OQIM-ASOSIDAGI HUJUMLARNI ANIQLASH TIZIMLARIDA YORLIQ SIZISHINI NAZORATLI ZOND USULIDA MIQDORIY O‘LCHASH

Allanov Orif Menglimuratovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
allanov@tuit.uz
Maxkamova Dildora Begaliyevna
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
d.maxkamova@tuit.uz

Annotatsiya. *Tezisda NetFlow-benchmark to‘plamlarida port identifikatorlarining hujum yorlig‘i o‘rnini bosuvchi sifatida ishlashini miqdoriy isbotlovchi nazoratli sizish-zond usuli bayon etiladi. Usul besh qadamdan iborat bo‘lib, talqin mutlaq ko‘rsatkichga emas, same va cross-dataset rejimlar orasidagi farqga tayanadi. NF-BoT-IoT-v2 da faqat portlarda o‘qitilgan zond same-dataset rejimda PR-AUC = 1,0000, cross-dataset rejimda esa 0,0613 (ROC-AUC 0,998 → 0,615) ko‘rsatdi. Bu farq sizish hajmining bevosita o‘lchovidir. Natija port raqamlarini uch semantik toifagacha soddalashtirish va baholashni majburiy cross-dataset rejimda o‘tkazish qarorlarini eksperimental asoslaydi.*

Kalit so‘zlar: *tarmoq hujumlarini aniqlash, NetFlow, yorliq sizishi, shortcut, nazoratli zond, cross-dataset baholash.*

Abstract. *The paper presents a supervised leakage-probe method that quantitatively demonstrates that port identifiers in NetFlow benchmark datasets act as a substitute for the attack label. The method consists of five steps, and its interpretation relies not on the absolute score but on the gap between the same-dataset and cross-dataset regimes. On NF-BoT-IoT-v2, a probe trained on ports only achieved PR-AUC = 1.0000 in the same-dataset regime and 0.0613 in the cross-dataset regime (ROC-AUC 0.998 → 0.615). This gap is a direct measure of the extent of leakage. The result provides experimental grounds for reducing port numbers to three semantic categories and for making cross-dataset evaluation mandatory.*

Keywords: *intrusion detection, NetFlow, label leakage, shortcut learning, supervised probe, cross-dataset evaluation.*

Аннотация. *В тезисах описан метод контролируемого зонда утечки, количественно доказывающий, что идентификаторы портов в эталонных наборах NetFlow выступают заменителем метки атаки. Метод состоит из пяти шагов, а интерпретация опирается не на абсолютный показатель, а на разницу между внутринаборным (same-dataset) и межнаборным (cross-dataset) режимами. На NF-BoT-IoT-v2 зонд, обученный только на портах, показал PR-AUC = 1,0000 во внутринаборном режиме и 0,0613 в межнаборном (ROC-AUC 0,998 → 0,615). Эта разница является прямой мерой объёма утечки. Результат экспериментально обосновывает решения об упрощении номеров портов до трёх семантических категорий и об обязательном проведении межнаборной оценки.*

Ключевые слова: *обнаружение вторжений, NetFlow, утечка меток, shortcut-обучение, контролируемый зонд, межнаборная оценка.*

Oqim asosidagi tarmoq hujumlarini aniqlash tizimlari (NIDS) bo‘yicha e’lon qilinayotgan natijalar, odatda, bitta benchmark to‘plamning trening va test qismlarida olinadi va ko‘pincha 0,99 dan yuqori ko‘rsatkichlarga yetadi. Biroq xavfsizlik sohasida mashinali o‘qitishning tizimli xatolarini tahlil qilgan ishlar [1], [2] bunday raqamlarning muhim qismi usul sifatidan emas, baholash nuqsonidan - ma’lumot sizishidan - kelib chiqishini ko‘rsatadi. Sizishning oqim darajasidagi eng xavfli ko‘rinishi - identifikator sizishi bo‘lib, IP-manzillar va port raqamlari to‘plam generatsiyasi jarayonida hujum sinfi bilan sun’iy bog‘lanib qoladi. Model esa hujumning mohiyatini emas, shu bog‘lanishni yodlaydi. L. Dhooge va hammualliflari metama’lumot xususiyatlarining modelni “ifloslantiruvchi” ta’sirini eksperimental ko‘rsatgan [3]; Z. Gu va hammualliflari esa Anomal-E kabi self-supervised graf modellarida target encoding orqali yorliqqa bog‘liqlik yuzaga kelishini aniqlagan [4].

Shu bilan birga, adabiyotda sizish asosan sifat tavsifi darajasida qoladi. Qaysi xususiyat guruhi qanchalik sizayotganini o‘lchash vositasi yo‘q. Mazkur maqolada nazoratli sizish zond usulini bayon etilgan va uni NF-v2 oilasidagi ikki to‘plamda [5]–[7] port kanaliga tatbiq etish haqida ma’lumotlar yoritilgan.

*Nazoratli zond usuli.*Zond deb ataylab faqat tekshirilayotgan xususiyat guruhida o‘qitilgan nazoratli klassifikatorga aytiladi. Usulning mantig‘i oddiy bo‘lib, unga ko‘ra agar xususiyat guruhi hujum sinfi haqidagi universal qonuniyatni kodlasa, u boshqa to‘plamda ham ishlaydi. Agar u to‘plamga xos identifikatorni kodlasa, boshqa to‘plamda zaiflik qiladi. Demak, same va cross-dataset rejimlar orasidagi farq sizish hajmining o‘lchovidir. Protsedura besh qadamdan iborat:

1) sizish kanalini ajratish - xususiyatlar to‘plami faqat shubhali guruh bilan cheklanadi;

2) shu cheklangan to‘plamda nazoratli klassifikatorni o‘qitish - nazoratli rejim ataylab tanlanadi, chunki u kanaldan olinishi mumkin bo‘lgan maksimal axborotni, ya’ni eng yomon holatni namoyon qiladi;

3) same-dataset baholash - yuqori natija kanalda sinf haqida axborot borligini ko‘rsatadi, biroq bu hali sizish isboti emas;

4) cross-dataset baholash - natija keskin pasayib ketsa, kanal to‘plamga xos identifikatorni kodlagan bo‘lib chiqadi;

5) nazorat guruhi bilan taqqoslash - xuddi shu protsedura statistik xususiyatlarda (bayt, paket, davomiylik va h.k.) takrorlanib, kuzatilgan effektning aynan tekshirilayotgan kanalga xosligi tekshiriladi.

Zond natijalarini o‘qish qoidasi 1-jadvalda umumlashtirilgan. Hal qiluvchi axborot ikki rejimning kombinatsiyasida va nazorat guruhining xatti-harakatida yotadi.

1-jadval

Zond natijalarini talqin qilish matritsasi

Same-dataset	Cross-dataset	Nazorat guruhi (stats)	Xulosa va chora
yuqori	yuqori	istalgan	kanal universal qonuniyatni kodlaydi - saqlanadi
yuqori	keskin tushib ketish	Tushib ketmaydi yoki moslashuv bilan tiklanadi	identifikator sizishi - kanal soddalashtiriladi yoki chiqariladi
yuqori	Tushib ketish, ROC < 0,5	ham tushib ketdi, ballar teskarilangan	domen siljishi - kanal saqlanadi, taqsimot moslashuvi talab etiladi
past	past	istalgan	kanal sinf haqida axborot tashimaydi - zond xulosasiz

Ikki uslubiy qoida usulni boshqa tadqiqotlarda qayta qo‘llanuvchan qiladi. Birinchisi - talqin qoidasi. Unda zondning mutlaq ko‘rsatkichi emas, rejimlar orasidagi farq o‘qiladi. Shu bois klassifikator tanlovidagi mo’tadil o‘zgarishlar xulosani o‘zgartirmaydi, chunki ular ikkala rejimga bir xilda ta’sir qiladi. Ikkinchisi - klassifikator mezoni. U yetarlicha kuchli, ammo giperparametr sozlashsiz barqaror bo‘lishi kerak, aks holda zond kanal xossasini emas, sozlash mahoratini o‘lchay boshlaydi. Statistik xususiyatlar ham cross-rejimda zaiflashsa, bu sizish emas,

taqsimot siljishi belgisidir — ikki hodisa turli mexanizmga ega va turli chora talab qiladi.

Eksperiment va natijalar. Zondlar M. Sarhan va hammualliflarining yagona NetFlow xususiyatlar to‘plamidagi [5] ikki to‘plamda tatbiq etildi. Korporativ trafikni aks ettiruvchi NF-UNSW-NB15-v2 [6] (hujum ulushi ≈ 3,8 %) va IoT-muhitni aks ettiruvchi NF-BoT-IoT-v2 [7] (hujum ulushi ≈ 99,6 %). Har bir to‘plamda port- va stats-zondlar same- va cross-dataset rejimlarda baholandi; port kanali target-encoded ko‘rinishda, ya’ni aynan sizish manbai bo‘lgan kodlash bilan berildi. Natijalar 2-jadvalda keltirilgan.

2-jadval

Port va stats zondlarning same va cross-dataset natijalari

Trening to‘plami	Xususiyat	Same PR-AUC	Same ROC-AUC	Cross PR-AUC	Cross ROC-AUC
NF-UNSW-NB15-v2	port	0,3640	0,8581	0,9995	0,9564
NF-UNSW-NB15-v2	stats	0,8735	0,9864	0,9807	0,1041
NF-BoT-IoT-v2	port	1,0000	0,9980	0,0613	0,6146
NF-BoT-IoT-v2	stats	0,9998	0,9700	0,0270	0,3545

Uchinchi qator sizishning eng yorqin isbotidir. NF-BoT-IoT-v2 da faqat port xususiyatlariga tayangan zond same-dataset rejimda ideal natija beradi (PR-AUC = 1,0000; ROC-AUC = 0,998). Sun’iy generatsiyada portlar sinf bilan deyarli funksional bog‘langan. Xuddi shu zond NF-UNSW-NB15-v2 ga o‘tkazilganda PR-AUC 0,0613 ga, ROC-AUC esa 0,998 dan 0,615 ga - tasodifiy taxminga yaqin darajaga tushib ketadi. PR-AUC qiymatlari mos ravishda 0,996 va 0,038 bazaviy ulushlarda turgani bois, rejimlararo taqqoslash bazaga bog‘liq bo‘lmagan ROC-AUC da o‘tkaziladi va ikkala metrika ham bir xil xulosani beradi. Demak, port raqamlari hujum sinfining mohiyatini emas, to‘plamga xos identifikatorni kodlaydi va yorliq o‘rnini bosuvchi sifatida ishlaydi.

Qolgan qatorlar usulning diagnostik quvvatini ko‘rsatadi. Birinchi qatorda cross rejimda PR-AUC ning 0,9995 gacha “yaxshilanishi” chalg‘ituvchi. Bu maqsad testning 99,6 % hujumdan iboratligi oqibati. ROC-AUC 0,956 esa shortcutning bir yo‘nalishda tasodifan ko‘chganini bildiradi, teskari yo‘nalishdagi qulash (0,0613) esa unga tayanib bo‘lmasligini isbotlaydi. Ikkinchi va to‘rtinchi qatorlar cross rejimda ROC-AUC 0,104 va 0,355 - ya’ni 0,5 dan past natija beradi. Ballar yo‘nalishi teskarilangan, bir to‘plamda normallikni bildirgan statistik

naqshlar boshqasida hujumga xos chiqadi. Bu sizish emas, sof domen siljishi. U xususiyatni taqiqlash bilan emas, taqsimot moslashuvi bilan bartaraf etiladi. Shu tariqa ikki hodisa aynan nazorat guruhi tufayli ajratiladi.

Statistik ishonchlilik nuqtai nazaridan kuzatilgan farqlar shu qadar yirikki (PR-AUC 1,000 → 0,061; ROC-AUC 0,998 → 0,615), rasmiy ahamiyatlilik testiga ehtiyoj qolmaydi. Effekt hajmi har qanday oqilona ishonch oralig‘idan tashqarida. Farqlar chegaraga yaqin bo‘ladigan zondlar uchun besh urug‘ natijalari ustida bootstrap-ishonch oraliqlarini qurish va faqat oraliqlar kesishmaganda farqni tan olish tartibi tavsiya etiladi.

Natijaning uslubiy oqibatlari. Zond natijasi uchta tekshiriladigan qarorni bevosita asoslaydi. Birinchisi - xususiyat siyosati: port raqamlari IANA taqsimotiga mos uch semantik toifagacha (tizim portlari, ro‘yxatdan o‘tgan portlar, dinamik portlar) soddalashtiriladi. Ikki toifa xizmat semantikasini yo‘qotadi, toifalarni ko‘paytirish esa asta-sekin to‘liq port raqamiga yaqinlashib, isbotlangan sizishni qaytaradi. Uchlik - semantik foyda va sizish xavfi o‘rtasidagi tekshirilgan muvozanat nuqtasi. Ikkinchisi - baholash rejimi: same-dataset ko‘rsatkich yakka o‘zi umumlashtirilmaydi, zero-shot cross-dataset rejim majburiy hisoblanadi. Uchinchisi - kengaytiriluvchanlik: eksporterlar yangi maydon qo‘shganda, sinf bilan potentsial qattiq bog‘langan har qanday diskret maydon avval xuddi shu zonddan o‘tkaziladi va natijaga ko‘ra soddalashtiriladi yoki saqlanadi.

Usul kanalga ham, to‘plamga ham bog‘liq emas, shu bois sizish tipologiyasining boshqa turlariga kengaytirish mumkin. Temporal-zond: bitta to‘plam ichida vaqt bo‘yicha kesilgan va tasodifiy bo‘linishlarda bir xil klassifikator o‘qitilib, tasodifiy bo‘linishning ustunligi vaqt sizishining o‘lchovi sifatida o‘qiladi - bu TESSERACT [2] talabining miqdoriy ko‘rinishidir. Guruh-zond: oqimlar sessiya yoki epizod bo‘yicha guruhlanib, guruhlar kesishmaydigan bo‘linish tasodifiy bilan solishtiriladi. Har ikki holda talqin qoidasi o‘zgarmaydi va mutlaq son emas, farq o‘qiladi.

Zond usuli yagona sizish nazorati baholash protokolining tarkibiy qismi sifatida rasmiylashtirildi. Protokolning sakkiz bandli tekshiruv ro‘yxatidagi ikki band bevosita zond natijasiga tayanadi, ya’ni portlar semantik toifalargacha soddalashtirilgan yoki ular uchun sizish-zondi o‘tkazilgan bo‘lishi hamda baholash kamida ikkita mustaqil to‘plamda, majburiy zero-shot cross-dataset rejimni o‘z ichiga olgan holda bajarilishi talab etiladi. Qolgan olti band (IP-manzillarni chiqarib tashlash, yorliqqa tayanuvchi kodlash va chegara tanlovini trening jarayonidan chiqarish, masshtablash parametrlarini faqat trening to‘plamida hisoblash, PR-AUC qiymatini bazaviy hujum ulushi bilan birga e’lon qilish, natijalarni besh urug‘

bo‘yicha o‘rtachalash va hisoblash muhitini hujjatlashtirish) zond bilan birgalikda yopiq nazorat tizimini hosil qiladi. Protokolning muhim xossasi shundaki, zond uning har bir taqiqini eksperimental tekshirish imkonini beradi, xususan, IP-manzillar bo‘yicha o‘tkazilgan xuddi shu zond kutilgan keskin pasayishni ko‘rsatmadi shu sababli bu natija ochiq qayd etilib, IP-manzillarni chiqarish taqiqi ehtiyot chorasi maqomida saqlandi. Demak, zond usuli nafaqat sizishni isbotlashga, balki biror taqiq eksperimental tasdiqlanmagan holatlarni ham ochiq ko‘rsatishga xizmat qiladi.

Xulosa

Taklif etilgan nazoratli zond usuli yorliq sizishini taxmindan o‘lchovga aylantiradi. Port kanali bo‘yicha bir korpus ichida 0,998, boshqasida 0,615 (PR-AUC 1,0000 → 0,0613). Usulning uchta xossasi uni mustaqil uslubiy hissa qiladi. Bular: nazorat guruhi orqali sizish va domen siljishini ajratish; mutlaq ko‘rsatkich emas, rejimlar farqini o‘qish qoidasi; ixtiyoriy diskret maydonga qayta qo‘llanuvchanlik. Zond o‘zi modelni baholamaydi, balki u xususiyat siyosatining har bir taqiqini e’tiqod darajasidan eksperimental hukm darajasiga ko‘taradi.

Foydalanilgan adabiyotlar

1. Arp D., Quiring E., Pendlebury F., Warnecke A., Pierazzi F., Wressnegger C., Cavallaro L., Rieck K. Dos and don’ts of machine learning in computer security // 31st USENIX Security Symposium. — 2022. — P. 3971–3988.

2. Pendlebury F., Pierazzi F., Jordaney R., Kinder J., Cavallaro L. TESSERACT: Eliminating experimental bias in malware classification across space and time // 28th USENIX Security Symposium. — 2019. — P. 729–746.

3. D’hooge L., Verkerken M., Volckaert B., Wauters T., De Turck F. Establishing the contaminating effect of metadata feature inclusion in machine-learned network intrusion detection models // Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). — 2022.

4. Gu Z., Lopez D.T., Alrahis L., Sinanoglu O. Always be Pre-Training: Representation learning for network intrusion detection with GNNs // arXiv:2402.18986. — 2024.

5. Sarhan M., Layeghy S., Portmann M. Towards a standard feature set for network intrusion detection system datasets // Mobile Networks and Applications. — 2022. — Vol. 27. — P. 357–370.

6. Moustafa N., Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems // Military Communications and Information Systems Conference (MilCIS). — Canberra, 2015. — P. 1–6.

7. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset // Future Generation Computer Systems. — 2019. — Vol. 100. — P. 779–796.

8. Maxkamova D.B. Tarmoq oqimini tahlil qilish asosida hujumlarni aniqlash usullari // “Raqamli transformatsiya: telekommunikatsiya, sun’iy intellekt va innovatsion texnologiyalar istiqbollari” Respublika ilmiy-amaliy anjumani materiallari. — Samarqand, 2026. — I tom. — B. 380–383.