ISNN 3030-3907

2026/3
VOLUME 3

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/3 VOLUME 3

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

NEYRON TARMOQLARIGA ASOSLANGAN PAKETLARNI DINAMIK FILTRLASH USULI VA ALGORITMI

Tashev Sarvar Norboboyevich
katta o‘qituvchi, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
E-mail: sarvar.tashev@gmail.com

Annotatsiya. Mazkur maqolada tarmoq trafigini aniqlash va filtrlash uchun neyron tarmoqlariga asoslangan paketlarni dinamik filtrlash usuli taklif etilgan. Tadqiqotda CNN, Deep Autoencoder va DNN elementlarini birlashtirgan CAPC modeli ishlab chiqilgan. Model paketlarning bayt darajasidagi xususiyatlarini tahlil qilib, xizmat trafigini tasniflaydi hamda zararli va foydali trafikni aniqlaydi. Trafik ma’lumotlari Wireshark orqali yig‘ilib, oldindan qayta ishlanadi va normallashtiriladi. Tajribalar natijasida taklif etilgan model mavjud modellarga nisbatan yuqori samaradorlikni ko‘rsatgan.

Kalit so‘zlar: Neyron tarmoqlar, mashinali o‘qitish, paketlarni filtrlash, CAPC modeli, tarmoq trafigi, trafik tasnifi, SDN, tarmoq xavfsizligi.

Abstract. This paper proposes a neural network-based dynamic packet filtering method for network traffic detection and filtering. In this study, a CAPC model combining CNN, Deep Autoencoder, and DNN elements is developed. The model analyzes byte-level characteristics of packets to classify service traffic and detect both malicious and legitimate traffic. Network traffic data are collected using Wireshark and then undergo preprocessing and normalization. Experimental results show that the proposed model demonstrates higher efficiency compared to existing models.

Keywords: neural networks, machine learning, packet filtering, CAPC model, network traffic, traffic classification, SDN, network security.

Аннотация. В данной статье предложен метод динамической фильтрации пакетов на основе нейронных сетей для обнаружения и фильтрации сетевого трафика. В исследовании разработана модель CAPC, объединяющая элементы CNN, Deep Autoencoder и DNN. Модель анализирует байтовые характеристики пакетов и выполняет классификацию сервисного трафика, а также выявляет вредоносный и легитимный трафик. Данные сетевого трафика собираются с помощью Wireshark, после чего проходят этапы предварительной обработки и нормализации. Результаты экспериментов показали, что предложенная модель демонстрирует более высокую эффективность по сравнению с существующими моделями.

ISSN 3030-3907

Ключевые слова: нейронные сети, машинное обучение, фильтрация пакетов, модель CAPC, сетевой трафик, классификация трафика, SDN, информационная безопасность сети.

KIRISH.

So‘ngi yillarda mashinali o‘qitish (MO‘) usullari tarmoq xavfsizligini ta’minlash masalalarini hal qilishda keng qo‘llanila boshladi. Mashinali o‘qitish tarmoq trafigini tahlillash va tasniflash uchun istiqbolli texnika sifatida qaralmoqda[1].

Mashinali o‘qitishga asoslangan usullar oldindan belgilangan qoidalar asosida tarmoq trafigini tahlillaydigan paketlarni teran tekshiruviga (DPI) qaraganda ilovalar paketlari yoki trafik oqimlaridagi yashirin xususiyatlarni tahlil qila oladi. Mashinali o‘qitishdagi neyron tarmoq modellarining konvergensiya (yaqinlashish) vaqti grafik protsessor (GPU) texnologiyasining tez rivojlanishi tufayli sezilarli darajada qisqardi va bu esa parallel hisoblash jarayonini ancha tezlashtirdi [2].

Xususan, teran o‘qitish paradigmasi neyron tarmoqlar turli sohalarda keng qo‘llanilmoqda. Ko‘plab teran o‘qitish modellari taklif etilgan bo‘lib, ularga trafikni qayta ishlashda ishlatiladigan konvolyutsiyon neyron tarmoqlar (CNN) va semantik tahlilda qo‘llaniladigan rekurrent neyron tarmoqlar (RNN) kiradi.

ADABIYOTLAR TAHLILI.

Teran o‘qitishning muhim tarkibiy qismi sifatida konvolyutsiyali neyron tarmoqlar ayniqsa tasvirni tanib olishda keng qo‘llanilib, ba’zida inson salohiyatidan ham ustun natijalarga erishmoqda. Konvolyutsiyali neyron tarmoqlarning tasvirni aniqlashdagi muvaffaqiyati tarmoq trafigini tasniflashda konvolyutsiyali neyron tarmoqlarining xususiyatlaridan foydalanish imkonini beradi.

Ixtiyoriy teran o‘qitish modelining qo‘llanilishi senariyga va kiritilayotgan ma’lumotlarga bog‘liq. Shu nuqtai nazardan, tarmoq paketlarining ma’lumot turi tasvirning ma’lumot turiga juda o‘xshashdir. Paketlar va tasvirlar 0 dan 255 gacha bo‘lgan bayt qiymatlaridan tashkil topgan bo‘lib, ularning asosiy farqlari faqat ma’lumot hajmi va o‘lchamlari bilan belgilanadi. Ma’lumot hajmi nuqtai nazaridan, Ethernet maydoni ma’lumot qismi (payload) maksimal 1500 bayt bo‘ladi - bu Ethernetning uzatishning maksimal birligi (MTU) bo‘yicha belgilanadi. Tasvir hajmi esa uning aniqligi, siqish formati va rangli bo‘lishiga bog‘liq. Ma’lumotlarning o‘lchamiga kelsak, paket - bu bir o‘lchamli bayt ketma-ketligi, tasvir esa ikki o‘lchamli piksellardan tashkil topgan.

Teran avtokodlovchilar (DAE - Deep Autoencoder) ko‘pincha nazoratsiz o‘qitish yoki o‘lchamni kamaytirish vazifalari uchun ishlatiladi [3]. Paketlarning

ISSN 3030-3907

kiruvchi o‘lchovi nisbatan katta bo‘lganligi sababli, tadqiqot ishida avtokodlash qo‘llanilgan. An’anaviy teran o‘qitish modellari parametrlarni tasodifiy tarzda ishga tushiradi. Har bir boshlang‘ich tasodifiy parametrlar modelning barqaror ishlashiga salbiy ta’sir ko‘rsatishi mumkin. Shu sababli, tadqiqotda avtokodlovchi paketdagi barcha baytlar orasidagi muhim ma’lumotni ajratib olish uchun foydalaniladi.

1D konvolyutsion qatlam bilan birgalikda ishlatilganda, avtokodlovchi kuchliroq kodlovchi vositaga aylanadi. Bu avtokodlovchi konvolyutsiyali neyron tarmoqlarning xususiyatlaridan foydalanib, ma’lumotni samarali tarzda ajratib oladi. Ushbu tarmoq tuzilmasi hali boshqa trafik tasniflash tadqiqotlarida qo‘llanilmagan. Kodlovchi (encoder) yaxshi boshlang‘ich parametrlar bilan mustahkam tarmoq tuzilmasi hisoblanadi. Hosil qilingan va o‘qitilgan kodlovchi paketlarni tasniflash uchun teran neyron tarmoq (DNN) klassifikatori bilan birlashtiriladi.

Yuqoridagi g‘oyalar asosida, Konvolyutsiyali avtokodlovchi paket tasniflovchi (CAPC) modeli taklif qilinadi. Bu model bir xizmatga tegishli paketlarni boshqasidan samarali farqlashga yordam beradi. Konvolyutsiyali avtokodlovchi paket tasniflovchi konvolyutsiyali neyron tarmoqlarning lokal sezish xususiyatlari, teran avtokodlovchilarning o‘lchamni kamaytirish va parametrlarni boshlang‘ich qiymatlash imkoniyatlaridan foydalanib, paketni aniq xizmat turiga tasniflaydi va shu orqali tasniflash aniqligini oshiradi. Tasniflash maqsadli ma’lumotlar to‘plami yozib olingan trafik va ISCX VPN-nonVPN-ning ochiq virtual xususiy tarmoq ma’lumotlar to‘plamini o‘z ichiga oladi.

Ushbu tadqiqotning asosiy jihatlarini quyidagicha umumlashtirish mumkin:

1D konvolyutsiya va avtokodlash kombinatsiyasiga asoslangan zamonaviy CAPC teran o‘rganish modeli ishlab chiqilgan. Paketlar aniq va umumiy tarzda foydali va zararli sifatida ajratiladi.

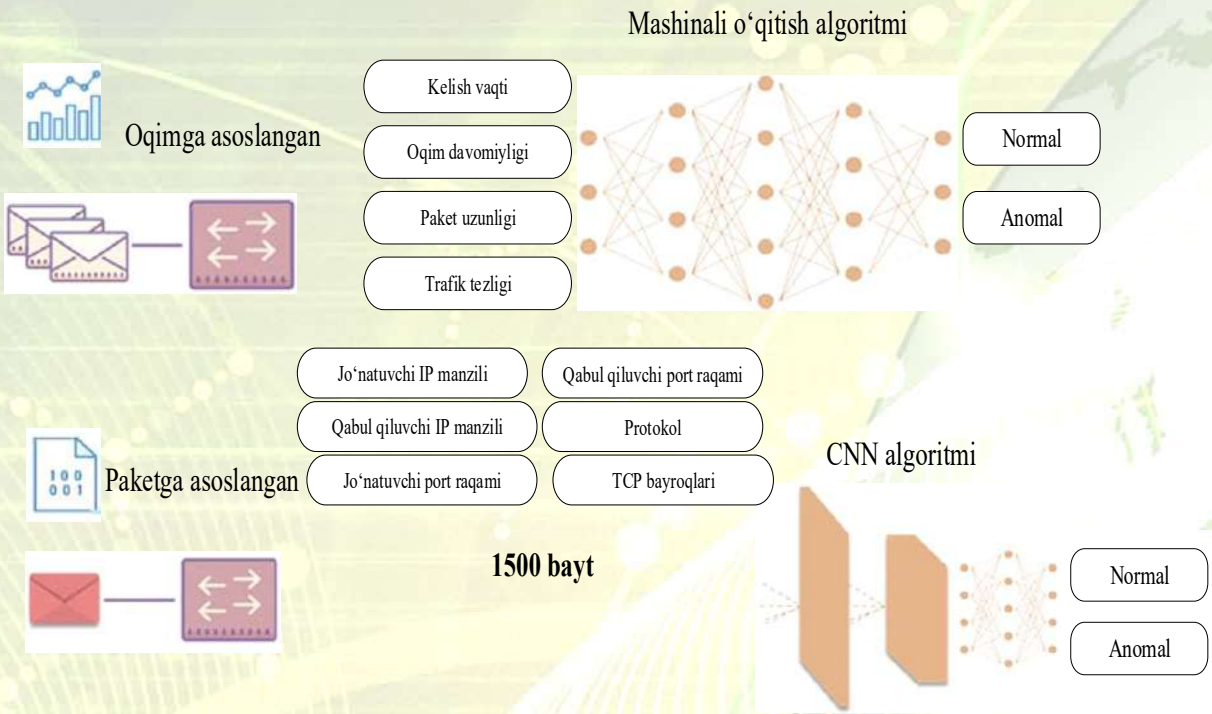
Maxfiy va ommaviy ma’lumotlar to‘plamlari modelni o‘qitish va samaradorlikni baholash uchun ishlatiladi. Paket ma’lumotlarini oldindan qayta ishlashning umumiy jarayoni, shu jumladan paketdagi manzillarni aniqlash, shu bilan modellarning ishlashini barqarorlashtirish namoyish etiladi [4].

Tajribalar bir nechta ishlash ko‘rsatkichlarini, jumladan, accuracy, F1-score, precision va recallni ko‘rsatish uchun taqdim etiladi. Modelni real holatda qo‘llash imkoniyatini ko‘rsatish uchun tasniflash vaqti ham baholanadi.

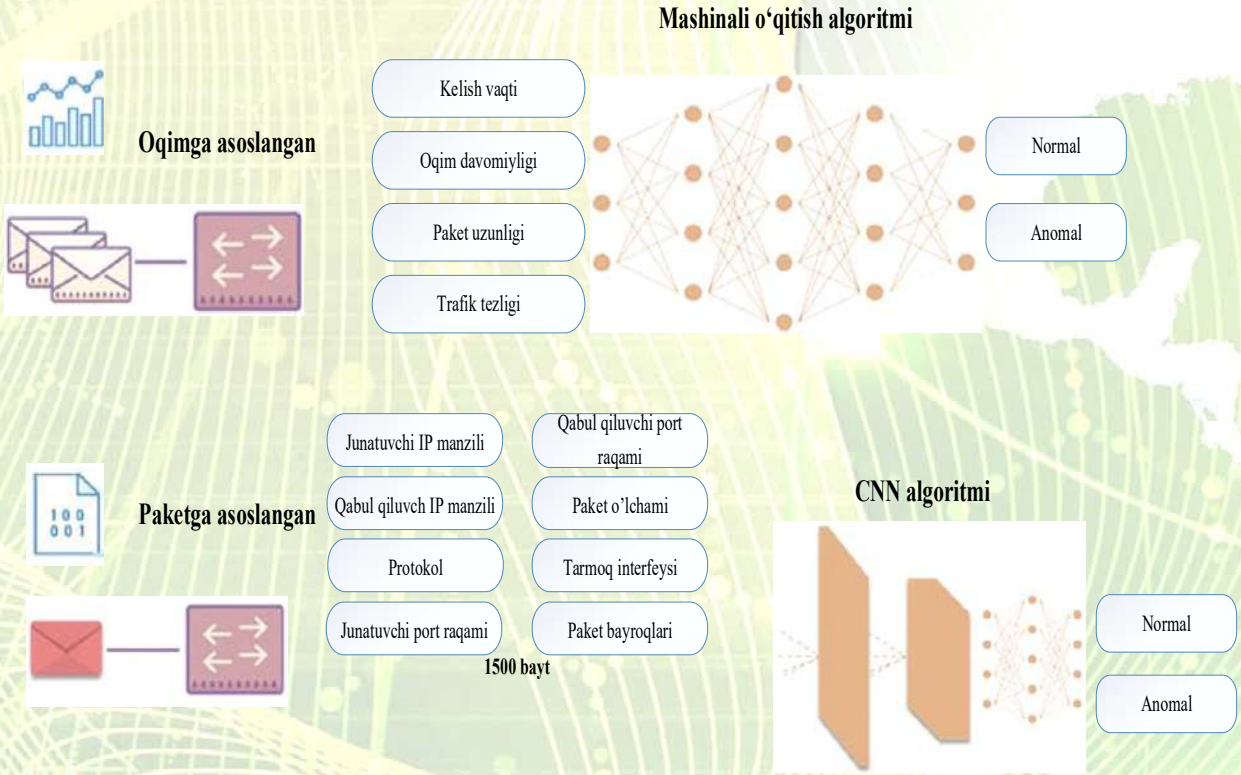
CAPC - bu nazoratli (supervised) o‘qitishga asoslangan model bo‘lib, teran o‘qitish modelini o‘qitish uchun belgilangan xizmat paketlarini talab qiladi. 1-rasmda o‘qitish ma’lumotlarining turiga qarab trafikni ikki xil yondashuvga

ISSN 3030-3907

ajratish mumkin: oqimga asoslangan (flow-based) **va** paketga asoslangan (packet-based) trafikni mavjud usuli ko‘rsatib o‘tilgan.



1-rasm. Oqimga va paketga asoslangan trafikni filtrlashning mavjud usuli



2-rasm. Xususiyatlar asosida oqimga va paketga asoslangan trafikni filtrlashning takomillashtirilgan usuli

2-rasmda xususiyatlar asosida oqimga va paketga asoslangan trafikni filtrlashning takomillashtirilgan usuli keltirilgan.

ISSN 3030-3907

Bundan tashqari, oqim xususiyatlari bilan birga bir nechta MO‘ algoritmlari ham qo‘llaniladi, masalan:

- Support Vector Machine (SVM) [5],
- Decision Tree [6],
- Neyron tarmoqlar (Neural Network) [7].

Oqimga asoslangan usullar paket yukini tekshirmaydi, lekin ular statistik xususiyatlarni tahlil qiladi hamda normal va zararli trafikni tasniflaydi, shuning uchun hatto shifrlangan trafikni tanib olish mumkin[8].

Paketga asoslangan (packet-based) usullar esa xizmat trafigidagi har bir alohida paketni tasniflaydi va paketdagi har bir baytni xususiyat sifatida oladi. Ma’lumot formati sababli bunday yondashuvlarda kiruvchi o‘lcham oqimga asoslangan yondashuvlarnikidan kattaroq bo‘ladi [9].

Ma’lumot formatiga qarab yondashuvlarni ajratishdan tashqari, trafik tasniflash usullari quyidagi uch asosiy turga ajratilishi mumkinligi ham ta’kidlangan:

1. Portga asoslangan (port-based) usullar.
2. Yuklamaga asoslangan usullar.
3. Mashinali o‘qitishga asoslangan usullar

Ko‘plab tadqiqotlarda oqim (flow) xususiyatlariga asoslangan o‘ziga xos xususiyat tanlash (feature selection) sxemalari taklif qilingan.

1-jadval

Trafikni klassifikatsiya qilish usullari

Yondashuv	Tavsif	Afzalliklar	Kamchiliklar
1	2	3	4
Portga asoslangan usullar	Paketlarni port raqam-lariga qarab klassi-fikatsiya qilish, masa-lan, HTTP protokoli uchun TCP port 80.	-Tezkor klassifikatsiya - Yuqori aniqlik	- Bir xil portdan foydalanadigan turli xizmatlar -Dinamik portlardan foydalanish
Yuklamaga asoslangan usullar	Ilova qatlamidagi yuklama (payload)ni protokol imzolari orqali tekshirish.	Dinamik portlardan foydalanuvchi xizmatlarni aniqlash	- Yuqori hisoblash xarajati -Shifrlangan ma’lumotlar - Yangi ilovalarni aniqlashda qiyin-chiliklar

ISSN 3030-3907

Mashinali o‘qitishga asosidagi usullar	Paket yuklamasi yoki statistik xususiyatlaridan belgilarni chiqarib, ML modeli bilan klassifikatsiya qilish.	- Dinamik portlar va shifrlangan ma’lumotlarni aniqlash -O‘xshash ilovalarni klasterlash	- Portga asoslangan usullarga nisbatan uzoq klassifikatsiya vaqti -Trening ma’lumotlari talab etiladi

Neyron tarmoqqa asoslangan tasniflagichlar esa o‘zining ichki parametrlari ustida ishlash orqali oqim xususiyatlariga nisbatan og‘irliklarni (weights) avtomatik yangilay oladi. Neyron tarmoq modellari nafaqat oddiy xizmat trafikini tasniflashda, balki anomaliyalarni aniqlash va hujumlarni aniqlash tizimlari (IDS)da ham qo‘llaniladi [10].

Teran o‘qitish (deep learning) usuli dastlabki paketlarni kirish sifatida olganda istiqbolli yechim bo‘lib, hatto shifrlangan trafik baytlari orasidagi yashirin bog‘liqliklarni aniqlay oladi [11].

Yakuniy ishlash samaradorligi DNN, DAE va CNN modellarining natijalari bilan solishtiriladi. Modelni o‘qitishda quyidagi ma’lumotlar to‘plamlaridan foydalaniladi:

- 16 ta xizmat bo‘yicha yozib olgan trafik;
- 24 ta xizmatdan iborat ochiq VPN-nonVPN to‘plami.

Modelning aniq (fine-grained) va umumiy (coarse-grained) tasniflash imkoniyatlari sinovdan o‘tkazilib, CAPCning samaradorligi va barqarorligi isbotlanadi. O‘qitilgan model SDN (Software-Defined Networking) muhitida amalda joylashtirilishi mumkin - ya’ni CAPC boshqaruv qatlamiga joylashtiriladi. Yangi xizmat paketi tarmoqga kirgan zahoti, u markaziy boshqaruvga uzatiladi va CAPC modeli yordamida darhol qaysi xizmatga tegishli ekani aniqlanadi.

Shundan so‘ng, tarmoq ichida uzatilayotgan barcha xizmat trafiklarini boshqarish uchun xizmatlar to‘plami (service pool) yaratilishi mumkin. Bu orqali dinamik marshrut tanlash (dynamic path decision), xizmat sifati nazorati (QoS enforcement) va anomaliyali trafikning oldini olish (prevention of anomaly traffic) kabi funksiyalarni amalga oshirish mumkin bo‘ladi.

Teran o‘qitish asosidagi paket tasniflagichni qurish uchun bir nechta bosqichlarni oldindan bajarish talab etiladi:

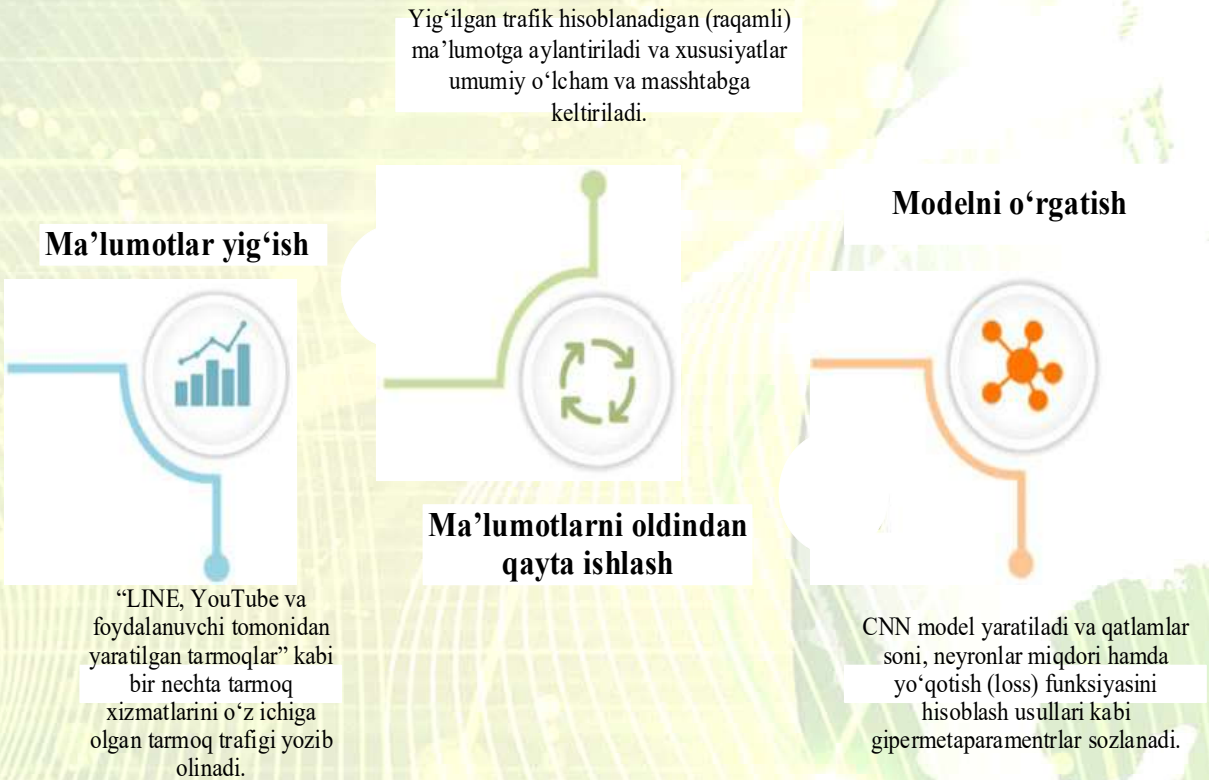
1. Ma’lumot yig‘ish;
2. Ma’lumotlarni oldindan qayta ishlash;
3. Modelni o‘rgatish.

ISSN 3030-3907

Birinchidan, turli xizmatlarga oid to‘plangan shaxsiy trafik (private traffic) ma’lumotlarini olinadi.

Ikkinchidan, ishlov berilmagan formatda yig‘ilgan trafikni hisoblash mumkin bo‘lgan ma’lumotlarga aylantirish va normallashtirish kerak. Har bir yozuv bir xil o‘lchamdagi kirish formatiga ega bo‘lishi kerak. Modelni loyihalash va qurish, giperparametrlarni belgilash va normallashtirilgan ma’lumotlar to‘plami asosida modelni o‘qitish ishlarini amalga oshiriladi.

Har bir bosqich 3-rasmda ko‘rsatilgan tarzda tasvirlangan.



3-rasm. Ma’lumot formati asosida trafikni filtrlash

Trafikni o‘qitishdan oldin xizmat ko‘rsatish trafikini yig‘iladi va har bir paket xizmat turiga qarab tasniflanishi kerak. Birinchi qadam - qaysi xizmatlarni yig‘ish kerakligini aniqlash. Shunga ko‘ra, quyidagi to‘rtta asosiy kategoriyalar trafigiga yo‘naltirilgan: fayllarni uzatish, video oqimlari, VoIP va masofadan boshqarish. Har bir asosiy toifada to‘rtta ilova, jami 16 ta xizmat mavjud bo‘lib, toifalar va xizmatlarning muvofiqligi 2-jadvalda keltirilgan.

2-jadval

Yig‘ilgan xizmat trafigi tavsifi

Fayllarni uzatish	Video ma’lumotlar	VoIP	Masofaviy boshqaruv
1	2	3	4
FTP	RTP/MPEG	LINE VoIP	RDP

ISSN 3030-3907

SFTP	RSTP video	Skype VoIP	VMware
OneDrive	UDP video	Zoom VoIP	XenServer
SCP	YouTube video	Join.me VoIP	NCU cloud

Ushbu tadqiqotda xizmat trafigini yozib olish uchun Wireshark dasturi [12] ishlatilgan.

Algoritmdan maqsad - rndtfc (i) ichidan svci ga tegishli tfcsvc (i) ni tutib olish. Har bir tutib olingan paket pktrnd (i) ning IP manzili tekshiriladi va shu paket svci ga tegishlimi-yo‘qmi aniqlanadi. Agar paket svci ga tegishli bo‘lsa, u holda tfcsvc (i) ga yig‘iladi, aks holda tashlab yuboriladi.

1-qadam. Trafikni tutish**:** $rnd_{tfc}(i)$ ishga tushiriladi - bu xizmat (svc) uchun trafikni yozishni boshlaydi va har bir kiruvchi paket $pkt_j^{rnd}(i)$ni tutadi.

2-qadam. Paketning IP manzilini tekshirish**:** Agar $IP_{svc}(i)$ qiymati $IP_{pkt}^{src}(j,i)$ yoki $IP_{pkt}^{dst}(j,i)$ga teng bo‘lmasa, bu paket tashlab yuboriladi (drop qilinadi).

3-qadam. Paket qabul qilinadi**:** Agar IP mos kelsa, $rnd_{tfc}(i)$ paketi $tfc_{svc}(i)$ yig‘iladigan trafik fayliga **qo‘shiladi.**

4-qadam. Manzillarni birxillashtirish: Quyidagi maydonlar o‘zgartiriladi:

- $MAC_{pkt}^{src}(j,i)$– manba MAC manzili
- $MAC_{pkt}^{dst}(j,i)$– manzil MAC manzili
- $IP_{pkt}^{src}(j,i)$– manba IP manzili
- $IP_{pkt}^{dst}(j,i)$ – manzil IP manzili

5-qadam. Trafikni saqlash: $tfc_{svc}(i)$ fayli .pcap formatida $pcap_{svc}(i)$ nomi bilan saqlanadi.

6-qadam. PCAP faylni matn formatiga o‘tkazish**:** pcap_svc(i) fayli o‘n oltilik (hex) matn ko‘rinishida txt_svc(i) ga eksport qilinadi**.**

Har bir paketdagi manzillar belgilangan (standart) qiymatlarga ko‘ra tasniflashini ta’minlaydi. Shunday qilinishi natijasida klassifikator trafikni bevosita IP yoki MAC manzillar asosida emas, balki mazmuni asosida tasniflaydi[13]. Oldindan ishlov berish teran o‘qitish(deep learning) modeliga kiruvchi paket ma’lumotlarini o‘qish va hisoblash imkonini beradi. Buning uchun ikki asosiy muammoni hal qilish lozim.

3-jadval

Belgilar tavsifi

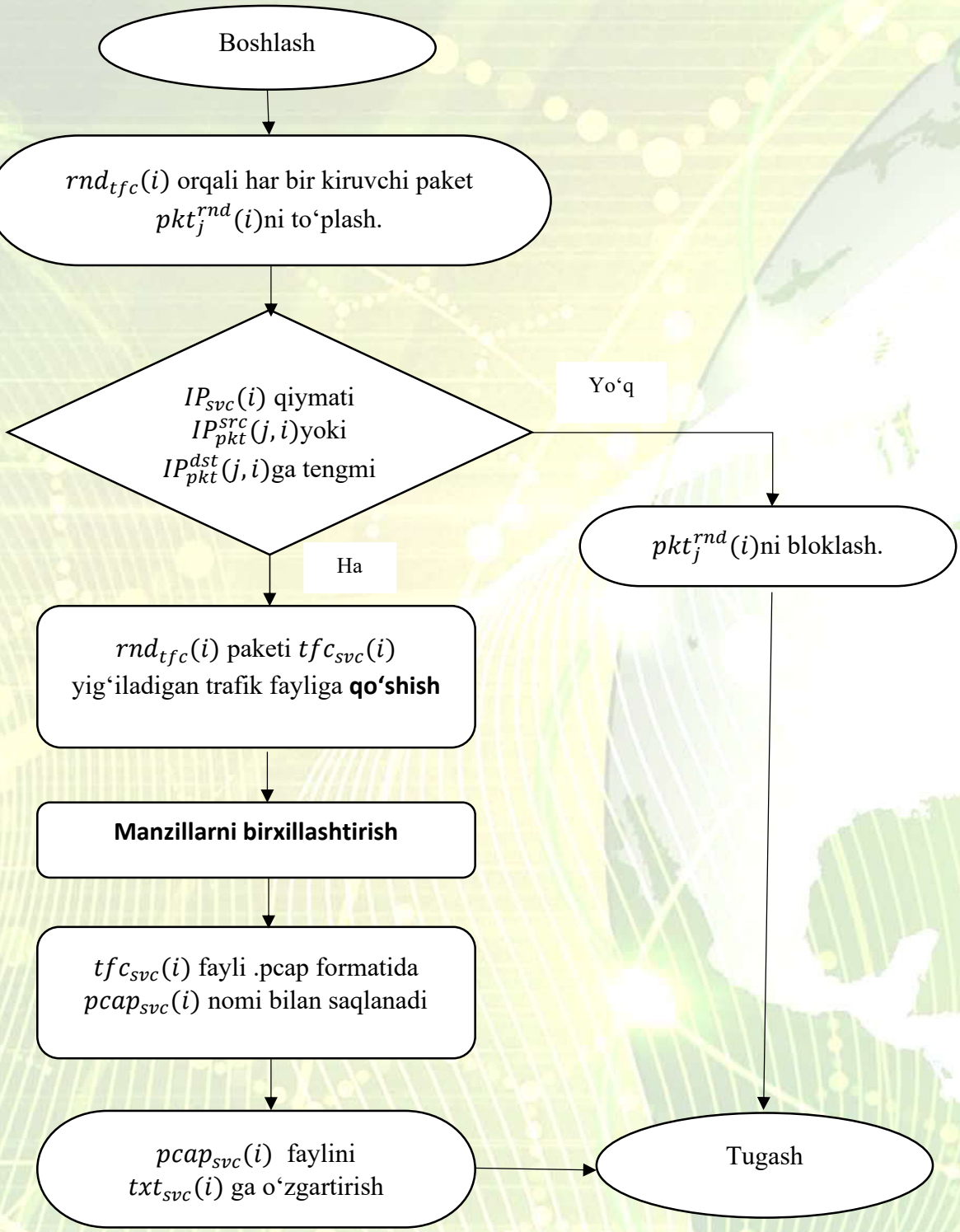
Formula	Tavsifi
svc_i	i^{th} xizmat

ISSN 3030-3907

$tfc_{svc}(i)$	svc_idagi har bir paketdan ma’lumot to‘plash
$rnd_{tfc}(i)$	i^{th} rounddagi $tfc_{svc}(i)$ yozuvlari
$pcap_{svc}(i)$	$tfc_{svc}(i)$ dagi PCAP yozuvlari
$txt_{svc}(i)$	$pcap_{svc}(i)$ ning tekst formatdagi fayli
$pkt_j^{rnd}(i)$	$rnd_{tfc}(i)$ dan j^{th} paket
$IP_{svc}(i)$	svc_i ning IP manzili
$MAC_{pkt}^{src}(j,i)$	$pkt_j^{rnd}(i)$ ning manba MAC manzili
$MAC_{pkt}^{dst}(j,i)$	$pkt_j^{rnd}(i)$ ning masofadagi MAC manzili
$IP_{pkt}^{src}(j,i)$	$pkt_j^{rnd}(i)$ ning manba IP manzili
$IP_{pkt}^{dst}(j,i)$	$pkt_j^{rnd}(i)$ ning masofadagi IP manzili

Birinchidan, mashinali o‘qitish modellari kirish ma’lumotlarining o‘lchami doimiy bo‘lishini talab qiladi, holbuki har bir paket uzunligi har xil bo‘lishi mumkin.

ISSN 3030-3907



4-rasm. Dinamik paketlarni boshqarish va manzillarni birxillashtirish algoritmining blok-sxemasi

Ikkinchidan, neyron tarmoqlar kirish ma’lumotlari o‘lchamiga juda sezgir; shuning uchun har bir paketdagi bayt qiymati 0–255 oralig‘idan 0–1 oralig‘iga o‘zgartirilishi kerak, buni quyidagi (1) formula yordamida bajariladi, shunda har bir bayt (xususiyat) modelga teng ta’sir ko‘rsatadi.

$$byte_k^{nrom}(j,i) = \frac{byte_k^{rec}(j,i)}{255} \qquad (1)$$

ISSN 3030-3907

Ma’lumotlarni oldindan qayta ishlashdan so‘ng olingan ma’lumotlar to‘plamiga asoslanib, autoencoder, 1D konvolyutsiya va teran neyron tarmog‘idan (DNN) iborat paket klassifikatorini qurish mumkin. Paket asosidagi klassifikator sifatida CAPC oqim xususiyatlarini yig‘ish uchun vaqt talab qilmaydi va to‘g‘ridan-to‘g‘ri olingan paket baytlaridan foydalanishi mumkin, dinamik paketlarni boshqarish va manzillarni birxillashtirish algoritmining blok-sxemasi 4-rasmda ko‘rsatilgan. Autoencoder katta hajmdagi kirish ma’lumotlarini siqib, kodlaydi[14].

Tenglamadagi belgilar 4-jadvalda tushuntirilgan.

4-jadval.

Tenglama tavsifi

Formula	Tavsifi
1	2
$txt_{tfc}^{nrom}(i)$	$txt_{svc}(i)$ ning normallashgan matn fayli
$rec_j^{text}(i)$	$txt_{svc}(i)$ ning j^{th} yozuvi
$len_{rec}(j,i)$	$rec_{tfcj}^{text}(i)$ dagi baytlar raqami
$byte_k^{rec}(j,i)$	$rec_j^{text}(i)$ ning k^{th} bayti
$byte_k^{nrom}(j,i)$	$byte_k^{rec}(j,i)$ ning normallashtirilgan bayti

ReLU funksiyasi (2):

$$ReLU(z) = \max[0, z] \qquad (2)$$

Bu funksiya kiruvchi z qiymatidan 0 dan kichik bo‘lganlarini 0 ga o‘zgartiradi, qolganlarini esa o‘zgartirmaydi.

CAPC modelidagi kodlovchi (encoder) uchta kodlash qatlamidan iborat bo‘lib, uning oxirgi qatlami max-pooling qatlamidir. Kodlovchidan keyin biriktirilgan neyron tarmoq - bu dekoder bo‘lib, uning tuzilishi kodlovchining teskari shaklidir.

Autoencoderning chiqish o‘lchami kirish o‘lchamiga teng bo‘lishi kerak. Shuning uchun, chiqish qatlamining maqsadli qiymatlari kirish qiymatlariga teng qilib o‘rnatiladi.

Dekoderning birinchi qatlami esa, kodlovchining oxiridagi max-pooling qatlamiga qarama-qarshi tarzda, up-sampling qatlami bilan boshlanadi, bu esa kodlovchining teskari tarmog‘ini yaratishga xizmat qiladi.

Oldindan o‘qitilgan 1D konvolyutsion encoderdan so‘ng DNN klassifikator qo‘shiladi. Shu sababli, encoder yaxshi boshlang‘ich nuqtasi bo‘lib, DNN klassifikatorining xizmatlarni toifalashida samarali ishlashini ta’minlaydi.

Encoder va klassifikator bog‘langan qatlam 1D konvolyutsion qatlam bo‘lib, klassifikator uchun kirish ma’lumotlariga tekislangan holatda beriladi.

ISSN 3030-3907

Kodlangan qiymatlar klassifikatorning kirishiga aylanadi.

5-jadval

Ochiq VPN ma’lumotlar to‘plami tavsifi

Xizmat turi	Paket turi	To‘liq soni	Tanlab olingan
AIM chat	real vaqtdagi matn	2,697	2,697
Elektron pochta mijozi	matn	21,297	10,000
Facebook audio	VoIP	199,272	10,000
Facebook chat	real vaqtdagi matn	12,605	10,000
Facebook video	real vaqtdagi video	98,663	10,000
FTP	fayl uzatish	237,455	10,000
Gmail chat	real-time text	8,417	8,417
Hangouts audio	VoIP	175,356	10,000
Hangouts chat	real vaqtdagi matn	24,415	10,000
Hangouts video	real vaqtdagi video	143,783	10,000
ICQ	real vaqtdagi matn	5,074	5,074
Netflix	video	27,442	10,000
SCP	fayl uzatish	45,385	10,000
SFTP	fayl uzatish	64,507	10,000
Skype audio	VoIP	142,490	10,000
Skype chat	real vaqtdagi matn	7,644	7,644
Skype file	fayl uzatish	154,849	10,000
Skype video	real vaqtdagi video	140,195	10,000
Spotify	musiqa	94,894	10,000
BitTorrent	P2P	67,428	10,000
Tor Twitter	web content	8,965	8,965
Vimeo	video	95,272	10,000
VoipBuster	VoIP	147,627	10,000
YouTube	video	217,345	10,000

Olingan natija va tahlillar. Ma’lumotlar to‘plamida to‘rtta asosiy xizmat turida jami 16 ta xizmat mavjud bo‘lib, har bir ilova uchun baholash maqsadida 10,000 ta paket olingan, jami 160,000 ta paket. Ushbu ma’lumotlar to‘plami to‘liq muvozanatlangan hisoblanadi, chunki har bir xizmat uchun namunalar soni bir xil. Boshqa tomondan, ommaviy ma’lumotlar to‘plamida 24 ta xizmat bor, ular orasida

ISSN 3030-3907

turli VPN yoki VPN bo‘lmagan shifrlangan turlar mavjud. Tadqiqotning maqsadi shundaki, ilova shifrlangan yoki shifrlanmaganidan qat’iy nazar, zararli tarfikni aniqlashdir. VPN va VPN bo‘lmagan trafik bitta ilovaga tegishli bo‘lsa ham, modelni o‘qitishda va sinovdan o‘tkazishda aralash holda ishlatiladi. Xizmatlarning soni muvozanatsiz bo‘lib, ba’zilari 100,000 dan ortiq, boshqalari esa 10,000 dan kam namunaga ega. Ma’lumotlarni imkon qadar muvozanatlash uchun har bir xizmat uchun eng ko‘pi bilan 10,000 ta namuna tasodifiy tanlab olinadi. Ma’lumotlar to‘plami o‘qitish va test maqsadlarida uch qismga bo‘linadi: o‘qitish, tekshirish va test ma’lumotlari, ularning har biri xizmat uchun namuna soniga muvofiq mos ravishda 70%, 10% va 20% nisbatda ajratilgan.

CAPC modelining samaradorligini isbotlash uchun uchta boshqa teran o‘qitish modeli qurilgan. Ular DNN, DAE va 1D CNN bo‘lib, bir qancha ilmiy ishlarda sinovdan o‘tgan va juda yaxshi natijalarga erishilgan. Biroq, ommaviy VPN ma’lumotlar to‘plami bo‘yicha bajarilgandagi tasniflash vazifalari mos ravishda faqat 17, 15 va 12 ta ilovani o‘z ichiga olgan. Ko‘proq murakkab (24 ta ilova) holatda yaxshiroq natija olish uchun taklif etilgan CAPC ushbu tadqiqotlarda ishlatilgan uchta model bilan solishtiriladi. DAE tuzilmasi DNNga o‘xshash, faqat unga autoencoder o‘qitishining qo‘shimcha jarayoni kiritilgan. CAPC esa 1D CNNga o‘xshash, faqat konvolyutsion qatlamlar oldindan tayyorlangan encoder asosida qurilgan. Har bir modelning kirish qatlami EthernetMTU hajmi sababli 1500 neyronlardan iborat, chiqish qatlami esa maqsad qilingankategoriyalar soniga bog‘liq (maxfiy ma’lumotlar uchun 16 va ommaviy ma’lumotlar uchun 24). Paketga asoslangan tasniflash modellari tarmoq muhitida ishlash imkoniyatini sinash uchun Mininet yordamida oddiy SDN muhiti yaratilgan[15]. Real vaqtda trafikni tasniflash uchun simulyatsiya qilingan tarmoq muhiti 5-rasmda keltirilgan.

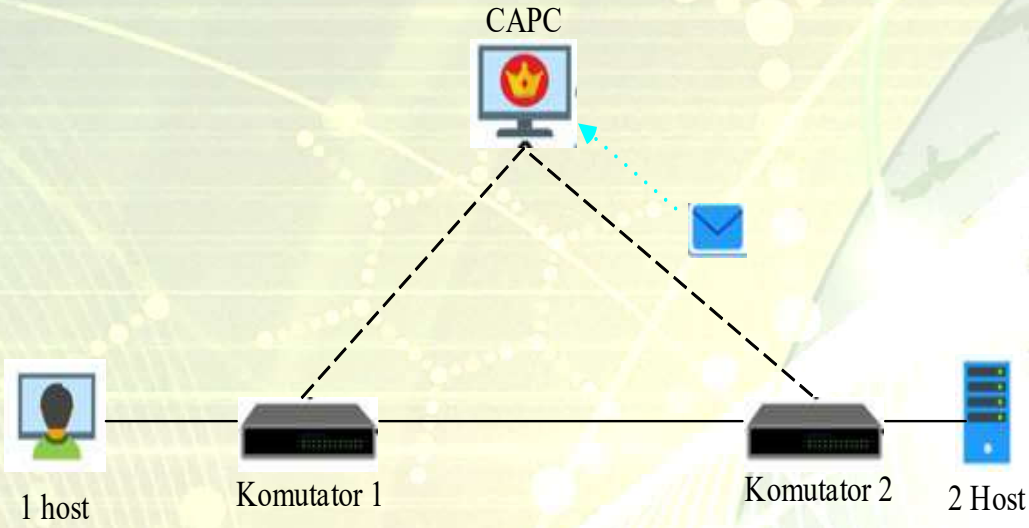
6-jadval

Uskuna va dasturiy ta’minot parametrlari

Qurilma va dastur	Xususiyatlari
1	2
CPU	Inter Core™ i7-4790 3.60GHz
GPU	NVIDIA GeFOrce GTX 1050 Ti 4G
GPU tezlashtirilgan vositalari	NVIDIA cuda 9.0.176
GPU tezlashtirilgan kutubxonasi	NVIDIA cuDNN 9.0
Tizim xotirasi	32 GB
Mashinali o‘qitish mexanizmi	TensorFlow-gpu 2.x
Mashinali o‘qitish mexanizmi	keras 2.1.5, scikit-learn 0.22.1
Ma’lumotlarni qayta ishlash	pandas 1.0.0, numpy 1.16.0
Trafikni to‘plash	Wireshark, tcpdump

ISSN 3030-3907

Paket modifikatori	tcprewrite 4.3.0
Paketlarni qayta ishlash kutubxonasi	libpcap 1.7.4
Video trafik generatori	VLC Media Player 3.0.8



5-rasm. Real vaqtda trafikni tasniflash uchun simulyatsiya qilingan tarmoq muhiti

XULOSA.

Ushbu muhit Ubuntu virtual mashinasida VMware serverda qurilgan. Tasniflash modellarini nazorat qiluvchi (controller) ichida joylashtirishgan va ular real vaqt rejimida kelayotgan paketlarni tasniflaydi. O‘zimiz tomonidan to‘plangan PCAP fayllari 2-xostda saqlangan (masalan, FTP, Skype VoIP va Windows RDP trafiklari). Trafikni qayta yo‘naltirish uchun BitTwist vositasi ishlatilgan. Xost 2-dan saqlangan trafik fayllari qayta yo‘naltiriladi. Birinchi kelayotgan paket preinstallyatsiya qilingan qoida asosida komutator (sw2) orqali controllerga packet-in xabari sifatida yuboriladi. Controllerga kelgan paket modellar tomonidan filtrlanadi va har bir model uchun tasniflashga ketgan vaqt yozib olinadi hamda taqqoslash uchun ishlatiladi. Yuqorida taklif etilgan neyron tarmoqlariga asoslangan paketlarni dinamik filtrlash usuli va algoritmi asosida tarmoq paketlarini samarali dinamik filtrlash jarayonining ishlash algoritmi ishlab chiqiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, 2020. - *8*, 222310-222354.

2. Çelebi, M., Özbilen, A., & Yavanoğlu, U. A comprehensive survey on deep packet inspection for advanced network traffic analysis: issues and challenges. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 2023. - 12(1), 1-29.

ISSN 3030-3907

3. Berahmand, K., Daneshfar, F., Salehi, E. S., Li, Y., & Xu, Y. Autoencoders and their applications in machine learning: a survey. Artificial intelligence review, 2024. - 57(2), 28.
4. De Keersmaeker, F., Cao, Y., Ndonda, G. K., & Sadre, R. A survey of public IoT datasets for network security research. IEEE Communications Surveys & Tutorials, 2023. - 25(3), 1808-1840.
5. Kurani, A., Doshi, P., Vakharia, A., & Shah, M. A comprehensive comparative study of artificial neural network (ANN) and support vector machines (SVM) on stock forecasting. Annals of Data Science, 2023. - 10(1), 183-208.
6. Costa, V. G., & Pedreira, C. E. Recent advances in decision trees: an updated survey. *Artificial Intelligence Review*, 2023. - *56*(5), 4765-4800.
7. Sharkawy, A. N. Principle of neural network and its main types. *Journal of Advances in Applied & Computational Mathematics*, 2020. - *7*, 8-19.
8. Papadogiannaki, E., & Ioannidis, S. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. ACM Computing Surveys (CSUR), 2021. - 54(6), 1-35.
9. Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R., & Saberian, M. Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Computing, 2020. - 24(3), 1999-2012.
10. Khan, A., Sohail, A., Zahoora, U., & Qureshi, A. S. A survey of the recent architectures of deep convolutional neural networks. Artificial intelligence review, 2020. - 53(8), 5455-5516.
11. Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R., & Saberian, M. Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Computing, 2020. - 24(3), 1999-2012.
12. T.S.Norboboevich, Y.B.Karamatovich and N. I. Ibrohimovich, "Verification of the pocket filtering based on method of verification on the model," 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-3, doi: 10.1109/ICISCT47635.2019.9011901.
13. Salman, O., Elhajj, I. H., Kayssi, A., & Chehab, A. A review on machine learning–based approaches for Internet traffic classification. Annals of Telecommunications, 2020. - 75(11), 673-710.
14. Ge, T., Hu, J., Wang, L., Wang, X., Chen, S. Q., & Wei, F. In-context autoencoder for context compression in a large language model. 2023. - *arXiv preprint arXiv:2307.06945*.

ISSN 3030-3907

15. Linhares, T., Patel, A., Barros, A. L., & Fernandez, M. SDNTruth: innovative DDoS detection scheme for software-defined networks (SDN). *Journal of Network and Systems Management*, 2023. - *31*(3), 55.

ISSN 3030-3907