ISNN 3030-3907

2026/3
VOLUME 2

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/3 VOLUME 2

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

TARMOQ TRAFIGINI SINFLASHTIRISH METODLARI VA ALGORITMLARI: AN'ANAVIY VA STATISTIK YONDASHUVLAR TAQQOSIY TAHLILI

Tojiyeva Feruza Qobiljon qizi
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari,
Infokommunikatsiya injinering kafedrasi
doktoranti
E-mail: 11feruza@gmail.com

Annotatsiya. Ushbu maqolada tarmoq trafigini sinflashtirishning uch asosiy yo'nalishi portga asoslangan, paket mazmuniga asoslangan hamda statistik yondashuvlar tizimli ravishda taqqosiy tahlil qilinadi. Portga asoslangan usullar sodda va tezkor bo'lsa-da, dinamik portlar va tunnellash sharoitida yetarli darajada barqaror ishlamaydi. DPI yondashuvi ma'lum protokollar uchun yuqori aniqlikni ta'minlaydi, biroq zamonaviy shifrlash texnologiyalari sharoitida paketning foydali yuklama qismiga to'liq kira olmasligi hamda hisoblash murakkabligining yuqoriligi bilan cheklanadi. Statistik oqimga asoslangan metodlar esa paket sarlavhasi atributlari va oqim ko'rsatkichlariga tayangan holda shifrlangan trafikda ham samarali natija beradi. Shu bilan birga, ushbu yondashuvda informativ xususiyatlarni tanlash hamda "yangi sinf" muammosi alohida yondashuvlarni talab etadi. Tadqiqot natijalari statistik yondashuvlarning trafikni erta bosqichda aniqlashda yuqori samaradorlikka ega ekanini ko'rsatdi.

Kalit so'zlar: tarmoq trafigi, sinflashtirish, NetFlow, shifrlangan trafik, oqim-statistika, erta tasniflash

Аннотация. В данной статье систематически проводится сравнительный анализ трёх основных направлений классификации сетевого трафика: на основе портов, на основе содержимого пакетов и статистических подходов. Методы, основанные на портах, отличаются простотой и высокой скоростью работы, однако в условиях динамических портов и туннелирования не обеспечивают достаточной устойчивости. Подход DPI обеспечивает высокую точность для определённых протоколов, но ограничен невозможностью полного доступа к полезной нагрузке пакета в условиях современных технологий шифрования, а также высокой вычислительной сложностью. Методы, основанные на статистике потоков, опираются на атрибуты заголовков пакетов и характеристики потоков, что позволяет эффективно работать даже с зашифрованным трафиком. Вместе с тем в рамках данного подхода задачи выбора информативных признаков и выявления «нового класса» требуют отдельных решений. Результаты

ISSN 3030-3907

исследования показали, что статистические подходы обладают высокой эффективностью при раннем обнаружении трафика.

Ключевые слова: сетевой трафик, классификация, NetFlow, зашифрованный трафик, статистика потоков, ранняя классификация.

Abstract. This article presents a systematic comparative analysis of three main approaches to network traffic classification: port-based, payload-based, and statistical approaches. Port-based methods are simple and fast; however, they do not provide sufficient robustness in environments with dynamic ports and tunneling. The DPI approach ensures high accuracy for certain protocols, but its applicability is limited by the inability to fully access packet payloads under modern encryption technologies, as well as by high computational complexity. Flow statistics-based methods rely on packet header attributes and flow characteristics, which makes them effective even for encrypted traffic. At the same time, within this approach, the selection of informative features and the “new class” problem require separate solutions. The results of the study showed that statistical approaches demonstrate high efficiency in the early identification of traffic.

Keywords: network traffic, classification, NetFlow, encrypted traffic, flow statistics, early classification.

KIRISH

Internet xizmatlarining kengayishi tarmoqda bir vaqtning o‘zida turli sinfdagi oqimlar ilova, striming va yuklab olish oqimlari harakatlanishiga olib keladi. Tashkiliy siyosatga rioya qilish, xavfsizlikni kuchaytirish va xizmat sifatini kafolatlash uchun bu oqimlarni aniqlash va to‘g‘ri sinflarga ajratish talab etiladi. Amaliyotda paket tarkibini o‘qishga tayanadigan paketlarni chuqur tahlil qilish texnologiyalari (Deep Packet Inspection, DPI) keng qo‘llanadi, biroq trafikning katta qismi shifrlangani sababli payloadga kira olmaslik, yuqori hisoblash tannarxi va maxfiylik cheklovlari ushbu yondashuvining qo‘llanishini keskin cheklaydi.

Ilovalar oqimlari tashkilot siyosatiga zid bo‘lishi, ishlab chiqarish samaradorligiga salbiy ta’sir ko‘rsatishi yoki xavfsizlik xavflarini yuzaga keltirishi mumkin. Masalan, ish vaqtida ko‘ngilochar striminglar va katta hajmdagi yuklab olish oqimlari tarmoq o‘tkazuvchanligini band etadi, ayrim xizmatlar esa ma’lumotlarni yashirin uzatish, C2-kanallar bilan aloqa yoki tarmoqni skaner qilish kabi xatti-harakatlarni maskalashi mumkin. Bunday oqimlar istalmagan yoki potensial xavfli oqimlar toifasiga kiritilib, ularni aniq ajratish siyosatga muvofiqlik, xavfsizlik va QoS boshqaruvi uchun zarurdir. Bundan tashqari, billing uchun ham tasniflash muhim hisoblanadi, hususan trafikni ilova yoki xizmatlar bo‘yicha ajratish to‘lovlarni to‘g‘ri hisoblashga yordam beradi, limitdan oshish yoki noto‘g‘ri foydalanish holatlarini erta ko‘rsatadi, bo‘limlar bo‘yicha xarajatni to‘g‘ri

ISSN 3030-3907

taqsimlashni osonlashtiradi va daromad yo‘qotilishining oldini oladi. Trafik real vaqt rejimida kuzatilsa, billingning aniqligi va shaffofligi yanada oshadi.

Internet trafigi turli protokollar asosida shakllanuvchi ko‘plab oqimlarning dinamik superpozitsiyasidan tashkil topadi. Zamonaviy tarmoqlarda shifrlangan trafik ulushining ortib borishi an’anaviy sinflashtirish usullarining samaradorligini sezilarli darajada pasaytirmoqda. Shu sababli oqimning statistik xususiyatlariga asoslangan sinflashtirish yondashuvlari ushbu muammoning istiqbolli yechimi sifatida qaralmoqda. Sun’iy intellekt texnologiyalarini qo‘llash esa o‘zgaruvchan internet muhitiga moslashish, trafik xususiyatlarini chuqurroq hisobga olish va sinflashtirish aniqligini oshirish imkonini beradi. Agar avval port raqamlari va an’anaviy identifikatsiya belgilariga tayanish yetarli bo‘lgan bo‘lsa, bugungi kunda ilovalarning turli protokollardan foydalanishi, tunnellash va dinamik portlarning qo‘llanilishi sababli bunday belgilar yetarli darajada ishonchli bo‘lmay qolmoqda.

TADQIQOT METODOLOGIYASI

An’anaviy tarmoq trafigini sinflashtirish usullari port raqamlari yoki paketning foydali yuklama qismiga tayangan holda paketlarni bevosita tahlil qilishga asoslanadi. Xususan, portga asoslangan yondashuvda paket sarlavhasi ko‘rib chiqilib, undagi manba va qabul qiluvchi port raqamlari ajratib olinadi. Hamda ushbu qiymatlar IANA tomonidan yuritiladigan mashhur va ro‘yxatdan o‘tgan portlar ro‘yxati bilan taqqoslanib, tegishli ilova protokoli aniqlanadi.

Ushbu yondashuv asosida bir qancha izlanishlar olib borilgan. Xususan, A.Madhukar, C. Williamson [1] tadqiqitchilar portga asoslangan yondashuv asosida tarmoq trafigini tahlil qilib chiqishgan. Maqolada ikki yil davomida Calgary universitetining internet tarmog‘idan o‘tgan p2p ilovalarining trafiklari tahlil qilingan. Olingan natijalar trafikni sinflashtirish va filtrlashda portga asoslangan yondashuvdan foydalanish 30% dan, maxsimal 70% gachan aniqlikga erishilgan. Natija P2P ilovalar uchun portga asoslangan yondashuvning bugungi kunda samarasiz ekanlgini ko‘rsatdi.

Port raqamlari asosida trafikni sinflashtirish va filtrlash bugungi kunda yuqorida ko‘rsatilgan sabablarga ko‘ra aniq natijalarni bermaydi. Bu zararli va keraksiz ma’lumotlarni tarmoqda ko‘payishi, tarmoq o‘tkazish qobiliyatining pasayishi va tarmoq unumdorligiga salbiy ta’sir ko‘rsatadi.

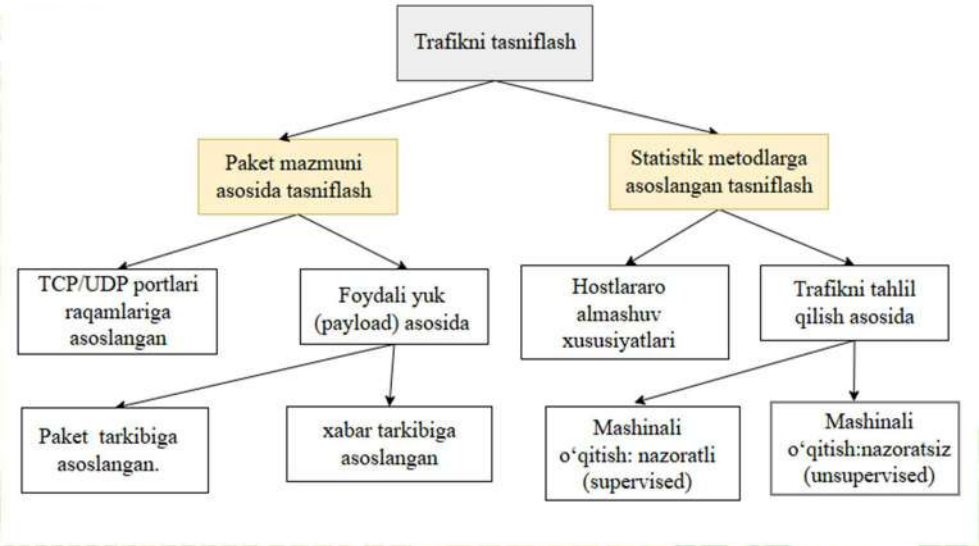
Foydali yuklama asosida tarmoq trafigini sinflashtirish va filtrlash, trafikni port raqami asosida aniqlashda kelib chiqaradigan muammolarni hal etish uchun ishlab chiqilgan. Foydali yuklamaga asoslangan yondashuvda protokolni identifikatsiyalash paketni foydali yuklama qismidan oldindan ma’lum bo‘lgan, har bir ilova uchun yagona hisoblangan belgini qidirib topish va uni bir xil guruhdagi oqimlar bilan o‘zaro munosabatini tahlil qilish orqali amalga oshiriladi.

ISSN 3030-3907

An’anaviy usullarning cheklovlari sabab, so‘nggi yillarda tarmoq trafikini aniq va samarali tasniflashga qaratilgan muqobil yondashuvlar bo‘yicha ko‘plab ishlar paydo bo‘ldi.

Eng istiqbolli yo‘nalishlardan biri statistik tasniflash bo‘lib, u trafik oqimlarining statistik parametrlaridan foydalanadi.

Statistik klassifikatsiya tarmoq oqimlarini tasniflashda keng qo‘llaniladigan zamonaviy usullardan biridir. Uning mohiyati shundan iboratki, turli xil ilovalar tomonidan yaratilgan trafik o‘ziga xos xususiyatlarga ega bo‘lib, ular ilovalarning ichki tabiatini va ishlash mexanizmlarini aks ettiradi. Ushbu xususiyatlar oqim atributlari ko‘rinishida ifodalanadi va ularni statistik metodlar yoki sun’iy intellekt yordamida sinflashtirish va filtrlash mumkin.



1- rasm. Tarmoq trafigini tasniflash usullari

Agar to‘liq va belgilangan o‘quv ma’lumotlar to‘plami mavjud bo‘lsa, tasniflash modelini qurish juda qulay. Bunda mashinali o‘qitishning yangi texnologiyalari qo‘llanadi. Ilgari olib borilgan ishlar statistik metodlar yordamida trafikni QoS xizmatlari sinflariga ajratishga qaratilgan. Masalan, oqimlarni tasniflashda quyidagi statistik darajalar o‘rganilgan:

- Paket darajasi: paket hajmining o‘rtacha qiymati, dispersiyasi, kvadratik og‘ishi.
- Oqim darajasi: oqim davomiyligi, bayt hajmi, oqimdagi paketlar soni.
- TCP darajasi: ulanish davomiyligi, o‘tkazilgan baytlar, oqimlar soni.
- Butun oqim xususiyatlari: nazorat oqimlari bilan solishtirilgan umumiy bayt hajmi va paketlar soni.

Ushbu atributlar asosida tasniflash modelini qurishda chiziqli diskriminant tahlil, eng yaqin qo‘shnilar metodi (k-NN) kabi algoritmlar qo‘llangan.

Statistik tasniflashga asoslangan yondashuvlarda, odatda, ikki asosiy algoritm qo‘llanadi:

ISSN 3030-3907

1. Xulq-atvoriy algoritmlar - oqimlarning umumiy xatti-harakatlarini ifodalaydi. Xulq-atvoriy algoritmlarning asosiy g‘oyasi – qaysi ilovalar ma’lum trafik oqimlarini yaratishini aniqlashdir. Tarmoqdagi hostlar o‘rtasidagi o‘zaro aloqani tahlil qilish orqali hostda ishga tushirilgan ilovalar turlarini aniqlash mumkin. Trafik sinflari va ularning xulq-atvoriy-statistik xususiyatlari o‘rtasidagi bog‘liqlik bo‘yicha bir qator TCP-ilovalarda amaliy tadqiqotlar olib borilgan va ularda trafik aloqalarining empirik modellarini qurish taklif etilgan.

2. Statistik algoritmlar - oqimlarning statistik xususiyatlariga asoslanadi. Ular ilovalarni aniqlashda muayyan trafik sinfiga xos bo‘lgan statistik belgilarni ajratib ko‘rsatadi. Bu yondashuv turli dasturlarni farqlash imkonini beradi. Statistik metodlar, odatda, ikki guruhga bo‘linadi:

- Nazoratsiz (unsupervised) usullar - oldindan belgilangan yorliqlar bo‘lmagan holatda oqimlarni klasterlash va guruhlash orqali tahlil qiladi. Masalan, k-means yoki hierarxik klasterlash.

- Nazoratli (supervised) usullar - oldindan belgilangan sinflar asosida model o‘rgatiladi va yangi trafik oqimlari shu model yordamida tasniflanadi. Masalan, Decision Tree, Random Forest, SVM.

Trafikni statistik usullar asosida tasniflash odatda ikki bosqichda amalga oshiriladi:

- O‘qitish (training) bosqichi. Bu bosqichda o‘quv ma’lumotlar to‘plami algoritmga kiritiladi va natijada tasniflash modeli quriladi.

- Tasniflash (testing) bosqichi. Bu yerda qurilgan klassifikator yangi trafik oqimlarining qaysi sinfga tegishli ekanini bashorat qilish uchun qo‘llaniladi.

MUHOKAMA VA NATIJALAR

Tadqiqot natijalari shuni ko‘rsatadiki, yorliqlangan statistik usullar orqali qurilgan klassifikatorlar aniqlik bo‘yicha paket tarkibini tahlil qiladigan klassifikatorlar bilan deyarli bir xil darajaga chiqishi mumkin. Eng muhimi, bunday natijaga kamroq hisoblash resurslari bilan erishiladi. Demak, statistik yondashuvlar amaliy tizimlar uchun tejamkor va samarali variant hisoblanadi. Ko‘rib chiqilgan yondashuvlarning qisqa taqqoslanishi 1-jadvalda berilgan.

Jadvaldan ko‘rinib turibdiki, port raqamlariga va paket yuklamasiga asoslangan yondashuvlar statik bo‘lib, ular paket sarlavhasi yoki imzolarni tahlil qilish orqali sinflarni aniqlaydi.

Statistik oqimlarga asoslangan yondashuv esa oqim xususiyatlari asosida vaqt bo‘yicha o‘zgaruvchi statistik parametrlarni hisoblab, trafik turini aniqlaydi. Shu sababli, aynan statistik oqim yondashuvi shifrlangan trafik uchun eng mos va aniqligi yuqori usul sifatida tadqiqotda qo‘llanildi.

ISSN 3030-3907

Quyidagi tadqiqotlar statistik yondashuvlar samaradorligini keng qamrovda taqqoslab bergan [1-5]. Turli ML klassifikatorlari Naive Bayes, Kernel Estimation bilan Naive Bayes, C4.5, Bayesian Network va Naive Bayes Tree oqim tasnifida sinovdan o‘tkazilib, belgilarni tanlash va hisoblash unumdorligiga alohida e’tibor beriladi. [6] da o‘yin trafigini ajratish natijalari tahlil qilinadi. Tadqiqotda statistik tasniflash usuli port raqamlariga tayangan usul va xost xatti-harakatiga asoslangan yondashuv bilan qiyoslanadi. [7-10] tadqiqotida bir nechta ajratish qobiliyatiga ega manbalardan olingan xususiyatlarni diskretlashtirish, shuningdek birinchi paketlar uzunligi va portlardan foydalanish masalalari ko‘riladi.

1-jadval.

An’anaviy va statistik yondashuvlari tahlili

Ko‘rsatkichlar	Portga asoslangan	Paketlarning tarkibigalamaga asoslangan	Oqim statistikalariga asoslangan
Aniqlik	past	yuqori	yuqori
Belgilarni ajratish murakkabligi	past	yuqori	belgilar to‘plamiga bog‘liq
Sinflashtirish murakkabligi	past	yuqori	o‘rtacha
Shifrlangan trafikni aniqlash	ha	yo‘q	ha
Aprior ma’lumot	Port raqamlar ro‘yxati	Trafik signaturalari	Belgilangan (yorliqlangan) ma’lumotlar

Yuqoridagi tadqiqot ishlari statistik trafik tasniflash modellari internet tarmog‘ining turli kuzatuv nuqtalarida ham qo‘llanishi mumkinligini ko‘rsatdi. Biroq bunday modellarning tarmoqqa sezgirligi yuqori: bir tarmoq ma’lumotlari bilan o‘qitilgan tasniflash modeli boshqa tarmoqda samaradorligini yo‘qotishi mumkin va yangi trafik bilan qayta o‘qitishni talab qiladi. Ilovalarni samarali identifikatsiya qilish uchun kam, lekin informativ va to‘liq xususiyatlar to‘plamini tanlash zarur [11].

Tasniflash uchun xususiyatlar shakllantirish maqsadida oqimlarning statistik tavsiflari aniqlanadi va ular model o‘qitishda qo‘llanadi. Yaxshiroq va aniqroq natijaga erishish uchun dastlabki ma’lumotlar to‘plamida tarmoqning turli nuqtalarida va turli vaqtlarda yozib olingan aralash trafik bo‘lishi kerak. Agar boshlang‘ich to‘plam faqat bir xil vaqtda va tarmoqning aynan bitta nuqtasida yozib olingan paketlardan iborat bo‘lsa, tekshiruv natijalari klassifikatorning juda yuqori aniqligini ko‘rsatadi.

ISSN 3030-3907

Keltirgan tahlil natijalari tarmoq trafigini tahlil qilish va aniqlashning uchta asosiy usulini taqqoslaydi: portga asoslangan, DPI, va statistik yondashuvlar. Quyida har bir usulning asosiy xulosalari va amaliy tavsiyalari jamlangan:

2-jadval.

Tarmoq trafigini tasniflashning mavjud yondashuvlari bo‘yicha qiyosiy tahlili

Yondashuv	Aniqlik	Avfzaligi	Xulosa
Portga asoslangan	P2P va dinamik portlarda 30-70	Tez va resurs talabi past	Aniq tasniflash uchun yetarli emas
Paket mazmuniga asoslangan	Shifrlanmagan trafikda deyarli 100% (to‘liq payload tahlilida). Birinchi kilobayt skanerlansa 79% gacha.	TLS/SSL, QUIC/HTTP/3 kabi shifrlash sababli ko‘p oqimlarda payload ko‘rinmas. Hisoblash tannarxi yuqori va muntazam signatura yangilanishi zarur.	Shifrlanmagan yoki ma’lum protokollar uchun aniq, ammo universal emas va shifrlangan trafikda yaroqsiz.
Oqimning statik va dinamik xususiyatlari asosida	Erta bosqichda (birinchi 6–10 paket) yuqori (80–96%). To‘liq atributlar bilan 95–99% gacha.	Shifrlangan trafikda ham ishlaydi. CPU/RAM talabi DPIga nisbatan ancha past.	Real vaqtli QoS (xizmat sifati) va siyosatlarni qo‘llash uchun eng amaliy va tavsiya etiladigan yechim.

Tahlil natijalariga ko‘ra, zamonaviy, shifrlangan trafikka boy tarmoqlarda Statistik yondashuvlar eng samarali va amaliy yechim hisoblanadi, chunki ular DPI kabi yuqori aniqlikni ta’minlab, portga asoslangan usullarga nisbatan shifrlash to‘siqlaridan qochishga va tez ishlashga qodir.

XULOSA VA TAKLIFLAR

Tahlillar shuni ko‘rsatdiki, tarmoq trafigini sinflashtirishning portga asoslangan, paket mazmuniga asoslangan va statistik yondashuvlari aniqlik, moslashuvchanlik, hisoblash murakkabligi hamda zamonaviy tarmoqlarda

ISSN 3030-3907

qo‘llanish imkoniyati jihatidan bir-biridan sezilarli farq qiladi. Portga asoslangan usullar soddaligi va tezkorligi bilan ajralib turadi, dinamik portlar, NAT, tunnellash va shifrlash texnologiyalari keng qo‘llanilayotgan muhitda yetarli darajada ishonchli natija bermaydi. DPI yondashuvi paket tarkibini chuqur tahlil qilish hisobiga ayrim protokollar va ilovalarni yuqori aniqlik bilan aniqlash imkonini beradi, biroq shifrlangan trafik ulushi ortib borayotgan sharoitda foydali yuklama qismiga kira olmaslik, yuqori hisoblash tannarxi va maxfiylik bilan bog‘liq cheklovlar sabab uning amaliy qo‘llanishda muammolar yuzaga kelmoqda.

Tahlil natijalari statistik yondashuvlar zamonaviy tarmoqlar, ayniqsa shifrlangan trafik ustun bo‘lgan muhitlar uchun eng istiqbolli va amaliy yechimlardan biri ekanini ko‘rsatdi. Ushbu yondashuv paket sarlavhasi atributlari hamda oqimning vaqt, hajm va xulq-atvor ko‘rsatkichlariga tayangan holda trafikni erta bosqichda ham samarali sinflashtirish imkonini beradi. Statistik yondashuvlarning asosiy afzalligi shundaki, ular DPIga nisbatan kamroq hisoblash resurslarini talab qiladi, shifrlangan trafikda ham ishlay oladi.

Shu bilan birga, statistik sinflashtirish yondashuvlarida informativ atributlarni tanlash, yangi yoki noma’lum sinflarni aniqlash, turli tarmoq muhitlariga moslashuvchanlikni ta’minlash hamda modelni qayta o‘qitish zarurati kabi masalalar dolzarb bo‘lib qolmoqda. Demak, statistik yondashuv yuqori samaradorlikka ega bo‘lsa ham, uning barqarorligini oshirish uchun xususiyatlar tanlovi, model generalizatsiyasi va moslashuvchan o‘qitish mexanizmlariga alohida e’tibor qaratish talab etiladi.

Amaliy nuqtai nazardan, zamonaviy telekommunikatsiya tarmoqlarida statistik yondashuv asosiy sinflashtirish mexanizmi sifatida tavsiya etiladi. Bunda noaniq yoki qo‘shimcha tekshiruv talab qiluvchi oqimlar uchun gibrid yondashuvni, ya’ni dastlab statistik tahlilni, so‘ng zarurat tug‘ilganda chuqurroq paket tahlilini qo‘llash maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. A. Moore, D. Zuev. “Internet Traffic Classification Using Bayesian Analysis Techniques.” *ACM SIGMETRICS*, 2005.
2. A. W. Moore, K. Papagiannaki. “Toward the Accurate Identification of Network Applications.” *PAM Workshop*, 2005.
3. A. Madhukar, C. Williamson. “A Longitudinal Study of P2P Traffic Classification.” *Proceedings of MASCOTS*, 2006.
4. S. Sen, J. Wang. “Analyzing Peer-to-Peer Traffic Across Large Networks.” *IEEE/ACM Transactions on Networking*, 2004.
5. A. Karagiannis, K. Papagiannaki, M. Faloutsos. “BLINC: Multilevel Traffic Classification in the Dark.” *ACM SIGCOMM*, 2005.

ISSN 3030-3907

6. N. Williams, S. Zander, G. Armitage. "A Preliminary Performance Comparison of Five Machine Learning Algorithms for Practical IP Traffic Flow Classification." *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 5, 2006.
7. T. Nguyen, G. Armitage. "Training on Multiple Sub-flows to Optimize the Use of Machine Learning Classifiers in Real Networks." *IEEE LCN*, 2006.
8. H. Kim, K. Claffy, M. Fomenkov, D. Barman, M. Faloutsos, K. Lee. "Internet Traffic Classification Demystified: Myths, Caveats, and the Best Practices." *ACM CoNEXT*, 2008.
9. J. Zhang, J. Luo. "Flow Classification for Encrypted Internet Traffic with Machine Learning." *IEEE INFOCOM Workshops*, 2020.
10. Ali, T. E., Chong, Y.-W. & Manickam, S. Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Appl. Sci.* 13(5), 3183 (2023).
2. 11.Ray D. Internet Traffic Classification Using Machine Learning Techniques. // *International Scientific Journal of Engineering and Management*, vol. 3, no. 4, p. 14, April 2024.

ISSN 3030-3907