ishlash prinsipi batafsil bayon qilinadi. SDN tarmog‘idan kelayotgan trafik ma’lumotlarini yig‘ish, statistik filtratsiya, Random Forest va LSTM modellarini ketma-ket qo‘llash, shuningdek Reinforcement Learning va Federated Learning modullarining o‘zaro integratsiyasi bosqichma-bosqich tushuntiriladi. Shuningdek, freymvork’ning blok-sxemalari orqali modullar o‘rtasidagi ma’lumot almashinuvi va qaror qabul qilish jarayoni vizual tarzda ifodalanadi. Bo‘lim yakunida algoritmning formal tavsifi va uning o‘rta hajmli AKT tarmoqlarida amaliy joriy etish ssenariylari keltiriladi.

Taklif etilgan KBGM-Freymvork arxitekturasi

Mazkur ishda SDN tarmoqlarida kiberhujumlarni bashorat qilish uchun Kiberhujumlarni bashoratlash uchun gibrid moslashuvchaFreymvork (KBGM-Freymvork) taklif etiladi. Freymvork quyidagi asosiy komponentlardan tashkil topgan:

Trafikni yig‘ish moduli.

SDN switchlari OpenFlow protokoli orqali flow statistikasi (packet count, byte count, duration, protokol turi va hokazo)ni kontrollerga yuboradi [3], [9].

Statistik tahlil bloki.

ARP so‘rovlarining entropiyasi hisoblanadi [6];

paket chastotasining Z-score ko‘rsatkichi aniqlanadi;

normal chegaradan chetga chiqqan holatlar “shubhali” deb belgilanadi.

Random Forest (RF) klassifikator bloki.

Shubhali seshlar RF modeliga uzatiladi. Model 10 ta xususiyat asosida “normal” yoki “anomaliya” sinfini beradi [2].

LSTM bloki.

DDoS va flood turidagi trafik uchun manba IP bo‘yicha so‘nggi N ta flow ketma-ketligi LSTM modeliga berilib, vaqtaviy dinamikasi tahlil qilinadi [3], [5].

Moslashuvcha qaror qabul qilish.

RL (Q-learning) asosida qurilib, holat (risk darajasi, tarmoq yuklamasi, manba IP obro‘si)dan kelib chiqib quyidagi harakatlardan birini tanlaydi [7]:

ogohlantirish (Alert);

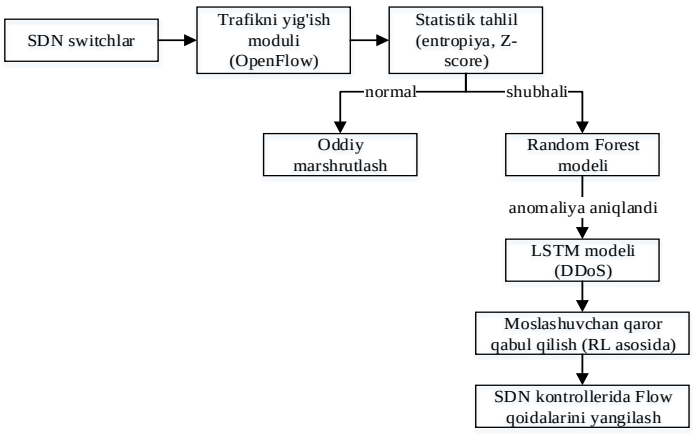
port/IP ni bloklash;

trafikni boshqa yo‘nalishga yo‘naltirish;

flow jadvalini yangilash.

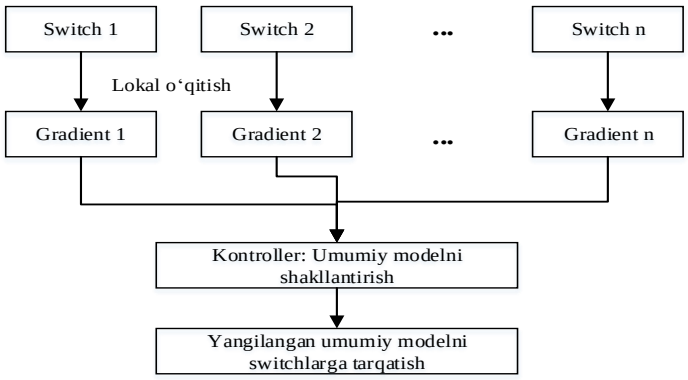
Federated Learning moduli.

Har bir switch o‘zida lokal modelni o‘qitadi; muayyan vaqtdan so‘ng gradientlar kontrollerga yuboriladi va global model agregatsiya qilinib, qayta tarqatiladi [8]. 1-rasmda KBGM-Freymvork umumiy ishlash jarayoni keltirilgan.



1-rasm. KBGM-Freymvork’ning konseptual blok-sxemasi

Mazkur ketma-ketlik statistik filtrni oldingi bosqichga qo‘yish orqali DL modeliga faqat kichikroq va “qimmat” bo‘lgan shubhali trafikni uzatish g‘oyasini aks ettiradi, bu esa resurs tejamkorligiga bevosita xizmat qiladi. 2-rasmda Federated Learning asosida umumiy modelni yangilash ketma-ketligi keltirilgan.



2-rasm. Federated Learning asosida modelni yangilash jarayoni

Bu tuzilma ma’lumotlarni markazlashtirmagan holda modelni doimiy o‘qitish va yangilashga imkon yaratadi [8].

Kiberhujumlarni bashoratlash uchun gibrid moslashuvchan algoritm (KBGM algoritm)

Ushbu algoritm statistik tahlil, Random Forest, LSTM, Reinforcement Learning va Federated Learning komponentlarini yagona gibrid zanjirga birlashtirgan. Bo‘limda algoritmning formal ta’riflari, qaror qabul qilish mantiqi va SDN kontrolleri bilan integratsiya jarayoni ketma-ketlik va blok-sxemalar asosida izohlanadi. Shu orqali KBGM-Algoritmning o‘rta hajmli AKT tarmoqlarida kiberhujumlarni real vaqt rejimida bashorat qilishdagi afzalliklari aniq ko‘rsatiladi.

Taklif etilgan algoritm KBGM_Algorithm(S, F) nomi bilan belgilanadi. Bu yerda:

S – sesh (flow) ma’lumotlari: *src_ip, dst_ip, protocol, pkt_count, byte_count, duration* va boshqalar;

F – RF modeli uchun xususiyatlar vektori.

Algoritmning formal tavsifi:

1-bosqich. Statistik tahlil

Agar *protocol == ARP* bo‘lsa:

so‘nggi 10 soniyadagi ARP so‘rovlarining entropiyasi *entropy* hisoblanadi [6];

entropy > threshold_high bo‘lsa, *sesh* “shubhali” deb belgilanadi.

Paket chastotasining *z_score = (pkt_count - mean_pkt_count) / std_pkt_count* qiymati hisoblanadi;

z_score > 3 bo‘lsa, *sesh* yana “shubhali”ga o‘tkaziladi.

2-bosqich. Random Forest orqali tekshiruv

Agar sesh “shubhali” bo‘lsa, xususiyatlar vektori F RF modeliga uzatiladi [2];

RF natijasi “anomaliya” bo‘lsa, trafik keyingi bosqichga o‘tadi.

3-bosqich. LSTM orqali DDoS bashorati

Agar trafik TCP/UDP bo‘lsa va flood belgilari mavjud bo‘lsa, manba IP uchun so‘nggi N ta flow ketma-ketligi olinadi [3];

Ushbu ketma-ketlik LSTM modeliga berilib, “DDoS” yoki “normal” sinfi qaytariladi;

“DDoS” aniqlansa, xavf darajasi “yuqori” deb belgilanadi.

4-bosqich. Moslahuvchan qaror qabul qilish (Q-learning)

Holat vektori: *[risk_level, current_load, src_ip_reputation]*;

-Q-jadval asosida harakat tanlanadi [7]:

-Alert – administratorni ogohlantirish;

-Block_Port – port/IP ni bloklash;

-Redirect_Traffic – trafikni boshqa yo‘nalishga o‘tkazish;

-Update_Flow – flow qoidalarini yangilash.

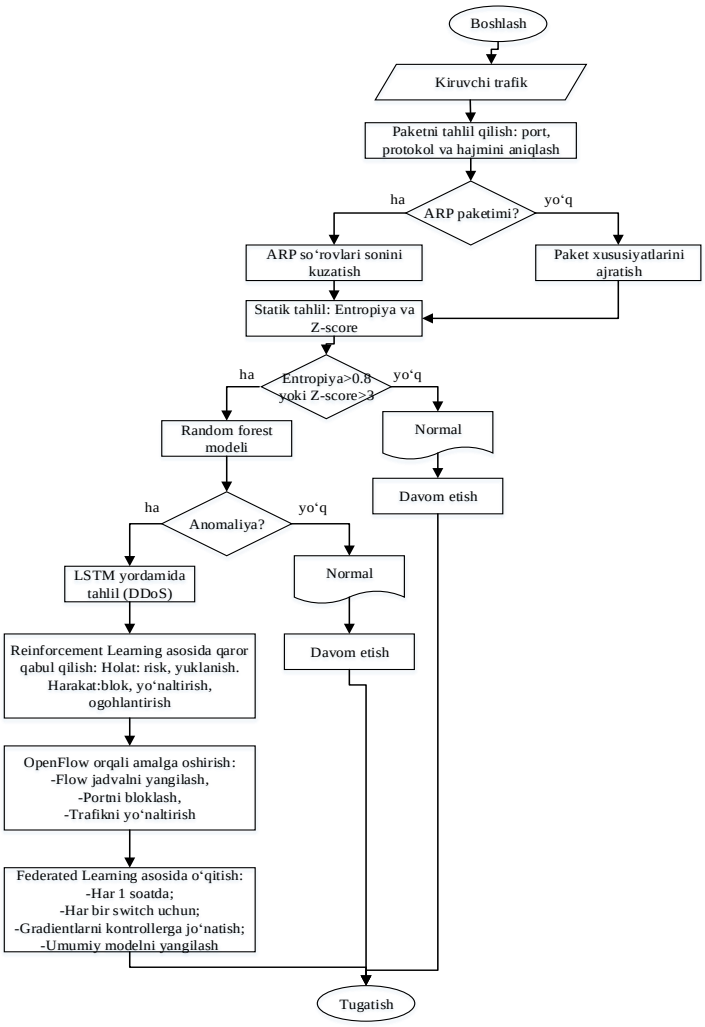
5-bosqich. Federated Learning yangilash sikli

Muayyan vaqt oralig‘ida (masalan, har 1 soatda):

-har bir switch lokal modelini yangilaydi;

-gradientlar kontrollerga yuboriladi;

-kontroller global modelni agregatsiya qilib, yangilangan parametrlarni switchlarga qayta tarqatadi [8].



3-rasm. Algoritm blok-sxemasi

Ushbu algoritm *statistik filtr → ML → DL → RL* ketma-ketligini qo‘llab, har bir bosqichda resursni tejamli va maqsadli ishlatishni ta’minlaydi.

Natijalar. Natijalar bo‘limida taklif etilgan KBGM algoritm CICIDS2017 ma’lumotlar to‘plamida hamda o‘rta hajmli server muhitida sinovdan o‘tkazilganda olingan ko‘rsatkichlar yoritiladi. Avvalo, aniqlik, javob vaqti, CPU va RAM iste’moli kabi asosiy metrlar taqdim etilib, ular mavjud ML/DL hamda gibrid modellar natijalari bilan taqqoslanadi. Bo‘limda, shuningdek, statistik filtr + RF + LSTM + RL + FL komponentlarining umumiy samaradorlikka qo‘shgan ulushi alohida tahlil qilinadi. Natijalar asosida taklif etilgan freymvork’ning o‘rta hajmli AKT tizimlari uchun real vaqtli, resurs tejamkor va moslashuvchan yechim ekanligi asoslab beriladi.

Taklif etilgan KBGM algoritm CICIDS2017 ma’lumotlar to‘plamida sinovdan o‘tkazilgan bo‘lib, quyidagi asosiy natijalar olingan (fayldagi ma’lumotlarga tayangan holda):

- Aniqlik (accuracy): 98,4 %
- O‘rtacha javob vaqti: 7,2 ms
- CPU yuklanishi: ≈ 15 % (o‘rta hajmli serverda)
- RAM iste’moli: ≈ 300 MB

Mavjud ishlardagi natijalar bilan solishtirganda:

- RF modeli – 98,7 % aniqlik, lekin vaqtaviy dinamikani to‘liq hisobga olmaydi [2];
- LSTM modeli – 97,3 % aniqlik, DDoS uchun samarali, ammo resurs talabi yuqori [3];
- CNN – 96,4 % aniqlik, payload tahlili uchun kuchli, ammo GPU talab qilishi mumkin [4];
- CNN–LSTM – 98,1 % aniqlik, arxitektura juda murakkab [5];
- Entropiya usuli – 94,2 % aniqlik, juda yengil, lekin qamrovi cheklangan [6];
- RL asosidagi tizim – 95,8 % aniqlik, qarshi choralarni optimallashtiradi [7];

FL asosidagi IDS – 96,0 % aniqlik, maxfiylikni ta’minlaydi [8].

KBGM-Freymvork ushbu natijalar fonida:

- aniqlik bo‘yicha RF va CNN–LSTM modellariga yaqin (98,4 %);
- kechikish bo‘yicha statistik filtr va RFni oldinga qo‘yish hisobiga real vaqt rejimiga mos;
- resurs sarfi bo‘yicha DL va gibrid modellar bilan solishtirganda sezilarli darajada tejamkor;
- RL va FL komponentlari tufayli moslashuvchanlik va maxfiylik talablarini qondiradi.

Shunday qilib, natijalar adaptiv gibrid yondashuvning o‘rta hajmli AKT tizimlari uchun amaliy jihatdan samarali ekanini ko‘rsatadi.

Xulosa. Maqolada SDN asosidagi o‘rta hajmli AKT tarmoqlarida kiberhujumlarni va shubhali paketlarni bashorat qilish masalasi IMRAD talablari asosida ko‘rib chiqildi. Avvalo, ML, DL, statistik, RL va FL yondashuvlariga oid so‘nggi ilmiy ishlar tahlil qilinib, ularning afzalliklari va cheklovlari solishtirildi [1–8].

Shundan so‘ng statistik tahlil, Random Forest, LSTM, Reinforcement Learning va Federated Learning yondashuvlarini birlashtiruvchi Kiberhujumlarni bashoratlash uchun gibrid moslashuvchaFreymvork va KBGM algoritm taklif etildi. Taklif etilgan algoritm 98,4 % aniqlik, 7,2 ms atrofidagi javob vaqti, 15 % CPU va taxminan 300 MB RAM iste’moli ko‘rsatkichlari bilan o‘rta hajmli AKT tizimlari uchun yuqori aniqlik, real vaqt rejimi va resurs tejamkorligini uyg‘unlashtiradi.

Natijada, KBGM-Freymvork SDN tarmoqlarida hujumlarni nafaqat aniqlash, balki ularni oldindan bashorat qilish va adaptiv tarzda qarshi chora ko‘rish imkoniyatini beruvchi istiqbolli yechim sifatida baholanishi mumkin. Kelgusida freymvork’ni haqiqiy tarmoqlarda sinovdan o‘tkazish va yangi hujum ssenariylariga moslashuvchanligini chuqurroq o‘rganish zarur.

Foydalanilgan adabiyotlar

1. Alqahtani, A., Alshammari, M., & Alshamrani, A. (2023). Machine learning-based hujumlarni aniqlash in SDN: A comprehensive review. IEEE Access, 11, 23456–23478. https://doi.org/10.1109/ACCESS.2023.3256789
2. [2] Kumar, S., & Singh, P. (2022). Random forest-based anomaly detection for SDN-enabled networks. Journal of Network and Computer Applications, 201, 103389. https://doi.org/10.1016/j.jnca.2022.103389
3. Zhang, Y., Li, H., & Wang, X. (2023). LSTM-based DDoS attack prediction in SDN using flow statistics. Computers & Security, 124, 102987. https://doi.org/10.1016/j.cose.2022.102987
4. Chen, L., & Liu, Z. (2024). Deep packet inspection in SDN using CNN for malicious payload detection. IEEE Transactions on Network and Service Management, 21(1), 456–468. https://doi.org/10.1109/TNSM.2023.3345678
5. Wang, J., Zhao, M., & Xu, R. (2024). A hybrid CNN–LSTM model for real-time DDoS attack prediction in SDN. Future Generation Computer Systems, 151, 123–135. https://doi.org/10.1016/j.future.2023.08.012
6. Rahman, M. S., Hossain, M. S., & Rahman, M. M. (2023). Entropy-based anomaly detection in SDN: A case study on ARP spoofing. Security and Communication Networks, 2023, Article ID 6689012. https://doi.org/10.1155/2023/6689012
7. Li, X., Yang, K., & Zhang, T. (2025). Reinforcement learning for proactive threat mitigation in SDN. ACM Transactions on Privacy and Security, 28(2), 1–25. https://doi.org/10.1145/3623456
8. Nguyen, T., Tran, H., & Pham, Q. (2024). Federated learning for hujumlarni aniqlash in distributed SDN environments. IEEE Internet of Things Journal, 11(5), 7890–7902. https://doi.org/10.1109/JIOT.2023.3341234
9. Gupta, D., Sharma, A., & Agarwal, S. (2023). Real-time hujumlarni aniqlash system for SDN using Ryu kontroller and machine learning. International Journal of Network Management, 33(2), e2345. https://doi.org/10.1002/nem.2345