ПРИКЛАДНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК,
БЕЗПЕКИ ТА МАТЕМАТИКИ, 2024, № 3

УДК 12.125

ВИЯВЛЕННЯ DDOS-АТАКИ НА ВИСОКОШВИДКІСНУ МЕРЕЖУ: ОПИТУВАННЯ

Савченко В. А. (ORCID: 0000-0002-3014-131X)
Поночовний П. М. (ORCID: 0009-0008-6480-6990)
Аверічев І. М. (ORCID: 0009-0008-9766-0115)
Державний університет інформаційно-комунікаційних технологій, Київ

HIGH-SPEED NETWORK DDOS ATTACK DETECTION: A SURVEY

Savchenko Vitalii, Ponochovnyi Petro, Averichev Ihor
State University of Information and Communication Technologies, Kyiv

Abstract. Having a large number of device connections provides attackers with multiple ways to attack a network. This situation can lead to distributed denial-of-service (DDoS) attacks, which can cause fiscal harm and corrupt data. Thus, irregularity detection in traffic data is crucial in detecting malicious behavior in a network, which is essential for network security and the integrity of modern Cyber–Physical Systems (CPS). Nevertheless, studies have shown that current techniques are ineffective at detecting DDoS attacks on networks, especially in the case of high-speed networks (HSN), as detecting attacks on the latter is very complex due to their fast packet processing. This review aims to study and compare different approaches to detecting DDoS attacks, using machine learning (ML) techniques such as k-means, K-Nearest Neighbors (KNN), and Naive Bayes (NB) used in intrusion detection systems (IDSs) and flow-based IDSs, and expresses data paths for packet filtering for HSN performance. This review highlights the high-speed network accuracy evaluation factors, provides a detailed DDoS attack taxonomy, and classifies detection techniques. Moreover, the existing literature is inspected through a qualitative analysis, with respect to the factors extracted from the presented taxonomy of irregular traffic pattern detection.

Keywords: denial of on high-speed service; distributed denial of service; cyber–physical system; machine learning; high-speed network; intrusion detection system; express data path.

Вступ. Зі збільшенням мережевого трафіку через впровадження таких пристроїв, як дистанційні датчики, інтелектуальні пристрої, безпілотні транспортні засоби, підключені до глобальної системи позиціонування (GPS), передача даних 5G, смартфони та хмарні обчислення, розмір Інтернету стрімко зростає [1]. У світі налічується приблизно 4,66 мільярда користувачів Інтернету, що становить 59,5% світового населення. Подібним чином, приблизно 53,6% населення планети є користувачами соціальних мереж, тоді як користувачі смартфонів складають 66,6%. Загалом у 2021 році загальна кількість населення, підключеного до цифрового світу, становила приблизно 7,83 мільярда, з очікуваним щорічним зростанням на 316 мільйонів користувачів. Очікуване зростання кількості користувачів Інтернету викликає тривогу, особливо коли йдеться про безпеку в Інтернеті та цілісність кіберфізичних систем (CPS) [2]. Хоча Інтернет допомагає з різними аспектами життя та робить життя зручнішим, він створює багато ризиків для безпеки. Типовим прикладом цих ризиків є зловмисні атаки, такі як атаки DoS, атаки в оману та атаки з відповіддю, які є типами кібератак. Їх цілі та методи різні. Метою DoS-атак є порушити доступність, а обманні атаки включають маніпуляції та обман, тоді як атаки відтворення зосереджені на перехопленні та повторному використанні дійсних даних для отримання несанкціонованого доступу або маніпулювання системами. Крім того, атаки типу «відмова в обслуговуванні» (DoS) пов'язані з порушенням конфіденційності користувачів і порушенням безпеки [3].

Як правило, дві форми DoS-атак викликають занепокоєння: DoS і DDoS (DDoS). Як правило, DDoS-атаки відбуваються через пов'язані пристрої з багатьох місць. Атака

може викликати незвичайну активність, яка перериває звичайний трафік певних серверів, служб і мереж через бомбардування даними з сусідньої інфраструктури. Ця незвичайна діяльність створює величезну безперервну кількість запитів на обслуговування до серверів і мереж, що ускладнює ідентифікацію надійного джерела. Наприклад, у середовищі Інтернету речей (IoT) зловмисник може швидко атакувати тисячі пристроїв у великих масштабах [4,5,6,7]. Для практичної мережі зв'язку CPS затримка часу є важливою проблемою. Надійний, адаптивний DSC, заснований на стратегії витримки та перспективі перемикання, був розроблений для комутованого нелінійного CPS із затримкою в часі під час гібридних атак на вимірювання датчиків [8]. Щоб дослідити стохастичні характеристики наскрізної затримки часу, спричиненої мережею, у контексті CPS інтелектуальної підстанції з критичним часом, компоненти CPS розумної підстанції, такі як потік даних, мережа зв'язку та інтелектуальні електронні пристрої (IED), моделюються [9]. У випадку атак із затримкою часу (TDA), які використовують слабкі місця каналу зв'язку, щоб завдати потенційно серйозної шкоди системі, багато підходів, запропонованих для виявлення TDA, оцінювалися виключно в автономному режимі та за суворих припущень щодо створення практичного методу боротьби з проблеми реального світу [10]. DDoS-атаки можуть бути атаками на прикладному рівні, атаками на протоколи та атаками на основі томів, і виявити їх складніше у високошвидкісних мережах (HSN). У мережах HSN, які складаються з оптоволоконних мереж зі швидкістю передачі даних 100 Гбіт/с, перемикання контексту обробки мережі через DoS-атаку може зменшити швидкість мережі через пакет, пов'язаний із системним викликом, і копію переходу, що поширюється по мережі [11].

Оскільки швидкість обробки даних у мережах зросла, виявлення DDoS-атак стало складнішим, що підвищує ризики для безпеки. Рисунок 1 ілюструє сценарій DDoS-атаки, що відбувається у високошвидкісній мережі. Крім того, дослідники стикаються з величезними проблемами у боротьбі з DDoS-атаками через швидкість мережі та різні типи даних, що надходять у мережу [12]. Було запропоновано кілька методів виявлення DDoS-атаки з двома поширеними типами виявлення, а саме виявлення зловживання та виявлення ненормального [13,14]. Обидві системи виявлення мають обмеження щодо параметрів, вибраних для виявлення мережевих шаблонів. Перевага виявлення зловживань полягає в тому, що воно забезпечує високу точність; однак для цього потрібна повна інформація в мережі. Навпаки, попередні знання про мережу не набуваються при ненормальному виявленні, але цей підхід не забезпечує високої точності, яку пропонує виявлення неправильного використання [15].

Останніми роками було проведено огляд кількох літературних джерел, присвячених DoS-атакам. Наприклад, у роботі [16] автори представили таксономію низькошвидкісних DoS-атак, засновану на трирівневому способі дії. Цей огляд включав низькошвидкісні атаки, атаки черги обслуговування та атаки якості обслуговування (QOS) і описував різні підходи до виявлення восьми низькошвидкісних DoS-атак. Однак у статті не розглядаються високошвидкісні мережеві DDoS-атаки, і автори в [17] представили сучасні методи захисту, які допомагають запобігти DDoS-атакам і пом'якшити шкоду, яку завдають користувацькій інформації. У цьому огляді детально розглядаються методи захисту для IoT і програмно-визначених мережевих пристроїв. Як не дивно, DDoS-атаки в сценаріях високошвидкісних мереж не розглядаються [18], де описано механізми захисту від DDoS-атак, включно з реагуванням на атаки, класифікацією трафіку і виявленням атак, але не деталі мережі. Мотивовані вищевикладеними спостереженнями, цілі цього огляду такі:

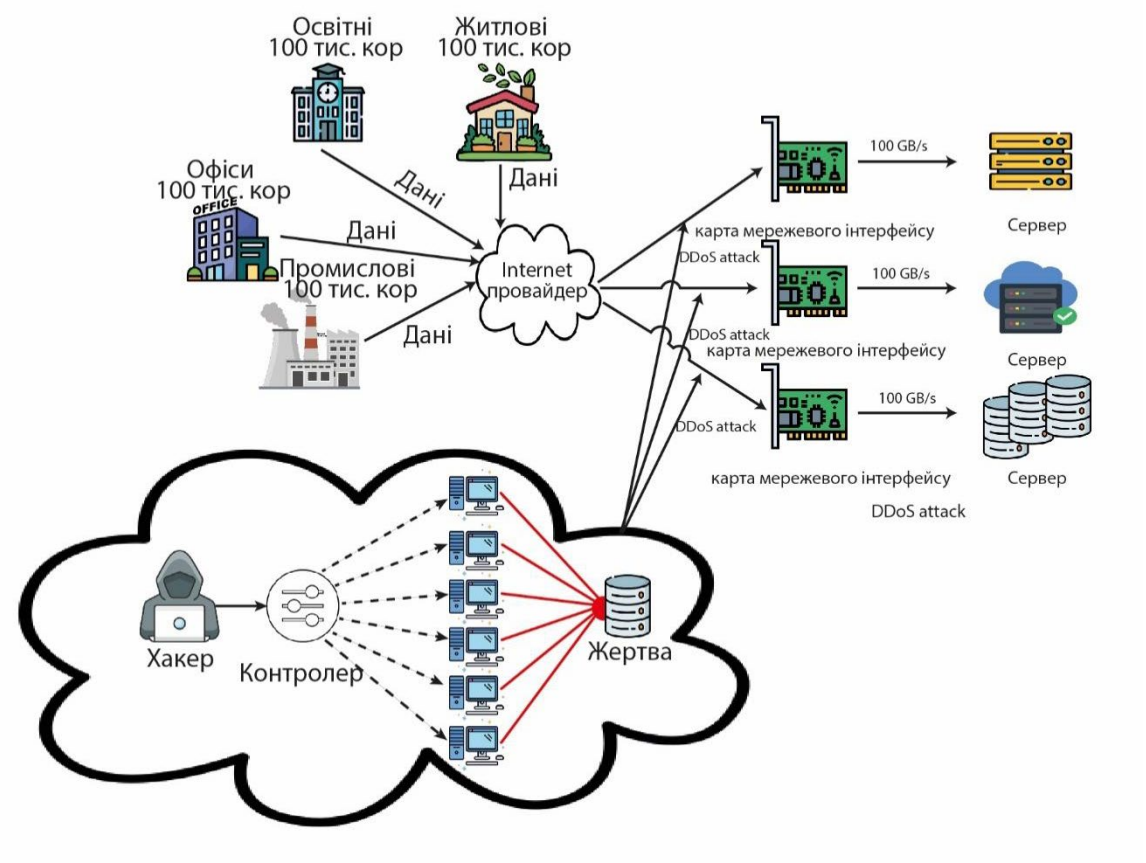

Рис. 1. DDoS-атаки в сценаріях високошвидкісних мереж.

- комплексний огляд типів DDoS-атак, методів виявлення та запобігання;
- огляд останніх DDoS-атак на високошвидкісні мережі;
- упорядкована таксономія шаблонів виявлення нерегулярного трафіку у високошвидкісних мережах;
- комплексне дослідження звичайних слабких і сильних сторін методів виявлення DDoS.

Аналіз останніх досліджень і публікацій. Останні дослідження та публікації свідчать про стрімке зростання кількості та потужності DDoS-атаки у 2024 році. У першому кварталі 2024 року кількість DDoS-атак зросла майже на 30% порівняно з аналогічним періодом 2023 року. Багато атак досягають критичних рівнів за 14 секунд порівняно з 55 секундами двома роками раніше.

За перше півріччя 2023 року кількість DDoS-атак зросла на 106% порівняно з іншим півріччям 2023 року. Середня тривалість атаки збільшилася на 18% до 45 хвилин, що коштує організації близько $270 тисяч за атаку.

Використання штучного інтелекту для розгортання та посилення DDoS-атаки дозволяє їм еволюціонувати, ставати все потужнішими, підривнішими та частішими. Перші кадрові, юридичні, консалтингові та транспортні компанії становлять 10% серед найбільших зареєстрованих DDoS-атак.

У 2021 році DDoS-атака була найпоширенішою загрозою, про яку повідомила половина респондентів. Наступні за поширеністю загрози – SQL-ін'єкції (38%) та програми-вимагачі (29%).

Найбільша DDoS-атака в історії сталася в лютому 2019 року на GitHub зі швидкістю 1,3 Тбіт/с та 126,9 млн пакетів у секунду. У червні 2020 року Cloudflare зафіксувала атаки зі швидкістю 754 млн пакетів за секунду протягом 4 днів.

Таким чином, DDoS-атаки залишаються все потужнішими, частішими та охоплюють ширше коло галузей завдяки використанню ШІ. Компанії необхідно вживати комплексних заходів для захисту від цієї загрози, включаючи WAF, захист від DDoS, керування ботами та безпеку API

Атаки на відмову в обслуговуванні. Атаки на відмову в обслуговуванні (DoS) перевантажують пристрій або мережу, роблячи їх недоступними. Зловмисники надсилають більше трафіку, ніж може обробити ціль, що призводить до її збою і робить її нездатною надавати послуги звичайним користувачам. Об'єктом атаки може стати будь-який сервіс, підключений до мережі або комп'ютера-мішені, наприклад, електронна пошта, онлайн-банкінг або вебсайти. Взаємопов'язані, розподілені мережі машин складаються з пристроїв (наприклад, пристроїв Інтернету речей), на які впливає віддалено кероване шкідливе програмне забезпечення, провокуючи DDoS-атаки [18]. Бот або група машин називається ботнетом. Ботнет може атакувати окремих ботів безпосередньо або надсилати інструкції віддалено. Бот-мережа спричиняє DoS на звичайний трафік у мережі або сервері, що зазнає атаки, при цьому кожен бот надсилає запити на певну IP-адресу. Важко відрізнити звичайний трафік від трафіку зловмисників. Поширеними прикладами DDOS-атак є переповнення UDP, переповнення SYN і посилення DNS. Сьогодні також відбуваються ультракороткі DDoS-атаки. Gcore стверджує, що середня тривалість DDoS-атаки у 2022 році становитиме 5-10 секунд, а пропускна здатність сегмента становитиме 5 Гбіт/с протягом 24 годин.

Типи DDOS атак. Існує багато типів DDoS-атак, деякі з них об'єднані в групи як комбінації багатовекторних атак, і класифікація цих різноманітних атак вимагає інших механізмів захисту. Для онлайн-сервісів атака на найслабшу ланку може вивести з ладу всю мережу. Надійні сервери доменних імен стають непрацездатними, коли їх перевантажують фальшивими запитами від зловмисників [19]. На рисунку 4 показано типи DDoS-атак.

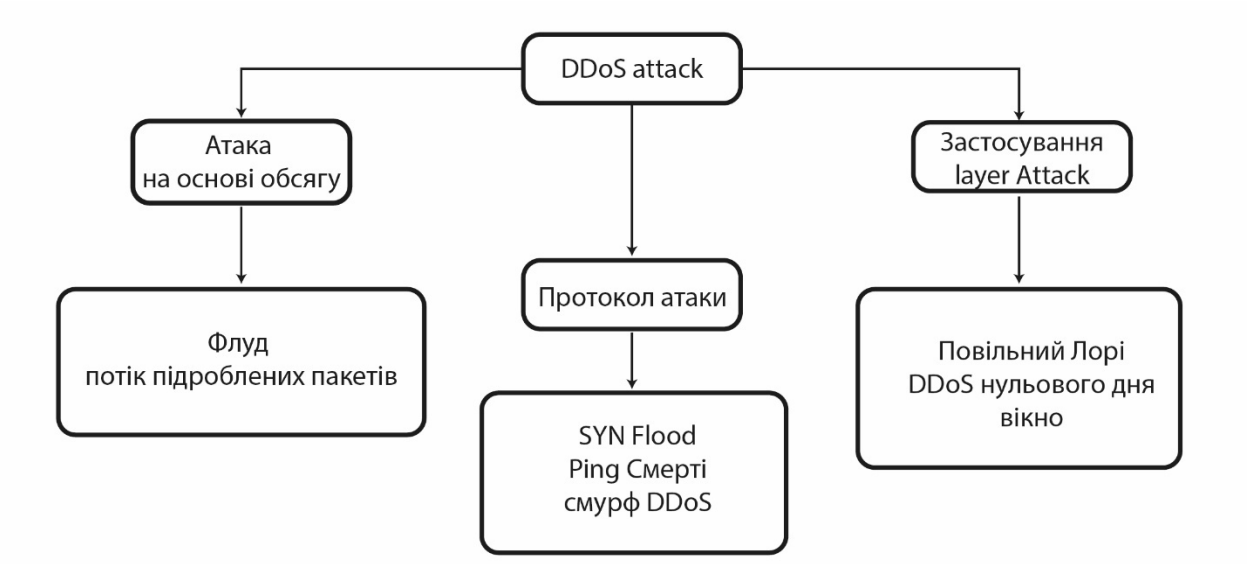

Рис. 2. Типи DDoS-атак

Атаки нульового дня. Ці атаки використовують невідомі вразливості мережевого програмного або апаратного забезпечення. Ці вразливості ще не відомі ні постачальникам, ні громадськості, і від них важко захиститися [19].

Fтаки відображення. Подібно до атак посилення, атаки відбиття використовують вразливі протоколи для посилення атакуючого трафіку. Однак, в атаці відбиття зловмисник надсилає запит на сторонній сервер, який, в свою чергу, надсилає відповідь в цільову мережу, збільшуючи розмір атакуючого трафіку. Важливо зазначити, що цей тип DDoS-атаки може відбуватися як на швидких, так і на повільних мережах, але може бути особливо руйнівним у швидких мережах через великий обсяг генерованого трафіку.

Посилення DNS. Об'ємні DDoS-атаки, відомі як DNS-ампліфікація ефективно використовують передові методи атаки з відображенням. Такі атаки насичують пропускну здатність за рахунок збільшення вихідних потоків даних. Зловмисник генерує великий обсяг трафіку, надсилаючи на сервер інформаційні запити, які генерують великий обсяг даних. Потім він підміняє адресу відповіді і відправляє інформацію назад на сервер. Таким чином, в атаці DNS-ампліфікації зловмисник надсилає серію відносно невеликих пакетів з різних джерел ботнету на загальнодоступний DNS-сервер. Кожен з цих пакетів містить довгий запит, наприклад, запит на пошук DNS-імені; DNS-сервер відповідає на кожен з цих розподілених запитів пакетом-відповіддю, який у кілька разів перевищує розмір початкового пакету запиту, і всі вони перенаправляються назад на DNS-сервер жертви.

SYN-флуд. Атака SYN-флуд обходить протокол тристороннього рукостискання для встановлення TCP-з'єднання між клієнтом і сервером [19]. Зазвичай таке з'єднання встановлюється шляхом надсилання клієнтом запиту на синхронізацію (SYN) на сервер і завершення клієнтом рукостискання остаточним підтвердженням (ACK); SYN-флуд працює шляхом швидкої передачі запиту на синхронізацію і відсутності остаточного підтвердження з боку сервера. Клієнт надсилає серверу запит на синхронізацію (SYN), сервер відповідає підтвердженням (SYN-ACK), і рукостискання завершується остаточним підтвердженням (ACK).

Пінг смерті. Атака Ping of Death відрізняється від стандартної exo-атаки ICMP Ping flood [20]. Вміст пакету зловмисно призначений для того, щоб викликати збій системи на стороні сервера. Дані в типовій пінг-флуд-атаці практично не мають значення, оскільки вона призначена для переповнення смуги пропускання за рахунок великого обсягу; пінг-смерть використовує слабкість пристрою жертви, надсилаючи пакети, які призводять до зависання або самознищення пристрою жертви. Ця техніка також може бути застосована до протоколів, відмінних від ICMP, таких як UDP і TCP.

Атаки на прикладному рівні. DDoS-атака на прикладний рівень – це атака HTTP-флуд [20]. За такої стратегії зловмисник часто взаємодіє з вебсервером і додатком. Веббраузер відображає всі взаємодії як звичайну активність користувача, але налаштований так, щоб споживати якомога більше ресурсів сервера. Запити зловмисника можуть варіюватися від отримання URL-адрес зображень або документів за допомогою GET-запитів до серверних процесів і баз даних за допомогою POST-запитів.

Ідентифікація DDoS-атак. Симптомами DDoS-атаки є те, що сервіси або сайти працюють вкрай повільно або стають недоступними. Інструменти аналізу можуть вказати на те, де відбуваються DDoS-атаки. Наприклад, тенденція до переповнення мереж підозрілими обсягами трафіку, що генерується з певних діапазонів IP-адрес, або трафіком з певними поведінковими профілями пристроїв, місцезнаходженням та інформацією веббраузерів, спрямованим на одну сторінку або кінцеву точку [21]. На рисунку 5 показано приклад базового потоку виявлення DDoS-атаки. Є три симптоми DDoS-атаки.

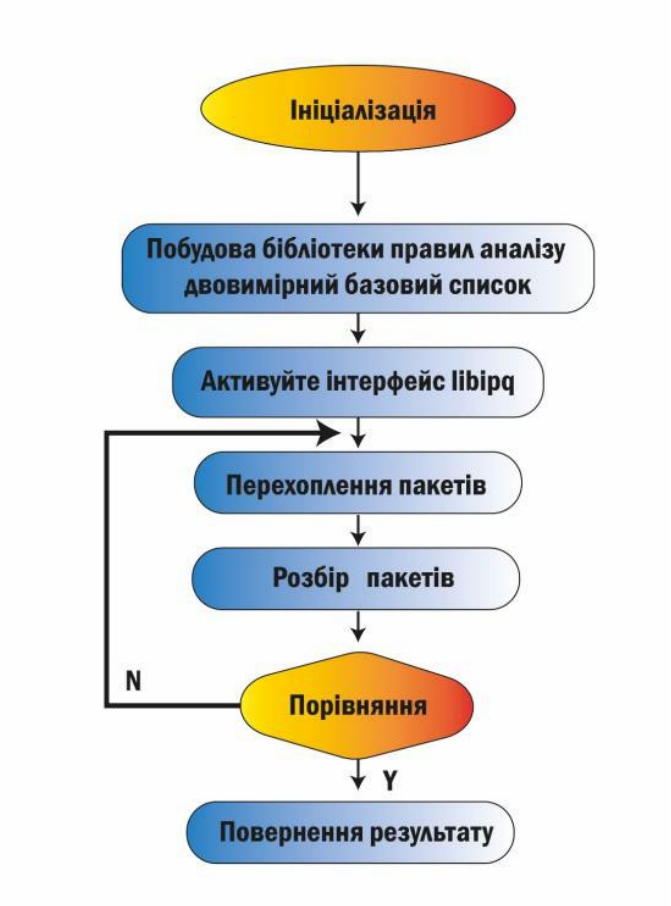

Рис. 3. Потік виявлення DDOS attack

Повільне завантаження вебсайтів або їхня недоступність, раптова втрата доступу до мережі Інтернет, уповільнення роботи комп'ютерів або відсутність реакції вказують на наявність DDoS-атаки. Першим кроком для виявлення DDoS-атаки є перевірка системного правила аналізу libpq - набору бібліотечних методів, які дозволяють програмі надсилати запит до сервера PostgreSQL і отримувати відповідь. Наступні кроки перехоплюють пакет, розбирають його і порівнюють з базою даних внутрішнього сервера. Якщо результат знайдено, він повертається, інакше пакет отримується з інтерфейсу libpq.

Методи виявлення DDoS-атак. Ботнет – це підключений до Інтернету пристрій, на якому працюють два або більше ботів. Ботнети можуть здійснювати DDoS-атаки, красти дані, розсилати спам або надавати зловмисникам доступ до пристрою та його підключень. Оператори можуть керувати та контролювати ботнети за допомогою програмного забезпечення [21]. Зловмисники можуть спричинити відключення бот-мереж заражених комп'ютерів у мережі або зробити послуги недоступними. У таблиці 3 детально описані методи виявлення цих DDoS-атак.

DDoS-атаки вимагають швидкого аналізу трафіку. Швидкість надходження даних з різних джерел становить близько 28 100 Гбіт/с, що є величезною кількістю, коли мова йде про командні рядки NIC 100 Гбіт/с. Аналіз пакетів Socketbase не підходить для швидкої обробки даних. Замість цього використовується Express Datapath, підпрограма Socketbase, яка використовує різні аспекти пакетного фільтру Берклі та розширених пакетних фільтрів Берклі. В даний час для виявлення та запобігання DDoS-атакам в мережі використовується декілька інструментів [22]. Ці інструменти здійснюють

моніторинг журналів подій з різних джерел для виявлення та запобігання DDoS-атакам. У таблиці 2 наведено перелік інструментів для запобігання DDoS-атакам.

Таблиця 1

Дослідження на основі методів виявлення DDoS-атак.

рік	DDOS атаки	Методи виявлення DDOS
2019 рік	Нанесення, об'ємна основа	Опорна векторна машина (SVM), PCA-KNN, нечітка логіка GA
2020 рік	Прикладний рівень	Ентропія, база сигнатур, опорна векторна машина (SVM), bat-алгоритм.
2021 рік	Прикладний рівень	Наївна байєсовська система, опорна векторна машина, дерево рішень, генетичний алгоритм і нечітка логіка, просторовий і часовий сусід.
2022 рік	Прикладний рівень, транспортний рівень	Довга короткочасна пам'ять (LSTM), низька швидкість, дозволений список і блок-список, обмеження швидкості, випадковий ліс, багаторівневий перцептрон, швидкий на основі всіх пакетів, розділяй і володарюй, механізм відра маркерів.
2023 рік	Прикладний рівень	Приріст інформації, випадковий ліс, LTSM, низька швидкість, SVM, RF, LR, KNN, DT, NB, DPS, процесорний час, PGA.

Таблиця 2

Порівняння інструментів запобігання DDoS-атакам.

Інструменти	Напади	Результат
Інструмент SolarWinds SEM	Це програмне забезпечення для виявлення та запобігання DDOS-атакам	Механізм SEM для ведення журналів і подій, які корисні для розслідувань після злому та пом'якшення DDoS.
ХАЛК	Це створює одиничний і нечіткий трафік	Це не вдається приховати особистість. Він може блокувати трафік через HULK.
Молот Тора	Сервер Apache та IIS	Tors hammer реалізує DoS-атаку, використовуючи повільну POST-атаку та HTML-дописи з повільною швидкістю протягом однієї сесії (фактична швидкість випадкового вибору становить 0,5–3 с).
Повільний лорі	DDOS-атаки на HTTP-трафік	Для запобігання DDOS-атакам на цільовий сервер надсилаються дані HTTP-трафіку.
Низькоорбітальна іонна гармата (LOIC)	DOS-атаки на трафік UDP, TCP і HTTP	LOIC перевіряє напругу мережі, а автори шкідливих програм створюють вірус.
XOIC	DoS-атака на протокол контрольних повідомлень Інтернету	У XOIC це інструмент для блокування атаки.

Виявлення DDos-атак у високошвидкісних мережах. Системи виявлення вторгнень з відкритим вихідним кодом Snort і Suricata описують, як оцінити показники падіння і точності в мережах 100 Гбіт/с за допомогою методу порівняння і контрасту [22]. Ця оцінка включає використання системних ресурсів, швидкість обробки пакетів, швидкість падіння пакетів і точність виявлення. Однак недоліком цієї роботи є те, що вона не враховує великі обсяги даних у мережі. Інша модель, модель навчання з дуже довгою короткочасною пам'яттю (VLSTM), вирішує проблеми високої розмірності та несправедливості. Її ефективність в експериментах була отримана з використанням відкритого набору даних UNSW-NB15. У деяких дослідженнях представлені втрати при реконструкції, втрати при класифікації та втрати при зсуві. Однак завдання виявлення аномалій для незбалансованих даних залишається складним.

M. A. Vieira представив нові методи фільтрації пакетів і представив розширену фільтрацію пакетів Берклі (eBPF) та експрес-шину, щоб надати приклади стандартизованих процедур для цих методів. Програми XDP пишуться на C або P4, а інструкції обробляються через ядро та інші програмовані пристрої, такі як інтелектуальні мережеві інтерфейсні карти [22]. Дослідження в першу чергу зосереджене на моніторингу мережі, аналізі трафіку, балансуванні навантаження та профілюванні системи. Крім того, автори розглядають швидкість передачі даних у мережі, але не звертають уваги на рівень втрат пакетів. У Таблиці 3 подано дослідження, проведені за останні п'ять років, класифіковані за різними параметрами, такими як рік, посилання на роботу, ключові особливості, переваги та недоліки.

Таблиця 3.

Дослідження DDoS-атак у високошвидкісних мережах.

рік	Основні характеристики	Переваги	Слабкість
2019 рік	Продуктивність поточного шляху часу (XDP)	Точно вчасно (JIT), гачок ядра.	Це необхідно для захоплення пакетів з високою швидкістю передачі даних.
2019 рік	Виявлення DDoS-атак на прикладному рівні	Аналіз моніторингу HTTP DDOS, виявлення, пом'якшення та запобігання.	Це дослідження не розглядає високошвидкісні мережі.
2019 рік	Модель класифікації Big-Flow	Набір даних мережевого трафіку, масштабований.	Не враховує коефіцієнт скидання пакетів.
2019 рік	Кібербезпека на основі даних використовується для аналізу інтернет-трафіку	Кібербезпека, аналіз мережевого трафіку, машинне навчання (ML) і виявлення соціальних шахрайств.	Необхідні дослідження для розгалужених мереж передачі даних, знання домену щодо моніторингу трафіку.
2020 рік	Система виявлення вторгнень з відкритим кодом: Snort і Suricata	Швидкість обробки пакетів, коефіцієнт падіння пакетів, точність виявлення.	Не враховує великі дані в мережі.
2020 рік	Експериментуйте з підсистемою Linux, щоб відстежувати контейнеризовані програми користувача	Interpledge, eBPF, Profiling, Tracing.	Він не створений для наскрізного перегляду розподіленої системи.
2021 рік	Запропонувати нову схему класифікації зловмисників на основі моделі довготривалої короткочасної пам'яті (LSTM).	LSTM, точність, пропускна здатність. Класифікація трафіку, штучний інтелект, шкідливий трафік.	Використовуючи майбутні стратегії навчання, вибір метрики для LSTM може бути зроблений точно.
2021 рік	У цій статті запропоновано нову модель обговорення дизайну навчання (LDDM)	Нижчий рівень хибнопозитивних і хибнонегативних результатів. DDoS атаки.	Усе ще покращуєте точність виявлення у високошвидкісній мережі 100 Гбіт/с.
2022 рік	Методи на основі сигнатур для пом'якшення DDoS та використання алгоритмів генерації пакетів (PGA) для виконання атак	Повноцінні рішення IDS/IPS, такі як Snort Suricata.	Розкрити весь потенціал eBPF і XDP (крос-компіляція, модульність).
2022 рік	Підхід NetFPGA SUME використовується для фільтрації пакетів і пом'якшення об'ємної атаки DDOS	Фільтрування пакетів було виконано в HSN з використанням одного ядра ЦП.	Тракт даних 100 Гбіт/с забезпечує чудове середовище для тестування.
2023 рік	HARNESS планує та служить як USR площини керування з точки зору стійкості до затримок і чутливості до затримок для автентифікації служб високої доступності.	XDP і eBPF використовуються для узгодженої та оптимізованої наскрізної роботи.	Не враховує коефіцієнт скидання пакетів.

Дослідники в роботі обробили великий обсяг мережевого трафіку за допомогою техніки верифікації, яка перевіряє надійність на основі результатів класифікатора. Якщо виявлено підозрілі пакети, модель класифікації Big-Flow коригується. Основна увага в цьому дослідженні приділяється роботі з наборами даних мережевого трафіку, але не враховується швидкість падіння пакетів. Згідно з [23], схема виявлення DDoS має низку характеристик трафіку. Схема забезпечує жорсткий контур контролю, генеруючи точні сигнали тривоги для кожної підмережі, реалізованої в площині даних, без використання зовнішніх контролерів. Результатом є точне виявлення на основі реалістичних атак з використанням доступних трас. Вона має справу з вхідними потоками і спостережуваним коефіцієнтом симетрії пакетів для кожної захищеної підмережі. Експрес-шляхи передачі даних є підходящою основою для захисту від DDoS-атак і створюють нову схему запобігання кіберзагрозам. Однак швидкість передачі пакетів для з'єднань, які не перевищують 10 Гігабіт, варіюється від 1 до 2 Мбіт/с. У таблиці 4 наведено порівняння нерегулярних моделей трафіку.

Таблиця 4.

Порівняння виявлення шаблонів нерегулярного трафіку.

Техніка виявлення	**Моніторинг руху**	**Фільтрування пакетів**	**NIC**	**Потік транспорту**
Kubernetes	Офлайн	Так, eBPF/XDP	NA	NA
Ядро JIT/транслятор	Офлайн	Так (eBPF/XDP)	Розумні мережеві карти	NA
Вібраційний LSTM	Онлайн	немає	NA	Довго/короткостроково
мова P4	Онлайн	Так, eBPF/XDP	Розумні мережеві карти	NA
Великий потік	Онлайн	немає	10 ГБ/с	Велика течія
Хрипи, Суріката	Офлайн	так	100	Довго/короткостроково
Модулі PMDA	Офлайн	Так (БНФ)	-	-
hXDP	Онлайн	Так (eBPF)	100 Гбіт/с	Велика течія
XDP	-	Bpf, eBPF, XDP	-	Довго/короткостроково

Підсистема Linux може відстежувати контейнеровані програми користувацького простору в роз'ємі Inter ledger і контролювати стек програмного забезпечення, що розробляється [23]. Під час тестів було досліджено та оцінено інструментальне середовище, розроблене в цьому проекті для підтримки eBPF. Проект не представляє наскрізний погляд на розподілені системи. Крім того, такі методи, як ідентифікація операційної системи користувача і аналіз зашифрованого трафіку HTTPS для відстеження локального провідника користувача, досягли точності класифікації 96,06% на 20 000 вибіркових даних, методи аналізу є потужними техніками. Зловмисники можуть використовувати статистику для ідентифікації операційної системи користувача.

Системи розподіленого управління даними (DDCS) можуть бути використані для кібербезпеки, керованої даними, аналізу соціального та інтернет-трафіку, збору даних про кібербезпеку, функціональної інженерії та моделювання кібербезпеки. У своєму огляді важливої нещодавньої роботи в галузі виявлення спаму та класифікації IP-трафіку він продемонстрував тісний зв'язок між даними, моделями та методологіями [23]. Однак швидкі дані в цій роботі не згадуються.

Запропоновано нову схему класифікації шкідливих програм на основі моделі довготривалої короткочасної пам'яті (Long Short-Term Memory, LSTM). Опис даних для ефективної класифікації трафіку може призвести до виникнення мережевих петель і проблем з пропускною здатністю; вибір LSTM дозволяє проводити точну класифікацію. Схема виявлення в DDoS має набір характеристик трафіку [24]. Ці характеристики відомі як офіційні параметри DoS і включають структуру потоку прибуття і спостережуваний рівень симетрії пакетів на захищену підмережу, де повне захоплення пакетів було

розроблено і реалізовано в системі 20 Гбіт/с (FPC-NM). Наносекундні часові мітки використовуються в системі FPC-NM для значного підвищення точності ретроспективного аналізу подій безпеки.

Система FPC-NM досягла пропускної здатності 17 Гбіт/с з нульовою втратою пакетів при 160 000 підключень. Ці параметри включають прийом пакетів, наносекундне маркування часу, балансування навантаження, попередню обробку пакетів, аналіз протоколів прикладного рівня, зберігання пакетів даних і управління журналами. Використовуючи стиснення LZ4, ця система може досягати швидкості в реальному часі до 10 Гбіт/с і 40 Гбіт/с. Ефективність стиснення і зберігання даних. Однак 70 Гбіт/с і 100 Гбіт/с не підтримуються. Оскільки промисловість і дослідницькі організації будують мережі зі швидкістю 100 Гбіт/с, щоб задовольнити попит на передачу даних, високошвидкісні мережі стають все більш поширеними і представляють собою серйозний технологічний виклик. Системи виявлення вторгнень не можуть ефективно обробляти мережеву активність з високими показниками моніторингу трафіку і втрат пакетів, які безпосередньо впливають на точність виявлення. У цій статті детально описано IDS з відкритим вихідним кодом Snort і Suricata та наведено порівняльні параметри в мережі зі швидкістю 100 Гбіт/с.

Висновки та подальші напрямки. У даній статті розглянуто DDoS-атаки та їхні типи, що можуть виникати у високошвидкісних мережах. Проблема DDoS швидко зростає, а кількість DDoS-атак стрімко збільшується протягом останніх кількох років. У дослідженні також розглядаються різні наявні рішення для виявлення DDoS-атак. До них відносяться механізми відстеження, що підрозділяються на проактивні та реактивні підходи, маркування пакетів, наприклад PPM і DPM, моніторинг постраждалих пакетів даних з використанням експрес-шляхів передавання даних і підвищення точності виявлення з точки зору фільтрації. Також розглянуто аналіз протоколів прикладного рівня для підвищення точності виявлення з погляду моніторингу та фільтрації уражених пакетів даних з використанням експрес-шляхів передачі даних. У статті доведено про зростаючу відмінність між звичайним і нерегулярним трафіком з точки зору DDoS-атак. Крім того, обговорюються вразливі місця високошвидкісних мереж, проблеми і завдання на мережевому рівні для максимального опрацювання пакетів: високошвидкісне опрацювання пакетів, виявлення і захист від DDoS ускладнені, а частота відкидання пакетів висока. Пом'якшення наслідків DDoS у високошвидкісних мережах швидко прогресує, і дослідники розробляють ефективні та інноваційні рішення. Невирішені проблеми та завдання є майбутнім напрямком для виявлення DDoS у високошвидкісних мережах: на основі карти мережевого інтерфейсу 100Gbe було запропоновано різні дослідження для обробки даних на високих швидкостях. Однак у цих дослідженнях часто не враховується швидкість втрати пакетів і управління даними на рівні ядра при використанні 100Gbe.

References

1. Haseeb-Ur-Rehman, R.M.A.; Liaqat, M.; Aman, A.H.M.; Ab Hamid, S.H.; Ali, R.L.; Shuja, J.; Khan, M.K. Sensor cloud frameworks: State-of-the-art, taxonomy, and research issues. *IEEE Sens. J.* **2021**, *21*, 22347–22370.
2. Chaâri, R.; Ellouze, F.; Koubâa, A.; Qureshi, B.; Pereira, N.; Youssef, H.; Tovar, E. Cyber-physical systems clouds: A survey. *Comput. Netw.* **2016**, *108*, 260–278.
3. Cisco, U. Cisco annual internet report (2018–2023) white paper. *Acessado Em.* **2021**, *10*, 1–35.
4. Li, Q.; Meng, L.; Zhang, Y.; Yan, J. DDoS attacks detection using machine learning algorithms. In *International Forum on Digital TV and Wireless Multimedia Communications*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 205–216.
5. Yusof, A.R.a.; Udzir, N.I.; Selamat, A. Systematic literature review and taxonomy for DDoS attack detection and prediction. *Int. J. Digit. Enterp. Technol.* **2019**, *1*, 292–315.

6. Cheng, J.; Xu, R.; Tang, X.; Sheng, V.S.; Cai, C. An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment. *Comput. Mater. Contin.* **2018**, *55*, 95–119.
7. Singh, K.J.; Thongam, K.; De, T. Detection and differentiation of application layer DDoS attack from flash events using fuzzy-GA computation. *IET Inf. Secur.* **2018**, *12*, 502–512.
8. Akbari, E.; Tabatabaei, S.M.; Yazdi, M.B.; Arefi, M.M.; Cao, J. Resilient backstepping control for a class of switched nonlinear time-delay systems under hybrid cyber-attacks. *Eng. Appl. Artif. Intell.* **2023**, *122*, 106128.
9. Zheng, A.; Huang, Q.; Cai, D.; Li, J.; Jing, S.; Hu, W.; Wu, J. Quantitative assessment of stochastic property of network-induced time delay in smart substation cyber communications. *IEEE Trans. Smart Grid* **2019**, *11*, 2407–2416.
10. Ganesh, P.; Lou, X.; Chen, Y.; Tan, R.; Yau, D.K.; Chen, D.; Winslett, M. Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems. *IEEE Trans. Smart Grid* **2021**, *12*, 3581–3593.
11. Ullah, S.; Choi, J.; Oh, H. IPsec for high speed network links: Performance analysis and enhancements. *Future Gener. Comput. Syst.* **2020**, *107*, 112–125.
12. El Sayed, M.S.; Le-Khac, N.-A.; Azer, M.A.; Jurcut, A.D. A Flow Based Anomaly Detection Approach with Feature Selection Method Against DDoS Attacks in SDNs. *IEEE Trans. Cogn. Commun. Netw.* **2022**, *8*, 1862–1880.
13. Papalkar, R.R.; Alvi, A.S. Analysis of Defense Techniques for DDOS Attacks in IoT—A Review. *ECS Trans.* **2022**, *107*, 3061.
14. Naqvi, I.; Chaudhary, A.; Kumar, A. A Systematic Review of the Intrusion Detection Techniques in VANETS. *TEM J.* **2022**, *11*, 900.
15. Almansor, M.; Gan, K. Intrusion detection systems: Principles and perspectives. *J. Multidiscip. Eng. Sci. Stud.* **2018**, *4*, 2458–2925.
16. Rios, V.D.M.; Inacio, P.R.; Magoni, D.; Freire, M.M. Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. *IEEE Access* **2022**, *10*, 76648–76668.
17. Gupta, B.; Chaudhary, P.; Chang, X.; Nedjah, N. Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Comput. Electr. Eng.* **2022**, *98*, 107726.
18. Ennemoser, F.J.; Sattler, P.; Zirngibl, J. State of the Art of DDoS Mitigation Techniques. In Proceedings of the Seminar IITM WS 21/22, Munich, Germany, 30 July–27 February 2022.
19. Falk, H. Building local networks with hubs. *Electron. Libr.* **1997**, *15*, 401–404.
20. Davis, E.L. Fast ethernet: 100BaseTX and 100BaseT4 network interface adaptor architectures. In *Emerging High-Speed Local-Area Networks and Wide-Area Networks*; SPIE: Cergy, France, 1995; pp. 37–41.
21. Adrian, D.; Durumeric, Z.; Singh, G.; Halderman, J.A. Zippier ZMap: Internet-Wide Scanning at 10 Gbps. In Proceedings of the WOOT 8th USENIX Workshop on Offensive Technologies, San Diego, CA, USA, 19 August 2014.
22. Arashloo, M.T.; Lavrov, A.; Ghobadi, M.; Rexford, J.; Walker, D.; Wentzlaff, D. Enabling Programmable Transport Protocols in High-Speed NICs. In Proceedings of the NSDI, 17th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, USA, 25–27 February 2020; pp. 93–109.
23. Naeem, M.; Jamal, T.; Diaz-Martinez, J.; Butt, S.A.; Montesano, N.; Tariq, M.I.; De-la-Hoz-Franco, E.; De-La-Hoz-Valdiris, E. Trends and future perspective challenges in big data. In *Advances in Intelligent Data Analysis and Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 309–325.
24. Zubaroğlu, A.; Atalay, V. Data stream clustering: A review. *Artif. Intell. Rev.* **2021**, *54*, 1201–1236.