SHAP TEXNOLOGIYASI ASOSIDA DDOS HUJUMLARINI ANIQLASH MODELINI OPTIMALLASHTIRISH

Raxmatov Furqat Abdirazzoqovich[1], Toshtemirov Muxammadi Shokir o‘g‘li[2]

[1]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti “Kompyuter tizimlari” kafedrasi dotsenti

[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti 2-kurs magistranti

[1]e-mail: furkat.rahmatov@gmail.com, [2]e-mail:muxammadi0799@gmail.com

Annotatsiya: Ushbu maqolada SHAP (SHapley Additive exPlanations) texnologiyasi yordamida DDoS hujumlarini aniqlash modelini optimallashtirish usuli taqdim etiladi. Uchta xalqaro benchmark dataset (CIC-DDoS2019, UNSW-NB15, Network Intrusion) ustida o'tkazilgan tajribalar shuni ko'rsatdiki, SHAP asosida tanlangan 10 ta belgi bilan o'qitilgan model to'liq belgilar to'plamiga nisbatan CIC-DDoS2019 da +0.82%, UNSW-NB15 da +2.04% yuqori aniqlik ko'rsatdi. Belgilar soni esa 74–87% ga qisqardi. Natijalar SHAP texnologiyasining DDoS aniqlash tizimlarida samarali feature selection usuli sifatida qo'llanilishi mumkinligini isbotlaydi.

Kalit so'zlar: DDoS hujumlari, SHAP, feature selection, Random Forest, tarmoq xavfsizligi, model optimallashtirish, explainable AI.

Abstract: This paper presents a method for optimizing a DDoS attack detection model using SHAP (Shapley Additive exPlanations) technology. Experiments conducted on three international benchmark datasets (CIC-DDoS2019, UNSW-NB15, and Network Intrusion) demonstrated that a model trained with 10 SHAP-selected features achieved higher accuracy compared to the full feature set — by +0.82% on CIC-DDoS2019 and +2.04% on UNSW-NB15. The number of features was reduced by 74–87%. The results confirm that SHAP technology can be effectively applied as a feature selection method in DDoS detection systems.

Keywords: DDoS attacks, SHAP, feature selection, Random Forest, network security, model optimization, explainable AI

1. KIRISH

DDoS (Distributed Denial of Service) hujumlari zamonaviy tarmoq xavfsizligining eng dolzarb muammolaridan biri bo'lib, ulardan yetkazilgan global zarar yildan yilga ortib bormoqda. Mashinali o'qitish algoritmlariga asoslangan aniqlash tizimlari keng qo'llanilmoqda, ammo ko'plab

tadqiqotlarda modellar yuzlab belgilar (features) asosida o'qitiladi. Bu esa hisoblash resurslarini ko'p talab qiladi va real vaqt tizimlarida samaradorlikni pasaytiradi [1].

Ushbu muammoni hal qilish uchun SHAP (SHapley Additive exPlanations) texnologiyasi asosida belgilarni tanlash va modelni optimallashtirish usuli taklif etiladi. SHAP — har bir belgining model qaroriga qanday ta'sir ko'rsatishini miqdoriy baholaydigan matematik asbob bo'lib, u o'yin nazariyasidagi Shapley qiymatlari asosida ishlaydi [2]. Ushbu yondashuv nafaqat modelning interpretatsiyasini ta'minlaydi, balki ortiqcha va shovqinli belgilarni samarali filtrlash imkonini beradi.

2. METODOLOGIYA

Tadqiqotda uchta xalqaro benchmark dataset ishlatilgan: CIC-DDoS2019 (431,371 qator, 18 turdagi DDoS hujumlari), UNSW-NB15 (257,673 qator, 7 turdagi tarmoq hujumlari) va Network Intrusion/CIC-IDS2017 (844,000+ qator, DDoS va normal traffic). Ma'lumotlar tozalanib, har bir klass uchun muvozanatlashtirilgan namuna olindi.

Metodologiya ikki bosqichdan iborat. Birinchi bosqichda Random Forest modeli to'liq belgilar to'plami bilan o'qitildi. Ikkinchi bosqichda SHAP TreeExplainer yordamida har bir belgining o'rtacha mutlaq SHAP qiymati hisoblanib, eng yuqori 10 ta belgi ajratib olindi. So'ngra model faqat shu 10 ta belgi bilan qayta o'qitildi va natijalar taqqoslandi (1-jadval).

5-jadval.

SHAP optimallashtirish natijalari

Dataset	To'liq belgilar	Top 10 belgilar	Qisqarish	Accuracy farqi
CIC-DDoS2019	77	10	87.0%	**+0.82%**
UNSW-NB15	39	10	74.4%	**+2.04%**
Network Intrusion	77	10	87.0%	0.00%

3. SHAP TAHLILI — TOP 10 BELGILAR

SHAP tahlili natijasida uchta dataset uchun aniqlangan eng muhim belgilar 2-jadvalda keltirilgan. Tadqiqot shuni ko'rsatdiki, Packet_Length_Mean, Fwd_Packet_Length_Min va Fwd_Packet_Length_Max belgilari bir necha datasetda takroran muhim sifatida aniqlandi — bu ularning DDoS hujumlarini aniqlashda universal ahamiyatga ega ekanligini tasdiqlaydi.

6-jadval.

SHAP asosida top 10 belgilar taqqoslamasi

O'rin	CIC-DDoS2019	UNSW-NB15	Network Intrusion
1	Flow_Bytes/s	sbytes	Init_Win_bytes_backward
2	Packet_Length_Min	smean	min_seg_size_forward
3	Fwd_Packet_Length_Min	ct_dst_src_ltm	Packet_Length_Mean
4	Avg_Fwd_Segment_Size	ct_srv_dst	Fwd_Packet_Length_Max
5	Avg_Packet_Size	sttl	Bwd_Packet_Length_Std
6	Packet_Length_Max	ct_srv_src	Average_Packet_Size
7	Packet_Length_Mean	dbytes	Packet_Length_Std
8	Fwd_Packet_Length_Max	dmean	Max_Packet_Length
9	Fwd_Packet_Length_Mean	sloss	Fwd_Packet_Length_Min
10	Fwd_Seg_Size_Min	ct_src_ltm	Packet_Length_Variance

Eng muhim belgilarning tarmoq xavfsizligi nuqtai nazaridan talqini: Flow_Bytes/s — DDoS hujumi paytida keskin oshadi, chunki tajovuzkorlar serverga katta hajmdagi paketlar yuboradi; Packet_Length_Min — UDP Flood va SYN Flood hujumlarida juda kichik paketlar ko'p miqdorda yuboriladi; Init_Win_bytes_backward — SYN Flood hujumida server ko'plab yarimta TCP ulanishlarini ochishga majbur bo'ladi va bu belgi anormal qiymatlarga ega bo'ladi.

4. NATIJALAR VA MUHOKAMA

Tajriba natijalari SHAP texnologiyasining samaradorligini aniq ko'rsatdi. CIC-DDoS2019 datasetida belgilar soni 77 tadan 10 taga qisqartirildi (87.0% qisqarish), biroq accuracy 91.49% dan 92.31% ga oshdi (+0.82%). UNSW-NB15 datasetida belgilar 39 tadan 10 taga tushirildi (74.4% qisqarish), accuracy esa 74.98% dan 77.02% ga ko'tarildi (+2.04%). Network Intrusion datasetida accuracy 99.80% darajasida o'zgarishsiz qoldi.

Bu natijaning ilmiy izohi quyidagicha: to'liq belgilar to'plamida korrelyatsiyalangan va shovqinli belgilar mavjud bo'lib, ular modelning qaror qabul qilish jarayoniga salbiy ta'sir ko'rsatadi. SHAP yordamida bu ortiqcha belgilar olib tashlanishi modeldagi shovqin ta'sirini kamaytiradi va umumlashtirish qobiliyatini oshiradi. Shuningdek, belgilar sonining 74–87% ga qisqarishi hisoblash resurslarini tejash va real vaqt tizimlarida tezkor ishlash imkoniyatini beradi.

5-fold cross-validation natijalari (RF: 91.65% ± 0.12%, 99.89% ± 0.04%) modelning barqarorligini tasdiqlaydi. ROC-AUC ko'rsatkichlari 0.9477 dan 1.0000 gacha bo'lgan oraliqda qayd etildi, bu esa modelning yuqori ajratish qobiliyatiga ega ekanligini bildiradi.

XULOSA

Ushbu tadqiqotda SHAP texnologiyasi asosida DDoS hujumlarini aniqlash modelini optimallashtirish usuli taklif etildi va uchta xalqaro benchmark datasetida eksperimental sinovdan o'tkazildi. Asosiy xulosalar quyidagilardan iborat:

1. SHAP asosida tanlangan 10 ta belgi bilan o'qitilgan model to'liq belgilar to'plamidan yuqori yoki teng aniqlikni ko'rsatdi — CIC-DDoS2019 da +0.82%, UNSW-NB15 da +2.04% oshdi;

2. Belgilar soni 74–87% ga qisqartirilishi hisoblash samaradorligini sezilarli oshiradi va real vaqt DDoS aniqlash tizimlarida qo'llash imkoniyatini kengaytiradi;

3. Packet_Length_Mean, Fwd_Packet_Length_Min va Fwd_Packet_Length_Max belgilari uchta xil datasetda ham muhim sifatida aniqlandi — bu ularning DDoS aniqlashda universal ahamiyatga ega ekanligini isbotlaydi;

4. SHAP texnologiyasi mashinali o'qitish modellarini interpretatsiya qilish bilan birga, samarali feature selection usuli sifatida ham qo'llanilishi mumkin.

FOYDALANILGAN ADABIYOTLAR

[1]. Waqas M. va boshq., "A Systematic Review of DDoS Attack Detection Techniques". – IEEE Access, 2022, 10, 45891–45924 b.

[2]. Lundberg S.M., Lee S.I., "A Unified Approach to Interpreting Model Predictions". – NeurIPS, 2017, 4765–4774 b.

[3]. Sharafaldin I., Lashkari A.H., Ghorbani A.A., "Toward Generating a New Intrusion Detection Dataset". – ICISSP, 2018, 108–116 b.

[4]. Moustafa N., Slay J., "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems". – MilCIS, 2015 b.

[5]. Anand V. va boshq., "Network Intrusion Detection Using SHAP-based Explainable AI". – IEEE ICCCNT, 2021, 1–6 b.

[6]. Farnaaz N., Jabbar M.A., "Random Forest Modeling for Network Intrusion Detection System". – Procedia Computer Science, 2016, 89, 213–217 b.