УДК 004.891 DOI: 10.31673/2412-4338.2022.042533

Наталенко М.М., Корецька В.О.
Державний університет телекомунікацій, Київ

ЕФЕКТИВНІСТЬ КЛАСИФІКАЦІЇ ДОДАТКІВ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ КОМП'ЮТЕРНИХ МЕРЕЖ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Анотація: *В статті розглянуто актуальність дослідження мережевого трафіку, що пояснюється входженням комп'ютерних мереж в життя кожної людини. Стрімкий розвиток комп'ютерних мереж спричинив зростання уваги до питань якості та надійності їх роботи.*

Дослідження аналізу трафіку комп'ютерних мереж актуально для забезпечення якості проводового та безпроводового зв'язку, інформаційних ресурсів та інформаційного пошуку.

Дослідження мережевого трафіку вказує на необхідність його класифікації для відображення мережевих даних в класи трафіків та типи додатків. Доцільно використання методів машинного навчання, що полегшує адаптацію системи до постійно змінних Інтернет-ресурсів, враховуючи специфіку мережевого трафіку. Вивчення мережевого трафіку вказує, що для успішної класифікації мережевого трафіку необхідно зберігати або обробляти увесь трафік, що проходить через мережу.

Визначено, що класифікація мережевого трафіку є важливим завданням в області комп'ютерних мереж. Метою класифікації мережевого трафіку є відображення потоку мережевих даних в певні типи додатків або класи трафіків. Проведеного огляд методів класифікації мережевого трафіку. Наведено результати порівняння сучасних підходів класифікації мережевого трафіку.

Незважаючи на спектр методів, класифікація мережевого трафіку знаходиться ще на стадії розвитку. Слід відмітити, що сучасні методи, зокрема на основі машинного навчання доводять ефективні результати.

Ключові слова: *мережевий трафік, комп'ютерна мережа, класифікація, методи, технології, додаток, класи, машинне навчання.*

Natalenko M.M., Koretska V.O.
State University of Telecommunications, Kyiv

EFFECTIVENESS OF CLASSIFICATION OF COMPUTER NETWORK TRAFFIC ANALYSIS APPLICATIONS USING MACHINE LEARNING METHODS

Abstract*: The article considers the relevance of network traffic research, which is explained by the introduction of computer networks into the life of every person. The rapid development of computer networks has caused increased attention to issues of quality and reliability of their work.*

The study of computer network traffic analysis is relevant for ensuring the quality of wired and wireless communication, information resources and information search.

The study of network traffic indicates the need for its classification to display network data into traffic classes and application types. It is advisable to use machine learning methods, which facilitates the adaptation of the system to constantly changing Internet resources, taking into account the specifics of network traffic. Network traffic analysis indicates that to successfully classify network traffic, all traffic passing through the network must be stored or processed.

It was determined that the classification of network traffic is an important task in the field of computer networks. The purpose of network traffic classification is to map the flow of network data into specific application types or traffic classes. An overview of network traffic classification methods

was conducted. The results of a comparison of modern approaches to the classification of network traffic are given.

Despite the range of methods, the classification of network traffic is still at the stage of development. It should be noted that modern methods, in particular based on machine learning, prove effective results.

***Keywords**: network traffic, computer network, classification, methods, technologies, application, classes, machine learning.*

1.Вступ

Мережевий трафік або трафік даних – це кількість даних, що переміщуються по мережі в певний момент часу. Дані в комп'ютерних мережах здебільшого інкапсульовані в мережеві пакети, які власне і забезпечують навантаження в мережі [1].

Актуальність проблеми мережевого трафіку пояснюється тим, що комп'ютерні мережі все більше входять в життя звичайної пересічної людини. Стрімкий розвиток комп'ютерних мереж спричинив зростання уваги до питань якості та надійності їх роботи. Дослідження аналізу трафіку комп'ютерних мереж актуально для забезпечення якості проводового та безпроводового зв'язку, роботи інформаційних ресурсів та інформаційного пошуку.

Класифікація мережевого трафіку є важливим завданням в області комп'ютерних мереж. Класифікація мережевого трафіку сприяє ідентифікації і класифікації різних додатків та протоколів, що передаються по мережі. Тобто мережевий адміністратор зможе ефективно контролювати цей трафік, оптимізуючи і встановлюючи пріоритети.

В останні роки спостерігається стрімке зростання шифрування мережевого трафіку, що ускладнює його класифікацію. Традиційні методики для класифікації мережевого трафіку демонструють низьку точність класифікації, що створює проблему класифікації зашифрованого трафіку.

2. Постановка проблеми.

Контроль доступу до Інтернет-ресурсів є актуальною проблемою з важливим прикладним значенням. Причинами цього є блокування доступу до нелегальної інформації, використання ресурсів в особистих цілях, запобігання витоку конфіденційної інформації тощо. Перед адміністраторами мереж постає першочергове завдання – визначення типу мережевого трафіку, що генерується користувачами. При цьому трафік може бути шкідливим, неприйнятним, таким, що виходить за межі звичайних бізнес-процесів.

Мережевий трафік є складним динамічним процесом. Метою класифікації мережевого трафіку є відображення потоку мережевих даних в певні типи додатків або класи трафіків. Для розв'язання проблеми класифікації широкого поширення набули технології машинного навчання, що довели свою ефективність. Більшість методів машинного навчання вивчають відношення між заданим набором властивостей (наприклад, номер порту, розмір потоку, інтервали між пакетами) і конкретним додатком. Цей набір властивостей використовується для створення моделі, яка в подальшому використовується для ідентифікації мережевого трафіку в режимі онлайн. Мережеві додатки використовують методи приховування протоколу, які довільно змінюють характеристики їх трафіку, що впливає на точність ідентифікації мережевого трафіку.

3. Мета і задачі дослідження.

Метою дослідження є підвищення ефективності класифікації додатків мережевого трафіку комп'ютерних мереж за умов апріорної невизначеності методами машинного навчання. Для реалізації мети запропоновано використовувати технології машинного навчання. Такі методи дозволять системі що розробляється легко адаптуватися до природи Інтернет-ресурсів, що постійно змінюються та враховувати специфіку аналізу мережевого трафіку.

4. Аналіз останніх досліджень і публікацій.

Дослідження мережевого трафіку вказує на необхідність його класифікації для відображення мережевих даних в класи трафіків та типи додатків. Доцільно використання методів машинного навчання, що полегшує адаптацію системи до постійно змінних Інтернет-ресурсів, враховуючи специфіку мережевого трафіку. Вивчення мережевого трафіку вказує, що для успішної класифікації мережевого трафіку необхідно зберігати або обробляти увесь трафік, що проходить через мережу.

Аналіз існуючих рішень класифікації за допомогою машинного навчання трафіку показує, що мають місце такі проблеми:

- більшість технологій машинного навчання працюють тільки з пакетним трасуванням, яке вимагає впровадження додаткового (часто дорогого) устаткування;

- вплив проріджування пакетів на класифікацію трафіку все ще недостатньо вивчено, незважаючи на те, що така технологія часто використовується мережевими операторами.

5. Результати дослідження.

Класифікація мережевого трафіку – це процес ідентифікації мережевих додатків або протоколів, що існує в мережі [2]. Класифікація мережевого трафіку дозволяє визначити, які види трафіку є у мережі, організувати трафік (тобто пакети) в класи або категорії трафіку на основі того, чи відповідає трафік певним критеріям, і обробляти деякі типи трафіку інакше.

Класифікація мережевого трафіку не є новою задачею для комп'ютерних мереж. Пошук ефективних рішень класифікації мережевого трафіку в різних умовах є сучасною актуальною задачею. Причиною є те, що мережевий ландшафт швидко змінюється і методи та алгоритми, ще недавно показували позитивний результат, в нових умовах значно втрачають свою ефективність або стають зовсім непридатними. З часом кількість підходів до класифікації значно розширилася, що і спричинило необхідність їх класифікації.

У контексті класифікації мережевого трафіку об'єктом класифікації є мережеві потоки, що складаються з послідовності мережевих пакетів, якими обмінюються пара вузлів з метою міжпроцесної взаємодії через комп'ютерні мережі.

Іншим основним поняттям класифікації мережевого трафіку є поняття класу. Існує безліч визначень класу в цій галузі, тому що мережевий трафік може бути розділений на класи за різними критеріями, такими як протокол рівня додатків, структура мережі тощо. Для загальних цілей класифікації трафіку існує два найбільш широко використовувані визначення – це конкретний протокол програми (FTP, HTTP, SMTP) та група схожих програм (web – серфінг, поштові клієнти тощо). Слід зазначити, що з певних цілей визначення класу може бути простіше (нормальний і аномальний) чи складнішим (конкретні реалізації чи версії протоколів). Клас зазвичай вказує на IP-трафік, сформований програмою або групою програм. Перед класифікацією необхідно визначити ознаки, які найбільше впливають на кінцеву точність.

В основі класифікації мережевого трафіку (Рис.1) є аналіз номерів портів пакетів на транспортному рівні (класифікація, заснована на портах), відновлення сигнатури протоколу з його корисного навантаження (класифікація, заснована на корисному навантаженні), статистичних методів аналізу характеристик обміну пакетами між хостами статистичних властивостей мережевого трафіку Кожен з підходів має свої переваги і недоліки.

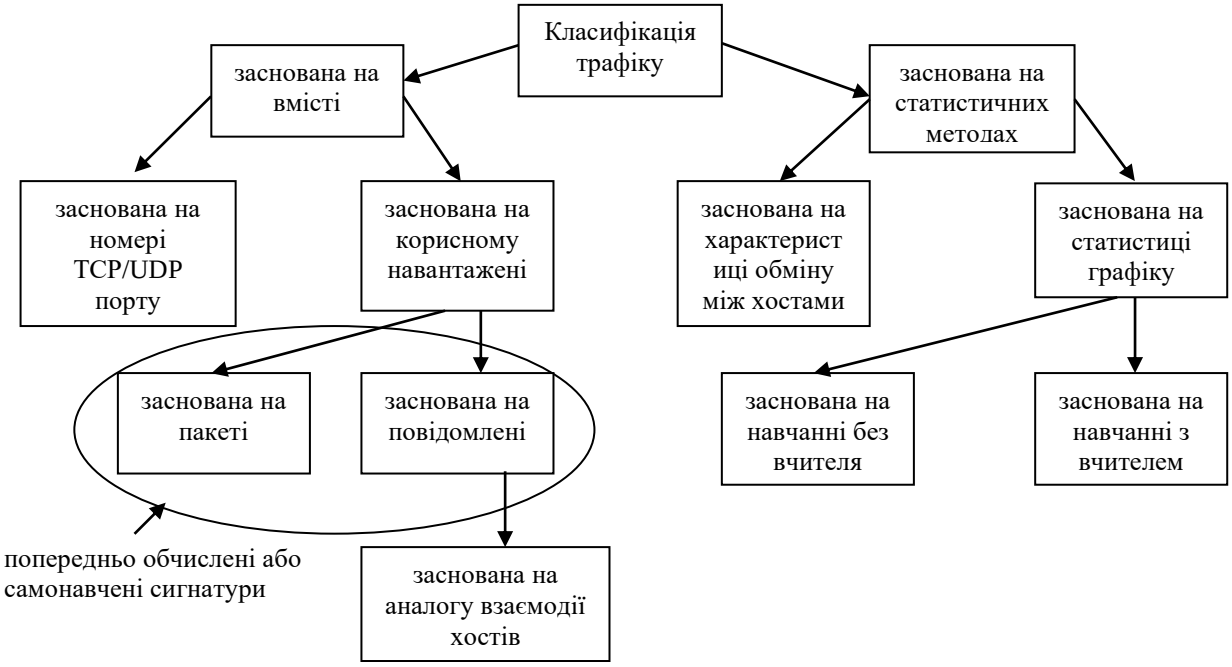

Рис.1. Класифікація мережевого трафіка

Традиційні методи класифікації мережного трафіку, засновані на номерах портів, і на інформаційному навантаженні, покладаються на пряме вивчення мережевих пакетів. Схема класифікації портів перевіряє заголовки пакета. Аналізуються поля заголовка, що містять номери портів джерела та одержувача, а потім визначається протокол застосування згідно зі списком зареєстрованих відомих номерів портів, який підтримується організацією IANA (Internet Assigned Numbers Authority).

Класифікація трафіку по портах інтегрована у більшість сучасних мережевих пристроїв та програмне забезпечення. Це ефективний і швидкий підхід до ідентифікації протоколів додатків спочатку використання мережі Інтернет, коли більшість програм використовували їх стандартні номери портів, зареєстровані в IANA. Тим не менш, з того моменту, як отримали свій розвиток програми на протоколі P2P, який часто вибирає довільні номери портів для того, щоб уникнути виявлення та фільтрації, метод класифікації портів ставав все менш і менш точним.

Ранні спроби досліджень класифікації, заснованої на корисному навантаженні, були присвячені конструюванню бібліотеки сигнатур протоколів та проблемі масштабованості у глибокому аналізі пакетів. З цією метою в деяких роботах представлений набір сигнатур протоколів, які були виділені вручну з доступних специфікацій протоколів і наборів даних. Проте, обчислювальні витрати глибокого аналізу пакетів значно вищі, ніж під час аналізу номерів портів. В результаті було запропоновано нові підходи для швидкого та ефективного пошуку сигнатур протоколів у навантаженні пакетів, які були покликані дозволити використовувати класифікацію, засновану на навантаженні, у високошвидкісних мережах (Рис. 2.).

Рис. 2. Класифікація заснована на корисному навантаженні

Підхід, заснований на інформаційному навантаженні пакета, вважається найбільш точною та надійною схемою класифікації трафіку. В нього є певні обмеження та складності. Насамперед, обчислювальні витрати такого методу є головною перешкодою для його застосування у високошвидкісних мережевих з'єднаннях. З одного боку, глибока перевірка пакета вимагає великих обчислювальних ресурсів для отримання його вмісту. Але з іншого боку, процес декодування протоколу та зіставлення сигнатур привносить навіть більшу складність обчислення. Дослідники вирішили подолати цю перешкоду шляхом запровадження ефективних методів порівняння сигнатур.

Другою складністю є отримання апріорної інформації про мережеві протоколи (формати повідомлень або сигнатури протоколів), що є непростим завданням. Насправді ця інформація зазвичай виділяється професіоналами шляхом ручного аналізу специфікацій протоколу (якщо є) або пакетних трейсів, що займає багато часу і вимагає автоматизації. Нарешті, інформаційний підхід не застосовується, коли немає доступу до навантаження пакета, наприклад, у разі класифікації зашифрованого трафіку.

Ранні спроби досліджень класифікації, заснованої на корисному навантаженні були присвячені конструюванню бібліотеки сигнатур протоколів і проблемі масштабованості в глибокому аналізі пакетів. З одного боку, деякі роботи представили набір сигнатур протоколів, які були виділені вручну з доступних специфікацій протоколів і наборів даних. З іншого боку, обчислювальні витрати глибокого аналізу пакетів значно вищі, ніж під час аналізу номерів портів. Таким чином, були запропоновані нові підходи для швидкого та ефективного пошуку сигнатур протоколів у навантаженні пакетів, які були дозволені використовувати класифікацію, засновану на навантаженні, у високошвидкісних мережах.

Технологія класифікації на основі корисного навантаження пакета DPI з'явилася в результаті заміни класифікації потоків портів. Вважалося, що у ній будуть усунуті недоліки, і загальна точність класифікації підвищиться. DPI класифікатори прийнято розглядати, поділяючи на типи за зростанням ступеня аналізу та обробки вмісту пакетів, та вимог до пам'яті:

• перший тип включає сигнатурні класифікатори, мета яких полягає у пошуку збігів за деякими масками, або сигнатури в корисному навантаженні прикладного рівня. Більшість пакетів різних протоколів прикладного рівня починаються з певного заголовка, на основі якого можна створити сигнатуру для гарантованого визначення протоколу або програми;

• на другому рівні DPI класифікаторів вводиться синтаксична перевірка, яка є покращеною версією першого типу і дозволяє не тільки визначати до якого додатку відноситься пакет, але й перевіряти правильність переданого пакета синтаксично. Припустимо, HTTP пакет має чітку структуру, де кожен пакет починається з команди (GET, POST, PUT і т.д.), за якими слідують заголовки, і тіло повідомлення, яке має бути укладено певні теги. Синтаксична перевірка забезпечує правильність сформованого пакета;

• третій рівень вводить так званий протокол відповідності, який контролює вміст пакета лише на рівні сеансу - тобто. при HTTP GET запит на сервер. Відповідь буде правильний статус відповіді від сервера. Завдяки протоколу відповідності з'являється можливість перевіряти відповідність поведінки з дійсною специфікацією різних протоколів;

• четвертий рівень визначає семантику даних. За допомогою неї можна перевірити все те, що було введено на попередніх рівнях, а також додатково перевірити, чи дійсно об'єкт, що передається за цим протоколом, є тим, чим він оголошений. DPI, що працюють на четвертому рівні, можуть, наприклад, перевіряти, чи дійсно вміст у тегах зображення протоколу HTTP є зображенням тощо.

Аналіз корисного навантаження рівня програми дозволяє розширити можливості класифікації, забезпечуючи перевірку семантики даних, протоколу відповідності та багато іншого. Однак це накладає додаткові вимоги до продуктивності та пам'яті при обробці трафіку. DPI класифікатори повинні отримувати своєчасні оновлення при появі нових, та внесення змін до існуючих протоколів та додатків, що неможливо без великого штату співробітників, що в свою чергу призводить до значних фінансових витрат. Слід також враховувати, що цей підхід може бути неможливим у поточних реаліях з великими обсягами зашифрованого та тунельованого трафіку. Показано, що класифікація, заснована на корисному навантаженні, для P2P-трафіку (шляхом дослідження сигнатур трафіку для прикладного рівня) може скоротити помилки першого і другого роду до 5% від загальної кількості байт більшості досліджуваних P2P-протоколів.

Сучасні практичні розробки (NetPDL, NBAR, SML, BinPac) повністю не вкладаються в цю таксономію, оскільки та сама технологія може належати кільком категоріям.

Через обмеженість традиційних методів, в останні роки з’явилося безліч досліджень та робіт з альтернативних підходів до точної та ефективної класифікації мережевого трафіку. Найбільш перспективним напрямом є статистична класифікація, яка використовує статистичні параметри потоків трафіку. Суть у тому, що трафік, що генерується різними типами додатків, має свої відмінні характеристики, що відображають унікальну поведінку та внутрішню природу додатків. Характеристики потоку можуть бути виражені у вигляді векторів ознак та статистичні методи або техніки машинного навчання можуть бути застосовані для класифікації. За наявності повного та поміченого тренувального набору даних, дуже просто побудувати класифікатор, використовуючи нові технології машинного навчання. Акцент зроблений на класифікації трафіку зі зведених показників {dstIP, dstPort} та дослідженні різної статистики трафіку, включаючи рівень пакета (середнє значення, дисперсія та середньоквадратичне значення розміру пакета), рівень потоку (середнє значення, дисперсія тривалості потоку, обсяг даних, кількість пакетів в потоці), рівень TCP з'єднання, всередині потоку (статистика інтервалів між пакетами в потоці), та властивості сукупності потоків (обсяг даних у контрольних потоках та потоках даних). Для класифікації було використано два алгоритми машинного навчання з вчителем: Лінійний Дискримінантний Аналіз та метод Найближчих Сусідів. Запропоновано метод класифікації трафіку, заснований на гістограмах BGP - рівня. Були використані процеси суміші Дирихле для моделювання емпіричних гістограм, виділених зі зведених показників із загальним конкретним BGP - префіксом.

До класифікації мережного трафіку, заснованих на статистичних методах, застосовано два типи алгоритмів (Рис. 3): поведінкові та статистичні алгоритми мережного та транспортного рівнів.

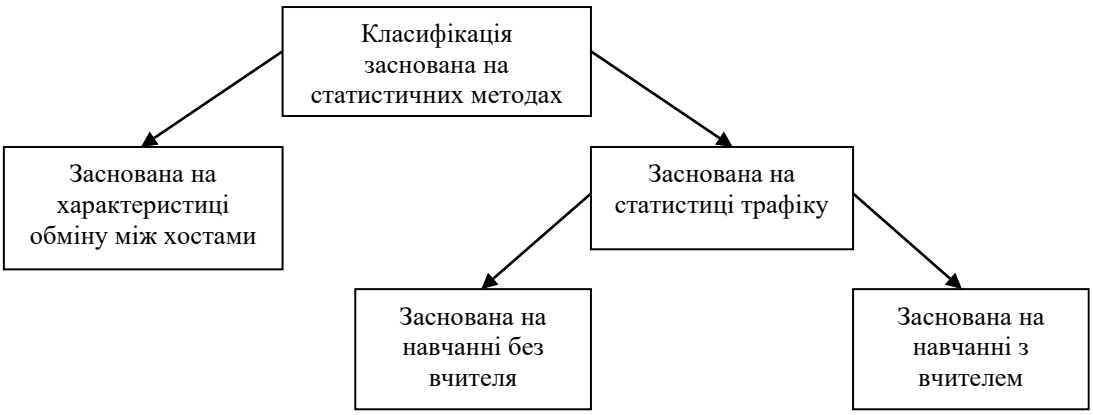

Рис. 3. Класифікація заснована на статистичних методах

Статистичні методи спираються на статистичні характеристики трафіку для ідентифікації програми та базуються на унікальності статистичних характеристик для певних класів додатків, що й дозволяє розділити різні вихідні програми. Статистичні методи, що базуються на статистиці трафіку, поділяються на дві групи: методи класифікації або навчання з учителем та методи кластеризації або навчання без учителя. Типова схема класифікації за статистикою трафіку і двох окремих етапів. Перший - навчання в оф-лайні, в якому тренувальний набір даних надходить на вхід алгоритму, що навчається, а на виході виходить класифікатор (імовірнісна модель або набір правил класифікації). Другий етап - класифікація, у якому класифікатор використовується для передбачення класу додатку у тестовому трафіку.

Залежно від того, чи є тренувальний набір даних поміченим чи ні, поділяють два основних методи, що застосовуються на першому етапі. Алгоритми навчання з учителем призначені для складання класифікаційної моделі на основі тренувальних наборів даних. На противагу цьому алгоритми навчання без вчителя (або кластеризація) намагаються виявити внутрішні структури в наборі непомічених даних і розділити їх на кластери відповідно до деяких ознак. Тут метою є створення чистих кластерів за типами додатків так, щоб результативні кластери могли бути пов'язані з реальними класами додатків та на їх основі могли бути побудовані підсумкові класифікатори. Було показано, що рівень точності, що досягається статистичними алгоритмами навчання з учителем, може бути таким самим високим, як і у класифікаторів, заснованих на навантаженні пакетів, але при менших обчислювальних витратах.

Машинне навчання з вчителем (Supervised Machine Learning Methods) – це метод, що вимагає повного позначеного набору даних, щоб класифікувати невідомі класи. Він працює шляхом навчання моделі з деякими позначеними наборами даних для отримання прогнозованого результату в нових вибірках даних. Однак при такому підході класифікація здійснюється з використанням двох етапів: навчання та тестування.

Алгоритм k-найближчих сусідів (k-nearest neighbor) – простий непараметричний класифікаційний метод, де для класифікації об’єктів у рамках простору властивостей використовуються відстані (зазвичай евклідові), пораховані до усіх інших об'єктів.

Байєсівська мережа відома як імовірнісна модель, яка використовує графову модель для представлення безлічі випадкових величин, а також використовує орієнтований ациклічний граф (DAG) для представлення цих множин.

C4. 5 дерево рішень(C4.5 Decision Tree) – це добре відомий алгоритм машинного, заснований на прийнятті рішень, який використовується для розробки одновимірного дерева рішень. Крім того, для знаходження простого дерева рішень використовується удосконалення ітераційного алгоритму дихотомізатора 3 (ID3).

Алгоритм машино опорних векторів (Support vector machine) – це ще один підхід, який використовується для статистичної теорії навчання (STL), де класифікація низькорозмірного простору може бути перенесена в більш зарозуміле.

Машинне навчання без вчителя (Unsupervised Machine Learning Methods) також називається кластерним, оскільки немає необхідності в маркуванні наборів даних. Машинне навчання без вчителя навчається на великих об'ємах даних і використовують статистичні властивості потоків трафіку для виведення про використовуваний сервіс.

Порівняння розглянутих підходів класифікації представлено Таблиці 1.

Таблиця 1.

Порівняння сучасних підходів класифікації

	Заснований на номерах портів	Заснований на навантаженні пакету	Заснований на статистиці потоків
Точність	Низька	Висока	Висока
Складність виділення ознак	Низька	Висока (DPI)	Залежить від набору ознак
Складність класифікації	Низька	Висока	Нижче середнього
Зашифрований трафік	Так	Ні	Так
Апріорна інформація	Список портів	Сигнатури	Помічені дані
Відкидання невідомого трафіку	Так	Так	(шум)

6. Висновки

Аналіз мережевого трафіку дає наступні переваги:

- визначення вузьких місць в мережі, ними можуть бути користувачі або додатки, які споживають велику кількість пропускної здатності, таким чином складаючи основну частину мережевого трафіку;
- мережева безпека – незвичайна кількість трафіку в мережі є можливою ознакою атаки. Звіти про мережевий трафік дають цінну інформацію про запобігання таких атак;
- мережева інженерія – знання рівнів використання мережі дозволяє аналізувати майбутні вимоги.

В статті представлено огляд існуючих рішень для класифікації мережевого трафіку. Було розглянуто традиційні методи класифікації трафіку, вказано переваги та недоліки методів. Вказано основні причини стрімкого шифрування трафіку, визначено проблему, яку створює шифрування, а саме ускладнення класифікації трафіку, запропоновано рішення за допомогою методів на основі машинного навчання. Розглянуто сучасні методи класифікації трафіку на основі машинного навчання.

Отже, незважаючи на спектр методів, класифікація мережевого трафіку знаходиться ще на стадії розвитку. Слід відмітити, що сучасні методи, зокрема на основі машинного навчання доводять ефективні результати.

Список використаної літератури:

1. Network Traffic [Електронний ресурс] – Режим доступу до ресурсу: https://www.techopedia.com/definition/29917/network-traffic.

2. Traffic Classification [Електронний ресурс] // Cisco – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/nsite/enterprise/wan/wan_optimization/wan_opt_sg/chap05.html.

3. Обзор задач и методов их решения в области классификации сетевого трафика [Електронний ресурс] / А. И.Гетьман, Ю. В. Маркин, Д. О. Обыденков, Д. О. Евстропов // Труды Института системного программирования РАН. – 2017. – Режим доступу до ресурсу: https://ispranproceedings.elpub.ru/jour/article/view/281.

4. IP security [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/ip-security-ipsec/.

5. Berkman, L., Kriuchkova, L., Zhebka, V., Strelnikova, S. Universal Method of Multidimensional Signal Formation for Any Multiplicity of Modulation in 5G Mobile Network Lecture Notes in Electrical Engineeringthis link is disabled, 2022, 831, стр. 305–321 (Scopus)

6. Корецька В.О., Ільїн О.Ю., Балашова Є.О., Чепур М.К., Жебка В.В., Удосконалення інформаційної технології для підвищення функціональної стійкості мережі за допомогою теорії графів. Телекомунікаційні та інформаційні технології. 2021. № 3 (72). С.46-53

References:

1. Network Traffic [Electronic resource] - Resource access mode: https://www.techopedia.com/definition/29917/network-traffic.

2. Traffic Classification [Electronic resource] // Cisco - Resource access mode: https://www.cisco.com/c/en/us/td/docs/nsite/enterprise/wan/wan_optimization/wan_opt_sg/chap05.html .

3. Overview of problems and methods of solving them in the field of network traffic classification [Electronic resource] / A. I. Getman, Yu. V. Markin, D. O. Obydenkov, D. O. Evstropov // Proceedings of the Institute of System Programming RAS. – 2017. – Resource access mode: https://ispranproceedings.elpub.ru/jour/article/view/281.

4. IP security [Electronic resource] - Resource access mode: https://www.geeksforgeeks.org/ip-security-ipsec/.

5. Berkman, L., Kriuchkova, L., Zhebka, V., Strelnikova, S. Universal Method of Multidimensional Signal Formation for Any Multiplicity of Modulation in 5G Mobile Network Lecture Notes in Electrical Engineering this link is disabled, 2022, 831, p. 305–321 (Scopus)

6. Koretska V.O., Ilyin O.Yu., Balashova E.O., Chepur M.K., Zhebka V.V., Improvement of information technology to increase the functional stability of the network using graph theory. Telecommunications and information technologies. 2021. No. 3 (72). P.46-53