TARMOQ TRAFIGINI BOSHQARISH VA TAHLIL QILISH MUAMMOLARI

Tojiyeva Feruza Qobiljon qizi
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari Infokommunikatsiya injinering kafedrasi doktoranti
E-mail: 11feruza@gmail.com
Mirzayeva Malika Bahadirovna
"Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" Milliy tadqiqot universiteti, Raqamli texnologiyalar va sun'iy intellekt kafedrasi dotsenti
E-mail: malikamirzaeva01@gmail.com

Annotatsiya: Maqolada Internet trafigini boshqarish va tahlil qilish bilan bog'liq dolzarb muammolar ko'rib chiqilgan. Unda avtonom tizimlarning ierarxik tuzilmasi, ichki va tashqi domenlarda trafikni nazorat qilishning o'ziga xosliklari tahlil qilinadi. Trafik tahlilining to'rtta agregatsiya darajasi IP-paket, oqim (flow), manba-manzil oqimi (OD-flow) va kanal darajasi misolida tahlil mexanizmlari yoritiladi. DPI, NetFlow, SNMP texnologiyalari asosida samarali monitoring usullari ko'rib chiqilgan. Tadqiqot natijalari tarmoq xavfsizligi va xizmat sifati oshirishda muhim amaliy ahamiyatga ega.

Kalit so'zlar: trafigini tahlil qilish, tarmoq boshqaruvi, avtonom tizimlar, DPI, NetFlow, SNMP, agregatsiya darajalari, anomal holatlar, trafik oqimi.

Аннотация: В статье рассматриваются актуальные проблемы управления и анализа интернет-трафика. Изучается иерархическая структура автономных систем, особенности контроля трафика на внутреннем и междоменном уровнях. Раскрываются четыре уровня агрегации трафика IP-пакет, поток, OD-поток и канальный уровень. Также анализируются методы глубокого анализа пакетов (DPI), NetFlow и SNMP. Полученные результаты имеют важное практическое значение для повышения качества обслуживания и сетевой безопасности.

Ключевые слова: анализ трафика, управление сетью, автономные системы, DPI, NetFlow, SNMP, уровни агрегации, аномалии, сетевой поток.

Abstract: The article discusses current challenges in network traffic management and analysis. It explores the hierarchical structure of autonomous systems and the peculiarities of traffic control at intra- and inter-domain levels. Four aggregation levels IP packet, flow, origin-destination flow, and link-level are analyzed in detail. Methods based on DPI, NetFlow, and SNMP technologies are reviewed. The

ISSN 3030-3907

research findings provide practical value for improving network reliability, traffic monitoring, and service quality.

Keywords: traffic analysis, network management, autonomous systems, DPI, NetFlow, SNMP, aggregation levels, anomalies, traffic flow.

Kirish

Bugungi kunda Internet texnologiyalarining jadal rivojlanishi natijasida foydalanuvchilarning tezkor, ishonchli va yuqori sifatli xizmatlarga bo‘lgan ehtiyoji sezilarli darajada ortmoqda. Real vaqt rejimida ishlovchi multimedia ilovalari, bulutli tizimlar, video oqimlar, hamda katta hajmdagi ma’lumotlar almashinuvining barchasi zamonaviy tarmoq infratuzilmasiga yuqori yuklama tushiradi va uni samarali boshqarish, tahlil qilish zaruratini oshirmoqda.

Tarmoq trafigining hajmi nafaqat ortmoqda, balki uning tarkibi ham murakkablashib bormoqda. Xizmatlar sonining ko‘payishi, shifrlangan va heterogen trafik oqimlarining ko‘pligi, turli xizmatlar tomonidan yaratilgan trafikning turfa xususiyatlari tarmoq muhitida resurslarni optimal taqsimlash va xizmatlar sifati (QoS)ni ta’minlash vazifasini yanada murakkablashtiradi.

Shu sababli, yirik tarmoq operatorlari va tadqiqotchilar tomonidan trafigini chuqur tahlil qilish, oqimlarning xarakterini aniqlash, trafik sinflarini avtomatik aniqlash va prioritetlashga oid ilg‘or algoritmlar va modellarni ishlab chiqish muhim strategik yo‘nalishga aylanmoqda.

Shuningdek, trafikni oqim darajasida (flow-level) tahlil qilish, uning yo‘nalishini aniqlash va asosli sinflarga ajratish, tarmoqni yanada samarali loyihalash va optimallashtirish imkonini beradi.

Shu nuqtai nazardan, ushbu maqolada tarmoq trafigini boshqarish va tahlil qilishning zamonaviy muammolari, mavjud yondashuvlarning afzalliklari va kamchiliklari, shuningdek, istiqbolli tadqiqot yo‘nalishlari keng qamrovda yoritiladi.

ADABIYOTLAR TAHLILI

Tarmoq trafigini aniqlash, kuzatish va modellashtirish bo‘yicha yondashuvlardan biri Feldmann[1] tadqiqotlarida IP tarmoqlarda real trafik talablarini aniqlash bo‘yicha amaliy yondashuv va metodik yechimlarni taklif qilishgan.

Maqolada trafik oqimlarini aniqlash uchun router darajasidagi tarmoq topologiyasi, trafik matritsalari, yo‘nalishlar (routing paths) va monitoring jarayonlari asosida statistik modellar qurilgan. Tadqiqotchilar IP tarmog‘i bo‘ylab oqimlar qanday taqsimlanishini aniqlash uchun NetFlow passiv monitoring texnologiyalarini qo‘llashgan.

ISSN 3030-3907

Ushbu uslubning asosiy afzalliklari to‘g‘ridan-to‘g‘ri trafikni o‘lchamasdan uning ichki xususiyatlarini modellashtirish imkoniyatidir. Bu esa yirik ISP (Internet Service Provider) tarmoqlari uchun muhim ahamiyat kasb etadi, chunki real trafikni har doim bevosita o‘lchashning imkoni bo‘lmaydi yoki bu juda katta resurs talab qiladi. Mazkur tadqiqot bugungi kunda tarmoq trafigini nazorat qilish, rejalashtirish va optimallashtirish bo‘yicha nazariy hamda amaliy manba sifatida qaraladi.

Feldmann[2] Web trafik talablarini bashorat qilish uchun innovatsion metodologiya taqdim etilgan. Ular aynan server loglari va packet traces integratsiya qilgan holda CDN orqali yuklangan sahifalar va unga bog‘lanib kelgan obyektlar hajmini tahlil qilishgan.

Ushbu metodologiya CDN orqali ishlashni o‘z boshlanishida tahlil qiladi, lekin server-loglarga asoslangan model orqali CDN tashqarisidagi obyektlarni ham aniqlaydi.

Geografik ma'lumotlar va BGP marshrutlash jadvallarini birlashtirib, turli mamlakatlar va AS’lar bo‘yicha trafik paternlari o‘rganiladi. Tadqiqot natijalari Interdomain trafikni, uning vaqt davomida barqarorligi va ASlararo trafik dinamikasini tahlil qilishda asosiy resurs vazifasini o‘taydi. Ilgari mavjud bo‘lmagan interdomain trafik matritsalarini yaratish orqali ilmiy va amaliy jihatdan trafikni boshqarish, tarmoqni rejalashtirish va axborot xavfsizligini yaxshilash uchun imkoniyatlar beriladi.

Zhang[3] NetFlow ma’lumotlariga asoslangan tarmoq trafigini chuqur o‘rganish (Deep Learning) yordamida tasniflash muammosini ko‘rib chiqishgan. An’anaviy uslublar shifrlangan trafikda samarasiz bo‘layotgani sababli, tadqiqotda chuqur neyron tarmoqlar (Deep Neural Networks, DNN) asosida model taklif qilingan. Ushbu model real trafik ma’lumotlari asosida sinovdan o‘tkazilib, 1,4 million holat bo‘yicha o‘rtacha 95% aniqlik natijasi qayd etilgan. Bundan tashqari, taklif etilgan metod boshqa uchta zamonaviy klassifikatorga nisbatan ustunligi bilan ajralib turadi.

Modelning afzalligi NetFlow ma’lumotlari yordamida trafikni shifrlangan sharoitda ham aniqlay oladi, bu esa xavfsizlik monitoringi, trafik hisobi, QoS va trafik prognozlash kabi sohalarda qo‘llash imkonini beradi. Ushbu tadqiqot ayniqsa yirik tarmoq operatorlari uchun muhim ahamiyat kasb etadi.

Chen[4] tomonidan taklif etilgan MIETT (Multi-Instance Encrypted Traffic Transformer) modeli shifrlangan tarmoq trafigini tasniflashdagi mavjud muammolarga zamonaviy transformer arxitekturasi asosida yechim taklif etadi. Ular an’anaviy token-level tahlil uslublarining cheklovlarini ko‘rsatib, oqim

ISSN 3030-3907

darajasidagi packetlararo o‘zaro bog‘liqliklarni e’tiborga oladigan ko‘p-instansli o‘rganish (multi-instance learning) yondashuvini joriy etganlar.

Ushbu model har bir tarmoq oqimini paketlar to‘plami sifatida ko‘radi va Two-Level Attention (TLA) mexanizmi orqali har bir paket va oqim darajasidagi dinamikalarni o‘rganadi. Bundan tashqari, Packet Relative Position Prediction (PRPP) va Flow Contrastive Learning (FCL) kabi pre-trening vazifalari yordamida model vaqt bo‘yicha va oqim xususiyatlariga sezgir bo‘ladi. Bu esa modelga shifrlangan trafikdagi murakkab naqshlarni aniqlashda ustunlik beradi.

MIETT modeli beshta turli trafik datasetlarida testdan o‘tkazilib, ilgari mavjud bo‘lgan modellar bilan solishtirilganda eng yuqori aniqlikka (SOTA) erishgan. Bu yondashuv ayniqsa payload mavjud bo‘lmagan shifrlangan trafikni faqat oqim xatti-harakatlariga asoslanib tasniflash vazifasida dolzarb yechim sifatida baholanadi.

Liu va hammualliflar tomonidan taqdim etilgan TransECA-Net modeli [5] shifrlangan trafikni sinflashtirish uchun gibrid yondashuvni taklif etadi. Ushbu modelda CNN va Transformer arxitekturasi birlashtirilib, ECANet moduli yordamida trafik oqimlaridan muhim atributlar avtomatik tarzda ajratiladi va vaqt bo‘yicha global bog‘liqliklar aniqlanadi. Tajriba natijalari ISCX VPN-nonVPN to‘plamida o‘tkazilgan bo‘lib, TransECA-Net modeli klassik modellarga nisbatan yuqori aniqlik (98.25%) va tezroq konvergentsiya (37.4% gacha) ko‘rsatgan.

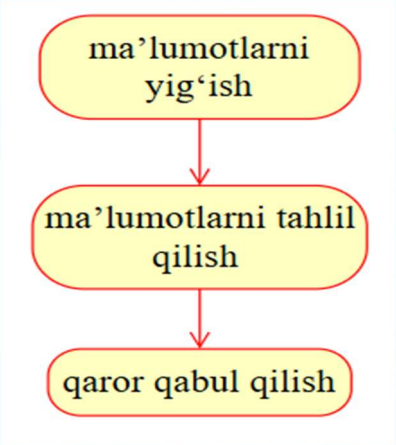
Mazkur yondashuvning afzalligi, yuqori aniqlik bilan real vaqtda trafik monitoring imkoniyati, shuningdek, chuqur o‘rganish texnikalarining samarali uyg‘unlashtirilganidir. TransECA-Net modeli shifrlangan trafikni tahlil qilishda dolzarb yechimlardan biri sifatida ko‘rilmoqda.

TADQIQOT METODOLOGIYASI

Trafikni nazorat qilish - tarmoq operatorlari uchun asosiy vazifalardan biridir, chunki butun tarmoq bo‘ylab trafik haqida ma’lumot olish juda murakkab va katta hajmdagi ma’lumotlar juda qimmatga tushadi. Tarmoqlar rivojlanishining dastlabki bosqichlarida trafik nazorati asosan “qo‘lda” trafik hajmi va yo‘nalishlarini aniqlashga asoslangan bo‘lib, bu ko‘proq operatorlar tajribasi va bilimlariga bog‘liq edi. Ammo so‘nggi yillarda avtomatlashtirilgan va katta hajmdagi trafikni qayta ishlay oladigan murakkab tizimlar ishlab chiqilmoqda.

Internet-provayderlar (ISP - Internet Service Provider) tomonidan trafikni nazorat qilish tizimlari ishlab chiqilishi va tarmoqni rejalashtirish va loyihalash jarayonlarini yaxshilashda qo‘llanilishi mumkin. Trafikni nazorat qilish jarayoni quyidagi uchta bosqichdan iborat (1-rasm).

ISSN 3030-3907



1-rasm. Trafikni nazorat qilish jarayoni

Har bir bosqich yuqorida ta’riflangan ssenariyda trafik hajmining ortib borishi sababli tobora muhim bo‘lib bormoqda.

Ma’lumotlarni yig‘ish bu murakkab jarayon bo‘lib, tarmoqning turli segmentlarida to‘planadigan katta hajmdagi ma’lumotlar bilan bog‘liq.

Ma’lumotlarni tahlil qilish bu murakkab jarayon, chunki tarmoq trafigining sezilarli darajadagi notekisligi tufayli tarmoqda ko‘plab ziddiyatli holatlar, to‘qnashuvlar yuzaga kelishi mumkin.

Qaror qabul qilish esa muhim va tanqidiy bosqich hisoblanadi, chunki hozirgi vaqtda Internetda taqdim etilayotgan xizmatlar turli xil va muhim ahamiyatga ega.

Internet juda tez rivojlanayotganiga qaramay, uning butun dunyo bo‘yicha tuzilishi hanuzgacha pog‘onali (ierarxik) shaklda saqlanib qolmoqda. Bu tuzilmada eng yuqori darajada joylashgan asosiy markazlar - avtonom tizimlar (inglizcha nomi: Autonomous Systems, qisqacha AS) bo‘lib, ular Tier 1 (Birinchi darajali tarmoq operatorlari) deb ataladi. Tier 1 Eng yuqori darajadagi Internet provayderlari bo‘lib, ular global miqyosda Internet aloqalarini ta’minlaydi, Barcha boshqa tarmoqlar (Tier 2, Tier 3) ularning tarmoqlariga ulanadi.

Avtonom tizim deganda - bitta yirik tarmoq operatori tomonidan boshqariladigan tarmoq qismi tushuniladi. Bu tarmoq o‘ziga tegishli IP manzillarga ega bo‘ladi va butun tarmoq bo‘ylab bitta yagona yo‘naltirish (marshrutlash) siyosatiga amal qiladi.

Oddiy qilib aytganda, AS bu - yirik tarmoq markazi, u o‘z yo‘nalish siyosatini mustaqil belgilaydi va boshqa tarmoqlarga ham Internetga chiqish imkonini beradi. Bunday tizimlar odatda katta hududni qamrab oladi va yuzlab yoki minglab foydalanuvchilarga xizmat ko‘rsatadi.

Tier 1 darajasiga mansub tarmoq operatorlari - bu global Internet infratuzilmasining eng muhim ishtirokchilari hisoblanadi. Ular dunyo bo‘ylab

ISSN 3030-3907

Internet tarmoqlarining o‘zaro bog‘lanishini ta’minlaydi va o‘zaro ma’lumot almashishda bir-biriga tranzit to‘lovi (ya’ni pul) to‘lamaydi.

Boshqacha aytganda, Tier 1 operatorlar - bu Internetning “magistral yo‘llari” bo‘lib, ularning tarmoqlari orqali pastki darajadagi operatorlar (masalan, Tier 2 yoki Tier 3) global Internetga ulanadi. Ushbu pastki darajadagi tarmoqlar esa Tier 1 operatorlaridan xizmat sotib oladi yoki ularga bog‘lanadi[6,7].

Hozirgi kunda Tier 1 darajasiga kiruvchi yirik va nufuzli operatorlar soni juda kam bo‘lib, ularga quyidagilar kiradi:

AT&T
Global Crossing (GLBC)
NTT Communications
Sprint
Tata Communications
Verizon Business (UUNET)
Savvis
TeliaNet
Bell Canada
XO Communications (XOXO)

Mazkur yirik operatorlar Internetdagi global trafik oqimini boshqarishda asosiy rol o‘ynaydi. Ularning barqaror va ishonchli ishlashi butun dunyo bo‘yicha Internet tarmog‘ining sifatli va uzluksiz faoliyat yuritishini ta’minlaydi.

Tier 1 darajasidagi internet-provayderlar (ISP) - bu Internet infratuzilmasining eng yuqori pog‘onasida joylashgan yirik tarmoqlar bo‘lib, ular global bog‘lanishni ta’minlovchi asosiy uzel (markaz) hisoblanadi.

Ulardan pastroq pog‘onada esa Tier 2 va Tier 3 darajasidagi provayderlar mavjud bo‘lib, ular ko‘proq mintaqaviy yoki mahalliy tarmoq operatorlari hisoblanadi. Bu pastki darajadagi provayderlar global Internetga chiqish uchun Tier 1 operatorlariga ulanadi yoki ularning xizmatlaridan foydalanadi.

Bundan tashqari, mahalliy topologiyaga ega bo‘lgan, mustaqil tarzda ishlaydigan avtonom tizimlar (AS) ham mavjud bo‘lib, ular odatda chekka (periferik) AS’lar deb ataladi. Ular odatda faqat o‘z ichki tarmog‘ida xizmat ko‘rsatadi yoki bir necha yirik provayder orqali tashqi tarmoqlarga ulanadi.

Umuman olganda, butun Internet strukturasida avtonom tizimlar ikki asosiy ko‘rinishda mavjud:

1. Ichki (intra-AS) tizimlar - bu bitta tarmoq operatori tomonidan boshqariladigan yagona tarmoq, ya’ni ichki marshrutlash siyosati asosida ishlaydi.

ISSN 3030-3907

2. Tashqi (inter-AS) tizimlar - bu turli operatorlar o‘rtasida bog‘langan tarmoqlar bo‘lib, ular tashqi marshrutlash protokollari orqali o‘zaro ma’lumot almashadi.

Trafik va tarmoq nazorati odatda har bir yirik avtonom tizim (AS) ichida amalga oshiriladi. Bu ichki darajada nazorat qilish nisbatan osonroq, chunki bunday tizimlarda tarmoq infratuzilmasi aniq belgilangan va yaxshilab strukturalashtirilgan bo‘ladi. Ammo tashqi darajada, ya’ni turli avtonom tizimlar o‘rtasida trafikni boshqarish ancha murakkab. Sababi, bu hududda tarmoq topologiyasi boshqa operatorlar tomonidan boshqariladi va yuzaga kelgan muammolarni hal qilish imkoniyatlari chegaralangan bo‘ladi[8].

Natijada, tarmoqning ichki va tashqi qismlari o‘rtasida turli noaniqliklar, resurs cheklovlari hamda boshqaruvdagi muvofiqlik muammolari paydo bo‘ladi. Bu ayniqsa, o‘zaro bog‘lanmagan, mustaqil ishlaydigan va o‘zining alohida siyosatiga ega bo‘lgan tarmoq operatorlari o‘rtasida yanada keskinlashadi.

Ma’lumki, tashqi operatorlar o‘rtasida to‘liq va erkin ma’lumot almashinuvi har doim ham mavjud emas. Bundan tashqari, har bir operator turli nazorat mexanizmlaridan foydalangani uchun ular o‘rtasidagi muvofiqlik va integratsiya jarayonlari ko‘pincha murakkab va sust bo‘ladi.

Shu sababli, domenlararo trafikni nazorat qilish, ya’ni trafik oqimini bir nechta avtonom tizimlar (AS) o‘rtasida boshqarish texnik va tashkiliy jihatdan ancha murakkab jarayon hisoblanadi. Har bir tizim o‘zining mustaqil siyosati va cheklovlariga ega bo‘lgani uchun, bunday holatda samarali nazorat o‘rnatish qiyinlashadi.

Shuning uchun ham, ko‘pchilik holatlarda trafikni boshqarish va tahlil qilish e’tibori ichki domen (ya’ni bitta AS doirasida) darajasiga qaratiladi.

Birinchidan, aynan ichki domen doirasida tarmoq operatori barcha tizim resurslariga ega bo‘lib, trafikni to‘liq nazorat qilish va muvofiqlashtirilgan qarorlar qabul qilish imkoniyatiga ega bo‘ladi.

Ikkinchidan, Internetning hozirgi global tuzilmasi hali ham oz sonli yirik avtonom tizimlarga tayanadi. Shu sababli butun Internetning ishlash barqarorligi va samaradorligi ana shu yirik AS’larning ishonchli va optimallashgan faoliyatiga bevosita bog‘liqdir.

Tarmoq operatorlari odatda o‘z tarmoqlarining barqaror va ishonchli ishlashiga xavf soluvchi turli xil noodatiy (anomal) hodisalar bilan tez-tez to‘qnash keladi.

Bunday holatlarni aniqlashdagi asosiy muammo shundaki, anomaliyalar doimiy ravishda o‘zgarib boradi ularning yuzaga kelish sabablari ham, ko‘rinish shakllari ham vaqt o‘tishi bilan yangilanadi yoki murakkablashadi.

ISSN 3030-3907

Tarmoq va trafikdagi buzilishlar quyidagi omillar natijasida yuzaga kelishi mumkin:

- Uskunalarning ishdan chiqishi (masalan, router yoki switch'larning nosozligi);
- Noto'g'ri konfiguratsiyalar yoki elektr ta'minotidagi uzilishlar;
- Foydalanuvchilarning kutilmagan yoki g'ayrioddiy xatti-harakatlari, masalan, juda katta hajmdagi trafik yoki to'satdan ko'paygan talablar;
- Marshrutlash (routing) jarayonidagi tashqi o'zgarishlar, ya'ni yo'naltirish qoidalarining o'zgarishi;
- Tarmoq hujumlari, jumladan:

✓ DoS (Denial of Service) hujumlari,
✓ Skanerlash va port probing,
✓ Zararlovchi dasturlar va viruslar orqali buzilishlar;

- Shuningdek, ilgari kuzatilmagan va noma'lum yangi hodisalar.

Bunday hodisalarni aniqlash va oldini olish uchun tarmoqni doimiy monitoring qilish, zamonaviy tahlil usullarini qo'llash va moslashuvchan xavfsizlik siyosatini yuritish muhim hisoblanadi.

Ushbu hodisalarni aniqlashdagi asosiy muammolardan biri shundaki, tarmoqdagi nosozliklar doimiy harakatda bo'lgan nishonlar kabi ular aniq bir joyda yoki aniq bir shaklda bo'lmaydi, doim o'zgarib turadi.

Bu esa ularni aniqlashni juda murakkablashtiradi, ayniqsa nosozliklar muntazam yangilanadigan va turli ko'rinishda paydo bo'ladigan hollarda.

Shu bilan birga, zararli trafikning yangi turlari ham doimiy ravishda paydo bo'lmoqda. Bunday vaziyatda oddiy, oldindan belgilangan qoidalar yoki anomaliyalar ro'yxatiga tayanadigan tizimlar yetarli bo'lmaydi.

Shuning uchun, trafikni tahlil qiluvchi zamonaviy tizimlar faqat avvaldan ma'lum bo'lgan nosozlik belgilariga emas, balki yangi va noma'lum anomal holatlarga ham moslasha oladigan moslashuvchan algoritmlarga ega bo'lishi zarur.

Tarmoqdagi trafikni tahlil qilish va nosozliklarni aniqlashda trafikning qanday darajada kuzatilayotgani ya'ni agregatsiya darajasi muhim rol o'ynaydi. Turli darajadagi agregatsiya orqali trafikni har xil aniqlikda baholash va turli tahlil usullarini qo'llash mumkin.

Trafik agregatsiyasining to'rtta asosiy darajasi mavjud bo'lib ular quyidagilar:

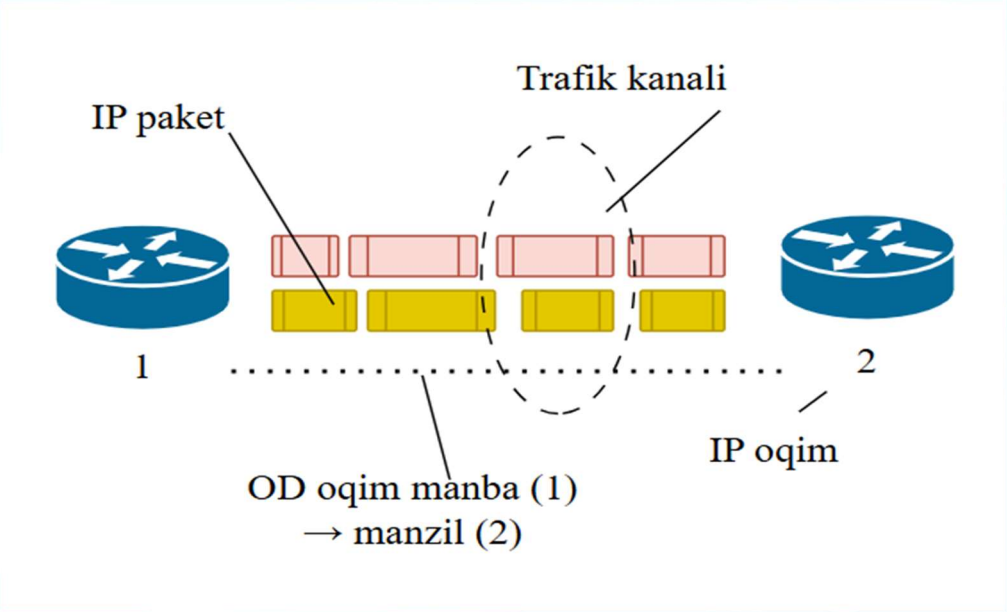
1. IP-paket darajasi - eng past, ya'ni eng aniq (detallangan) daraja. Bu yerda har bir paket alohida ko'riladi.
2. IP-oqim (IP-flow) darajasi - bir xil atributlarga ega bo'lgan ketma-ket paketlar guruhi.

ISSN 3030-3907

3. Manba-manzil oqimi (OD-flow) - ma’lum bir manba tugun va manzil tugun o‘rtasidagi umumiy trafik.

4. Kanal trafik darajasi (link-level traffic) - butun tarmoq bo‘ylab muayyan kanallar orqali oqayotgan umumiy trafik.

Har bir daraja ma’lumotlarni qay darajada chuqur tahlil qilish mumkinligini belgilaydi. Agregatsiya darajasi past bo‘lsa, aniqlik yuqori bo‘ladi, lekin resurs talabi ham ortadi. Yuqori agregatsiya esa umumiy ko‘rinishni beradi, lekin mayda anomaliyalarni yashirib qo‘yishi mumkin[9].



2-rasm.Trafik agregatsiyasining darajalari

Paket darajasida trafikni tahlil qilish bu eng past (ya’ni eng mayda) agregatsiya darajasi bo‘lib, trafikning har bir IP-paketi alohida ko‘rib chiqiladi. Bu usul aniqlik darajasi juda yuqori bo‘lgan tahlilni amalga oshirish imkonini beradi, chunki paket ichidagi foydali yuk (payload) va nazorat ma’lumotlariga to‘g‘ridan-to‘g‘ri kirish mumkin bo‘ladi.

Paket darajasidagi tahlil odatda xavfsizlik, trafik sinflashtirish yoki chuqur kontent tahlili kabi sohalarda qo‘llaniladi. Aynan shu darajadagi tahlil uchun ko‘plab algoritmlar va uslublar ishlab chiqilgan.

Ular orasida eng mashhurlari:

- DPI (Deep Packet Inspection) - IP-paketning tarkibini (foydali yukini) chuqur tahlil qilish orqali trafik turini aniqlaydi;
- Paket imzolari (Packet signature) - oldindan ma’lum andozalar (imzolar) asosida trafikni tanib olishni ta’minlaydi.

Shu bilan birga, ushbu darajadagi tahlil resurslar talab qiladi va shifrlangan trafik mavjud bo‘lganda, paket tarkibiga kirish imkoni cheklangan bo‘ladi.Ko‘plab trafikni tasniflash usullari aynan shu daraja uchun ishlab chiqilgan. Jumladan:

- Chuqur paket tekshiruvi (DPI – Deep Packet Inspection)

ISSN 3030-3907

- Paket imzolari asosidagi texnologiyalar
- Sniffing (trafikni tinglash) usullari

IP-paketlar kuzatuv nuqtalarida to‘plangan holda trafik oqimlari (flow) sifatida tahlil qilinishi mumkin. Bunday hollarda yagona analiz qilinadigan birlik bu oqim (flow) bo‘ladi.

IP-oqimlar, NetFlow texnologiyasi asosida tahlil qilinadi. Bu usul paketlar darajasidagi chuqur tahlilga qaraganda kamroq hisoblash resurslarini talab qiladi va eng yaxshi natija va samaradorlikni beradi.

OD-oqimlar (Origin-Destination flow) manba va manzil o‘rtasidagi barcha oqimlar majmuasidan iborat.

Bunda, manba tuguni 1 bo‘lsa va manzil tuguni 4 bo‘lsa, barcha oqimlar shu ikki tugun o‘rtasida OD-oqim sifatida birlashtiriladi.

OD-oqimlar IP-oqimlarga qaraganda kamroq aniqlikda bo‘ladi, ammo tarmoq monitoringi va boshqaruvining ko‘plab muammolari uchun ularning aniqligi yetarli hisoblanadi.

OD-oqimlar agregatsiyasi odatda IP-oqimlar nazoratiga qaraganda ancha soddalashgan, chunki asosiy e’tibor trafik hajmi va IP-manzillar jufti o‘rtasidagi umumiy oqimga qaratiladi (masalan, NetFlow asosida) [1].

OD-trafigining umumiy hajmi ikki tugun (uzel) o‘rtasida o‘lchanadi. Bu hajm kanalning fizik o‘tkazuvchanligi bilan bog‘liq bo‘lib, uni baholash oson.

Nihoyat, trafik agregatsiyasining eng yuqori darajasi bu trafik kanallari darajasidir. Bu usul butun tarmoqni global tarzda modul tuzilmalarda nazorat qilish va trafikni yo‘naltirishga imkon beradi.

Global darajadagi QoS (Quality of Service)ni pasaytiruvchi anomal trafikni aniqlash va oldini olishda bu muhimdir.

Tarmoqdagi anomal holatlar, paketlar yo‘qolishi yoki ortiqcha kechikishlar orqali yuzaga keladi. Shuning uchun trafik monitoringi tizimlari faqat aniqlash bilan cheklanmasdan, anomaliyalar joylashuvini aniqlash va oldini olish choralarini ham ko‘rishi kerak.

MUHOKAMA VA NATIJALAR

Tadqiqot davomida tarmoq trafigini tahlil qilishning dolzarb muammolari va ularni hal qilishda qo‘llanilayotgan usullar ko‘rib chiqildi. Trafikni real vaqtda kuzatish, tahlil qilish hamda sinflashtirish imkonini beruvchi zamonaviy texnologiyalar, xususan, chuqur o‘rganish (deep learning) modellari orqali aniqlikni oshirishga erishilmoqda.

O‘rganilgan tadqiqotlar shuni ko‘rsatadiki, an’anaviy usullar shifrlangan trafikni aniqlashda tobora samarasiz bo‘lib bormoqda. Shu sababli, transformatorlarga asoslangan yondashuvlar, avtomatik atribut ajratish va ko‘p

ISSN 3030-3907

bosqichli o‘rganish texnikalari orqali real vaqtda trafikni yuqori aniqlikda sinflashtirish imkoniyati yaratilmoqda.

Ushbu maqola doirasida tarmoq trafigi bilan bog‘liq asosiy muammolar trafik hajmining ortishi, shifrlangan trafikning keng tarqalishi va trafik oqimlarining noaniqligi yechimga muhim yo‘nalishlar sifatida ko‘rsatildi. Tahlillar bu muammolarga texnologik javoblar shakllanayotganini, ammo ularni real tarmoqlarda qo‘llash uchun moslashtirish va samaradorlikni oshirish hali dolzarbligicha qolayotganini tasdiqlaydi.

XULOSA VA TAKLIFLAR

Tarmoq trafigini boshqarish va tahlil qilish bugungi kunda yuqori sifatli, uzluksiz va xavfsiz Internet xizmatlarini taqdim etishda asosiy omillardan biri hisoblanadi. Internet infratuzilmasi ierarxik tuzilishga ega bo‘lib, Tier 1 darajasidagi yirik avtonom tizimlar global bog‘lanishning asosiy ustunlari sifatida xizmat qiladi. Trafikni ichki va tashqi domenlar darajasida nazorat qilishning o‘ziga xos qiyinchiliklari mavjud bo‘lib, ayniqsa domenlararo muvofiqlashtirishda resurs va siyosat cheklovlari katta rol o‘ynaydi.

Trafikni tahlil qilishda agregatsiya darajasining to‘g‘ri tanlanishi, nosozliklar va anomal holatlarni aniqlashda hal qiluvchi ahamiyatga ega. IP-paket, oqim (flow), manba-manzil oqimi (OD-flow) va kanal darajalarida tahlil qilish usullari turli darajadagi aniqlik va hisoblash resurslariga talab qo‘yadi. Chuqur paket tahlili (DPI), NetFlow va SNMP kabi vositalar yordamida aniq va samarali tahlil olib borish imkoniyati yaratiladi.

Ushbu tadqiqotda yoritilgan yondashuvlar va tahlillar tarmoq operatorlari uchun trafikni samarali nazorat qilish, xizmatlar sifatini saqlash, tarmoq ishonchliligini oshirish va anomaliyalarni aniqlash imkonini beradi.

Takliflar:

1. Statistik va avtomatlashtirilgan trafik tahlilini birlashtirish an’anaviy vositalarni sun’iy intellekt asosidagi modellar bilan integratsiya qilish orqali trafikni real vaqtda aniqlash va bashorat qilish samaradorligini oshirish mumkin.
2. DPI va NetFlow ma’lumotlariga asoslangan chuqur o‘rganish modellarini joriy etish ayniqsa shifrlangan trafik sharoitida kontentga asoslanmagan, lekin oqim xatti-harakatlarini tushunishga asoslangan yondashuvlar afzallik beradi.
3. Mahalliy va global darajadagi trafik monitoring tizimlarini muvofiqlashtirish tarmoqlar o‘rtasida trafik oqimini to‘g‘ri boshqarish uchun ko‘p darajali (hierarchical) monitoring arxitekturasini ishlab chiqish lozim.
4. Tarmoq xavfsizligini oshirish maqsadida tahlil natijalarini filtratsiya va prioritizatsiya tizimlariga bog‘lash xizmat sifati (QoS) va xavfsizlik siyosatlariga asoslangan trafikni saralash imkoniyatlarini rivojlantirish zarur.

ISSN 3030-3907

5. Tarmoq holatini tasniflash va vizualizatsiya qilish uchun zamonaviy grafik interfeyslar yaratish bu tizim administratorlari uchun qaror qabul qilishni soddalashtiradi va reaksiyani tezlashtiradi.

Shunday qilib, raqamli infratuzilmalarning kengayib borishi bilan birga, ularni samarali boshqarish va tahlil qilish bo‘yicha kompleks, avtomatlashtirilgan va moslashuvchan yechimlar zarur bo‘lmoqda. Kelajakda zamonaviy yondashuvlarni joriy etish orqali tarmoqlarni yanada barqaror va xavfsiz qilish mumkin bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Feldmann, A., Greenberg, A., Lund, C., Reingold, N., & Rexford, J. (2001). Deriving traffic demands for operational IP networks: Methodology and experience. IEEE/ACM Transactions on Networking, 9(3), 265–280. https://doi.org/10.1109/90.929845

2. Feldmann, A., Kammenhuber, N., Maennel, O., Maggs, B., De Prisco, R., & Sundaram, R. (2004). A methodology for estimating interdomain web traffic demand. In Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC), October 25, 2004. DOI: 10.1145/1028788.1028833

3. Zhang Long, Wang Jinsong. Network Traffic Classification Based on a Deep Learning Approach Using NetFlow Data. // The Computer Journal. – 2022. – Vol. 66, No. 8. – DOI: 10.1093/comjnl/bxac049 [3] Zhang L., Wang J. (2022). Network Traffic Classification Based on Deep Learning Using NetFlow Data. The Computer Journal, 66(8). https://doi.org/10.1093/comjnl/bxac049

4. Xu-Yang Chen, Lu Han, De-Chuan Zhan, Han-Jia Ye. MIETT: Multi-Instance Encrypted Traffic Transformer for Encrypted Traffic Classification. arXiv preprint, 2024.

5. Liu, Z., Xie, Y., Luo, Y., Wang, Y., & Ji, X. (2025). TransECA-Net: A Transformer-Based Model for Encrypted Traffic Classification. Applied Sciences, 15(6), 2977. https://doi.org/10.3390/app15062977

6. Krylatov, A.; Puzach, V.; Shatalova, N.; Asaul, M. Optimization of traffic lights operation using network load data. Transp. Res. Procedia 2020, 50, 321–329.

7. Makarova, I.; Shubenkova, K.; Pashkevich, A. Efficiency Assessment of Measures to Increase Sustainability of the Transport System. Transport 2021, 36, 123–133.

8. Navarro-Ortiz, J.; Romero-Diaz, P.; Sendra, S.; Ameigeiras, P.; Ramos-Munoz, J.J.; Lopez-Soler, J.M. A Survey on 5G Usage Scenarios and Traffic Models. IEEE Commun. Surv. Tutor. 2020, 22, 905–929.

ISSN 3030-3907

9. Rescio, T.; Favale, T.; Soro, F.; Mellia, M.; Drago, I. DPI Solutions in Practice: Benchmark and Comparison. In Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 27 May 2021; pp. 37–42.

ISSN 3030-3907