ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2024-80-36
УДК 004.056.53:004.85

ЯНКО Аліна
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
https://orcid.org/0000-0003-2876-9316
e-mail: al9_yanko@ukr.net
ПРОКУДІН Андрій
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
https://orcid.org/0009-0008-2165-8457
e-mail: auprokudin@gmail.com
ФІЛЬ Ілля
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
https://orcid.org/0000-0003-4582-1163
e-mail: Kentlovesread@gmail.com
КРУК Олег
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
https://orcid.org/0009-0004-4241-2676
e-mail: olegkruk1975@gmail.com

ВИЯВЛЕННЯ АТАК ТИПУ LDDOS ЗА ДОПОМОГОЮ SDN МЕРЕЖ З ЕЛЕМЕНТАМИ МАШИННОГО НАВЧАННЯ

Стаття присвячується виявленню розподілених атак на відмову в обслуговуванні (DDoS), які є серйозною загрозою для комп'ютерних мереж. У даному дослідженні розглянуто можливість виявлення атак типу low-rate DDoS з використанням машинного навчання на основі програмно-конфігурованих мереж (SDN). Технології машинного навчання (ML) та глибинного навчання (DL) у поєднанні з SDN демонструють значний потенціал у ефективній протидії цим мережевим загрозам. Попередні дослідження переважно зосереджувались на високочастотних DDoS-атаках, ігноруючи низькочастотні DDoS-атаки, які схожі на легітимний трафік, та часто використовували застарілі набори даних. Незважаючи на те, що дослідники використовують різні алгоритми офлайн-навчання для виявлення DDoS-атак, онлайн-класифікатори навчання залишаються недостатньо дослідженими. Мета дослідження – запропонувати модель виявлення вторгнень, адаптовану для SDN-мереж, з використанням онлайн-класифікатора пасивно-агресивного навчання. У рамках дослідження було детально описуємо запропоновану методологію, включаючи етапи офлайн та онлайн навчання. Запропонована модель досягає середнього показника виявлення 99,7% для нормального та DDoS-трафіку, перевершуючи аналогічні моделі на кількох наборах даних, ефективно виявляючи та локалізуючи DDoS-атаки.

Ключові слова – виявленню атак; машинне навчання; модель виявлення вторгнень; низькошвидкісні атаки; програмно-конфігурована мережа; розподілена атака на відмову в обслуговуванні.

YANKO Alina, PROKUDIN Andrii, FIL Illia, KRUK Oleg
National University «Yuri Kondratyuk Poltava Polytechnic»

DETECTION OF LDDOS ATTACKS USING SDN NETWORKS WITH MACHINE LEARNING ELEMENTS

The article is devoted to the detection of distributed denial-of-service (DDoS) attacks, which pose a serious threat to computer networks. This study explores the possibility of detecting low-rate DDoS attacks using machine learning based on software-defined networking (SDN). The research is conducted on the basis of the application of the latest approach to the deployment of corporate networks, using virtualization technology using SDN networks. This enables centralized management of the network architecture, regardless of its complexity, thanks to a software-based controller. SDN is implemented on the basis of the OpenFlow protocol, which manages traffic: redirects, allows or prohibits the flow based on established policies. Machine learning (ML) and deep learning (DL) technologies, combined with SDN, demonstrate considerable capability to efficiently counter these network threats. Previous research has mainly focused on high-frequency DDoS attacks, ignoring low-frequency DDoS attacks that resemble legitimate traffic and frequently used legacy datasets. Although researchers utilize multiple offline learning algorithms to detect DDoS attacks, online learning classifiers are still insufficiently studied. The aim of the research is to propose an intrusion detection model adapted for SDN networks using an online passive-aggressive learning classifier. The effectiveness of the proposed model in detecting low-rate DDoS attacks while maintaining a low level of false positives is evaluated using different data sets, including specially simulated traffic scenarios The suggested model attains an average detection rate of 99.7% for both normal and DDoS traffic, outperforming similar models on multiple datasets, and effectively detecting and localizing DDoS attacks. The proposed model will contribute to the development of effective mechanisms for detecting and responding to low-rate DDoS attacks in SDN networks.

Keywords: attack detection; machine learning; intrusion detection model; low-rate DDoS attacks; software-defined network; distributed denial of service.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Програмно-конфігуровані мережі (SDN) – це сучасна мережева архітектура, розроблена для подолання обмежень традиційних мереж [1]. SDN забезпечують швидку конфігурацію, масштабованість та управління через динамічну, програмовану архітектуру, що перевершує традиційні обмеження мереж. Відокремлюючи площину управління, яка відповідає за маршрутизацію та інтерфейси, від площини даних, яка обробляє перенаправлення трафіку, SDN пропонує більшу гнучкість та здатність реагувати на змінювані вимоги. Крім того, SDN забезпечує налаштування мережі, уніфіковані можливості управління та глобальний огляд топології мережі на рівні контролера [2, 3], що робить її популярним вибором у різних секторах. Однак SDN не є захищеною від вразливостей безпеки, які можуть бути використані в її архітектурних площинах. Виявлення розподілених атак на відмову в обслуговуванні (DDoS) залишається складним завданням, яке загрожує як традиційним, так і SDN-мережам.

Атаки DDoS становлять зростаючу та складну проблему, яка посилюється з розвитком Інтернету, включаючи Інтернет речей (IoT) та технологію п'ятого покоління (5G) [4]. Ці надзвичайно руйнівні атаки націлені на конкретні сегменти мережі для порушення нормальних системних сервісів.

Низькошвидкісні атаки low-rate DDoS (LDDoS) нещодавно з'явилися як окремий тип, що відрізняється від традиційних високошвидкісних і об'ємних DDoS-атак. Атаки LDDoS відправляють пакети з такою швидкістю, що вона не перевищує пропускну здатність мережі або системи, намагаючись використати вразливості та перевантажити ресурси протягом тривалішого періоду. Виявлення атак LDDoS є складним завданням, оскільки вони генерують трафік нижче порогу звичайних методів виявлення аномалій [5].

Технології машинного навчання (ML) та глибинного навчання (DL) у поєднанні з SDN демонструють значний потенціал у ефективній протидії цим загрозам. Хоча техніки машинного навчання вже застосовувалися для виявлення атак LDDoS у мережах на базі SDN, багато наявних підходів орієнтовані на пакетну обробку і не мають можливостей для роботи в реальному часі [6]. Щоб вирішити ці проблеми, у цій статті пропонується онлайн-модель машинного навчання з використанням пасивно-агресивного (PA) класифікатора [7] для виявлення атак LDDoS у мережах на базі SDN. Запропонована модель обробляє великі обсяги даних мережевого трафіку в реальному часі та поступово оновлює параметри моделі з використанням PA класифікатора. Необхідно оцінювати продуктивність моделі на кількох наборах даних, включаючи CICDDoS2019 [8], InSDN [9], slow-read-DDoS [10], а також на спеціально створеному наборі даних, згенерованому зі змодельованих сценаріїв мережевого трафіку за допомогою Mininet [11] і контролера Ryu [12]. Наші результати демонструють, що запропонована модель досягає високої точності та перевершує існуючі методи виявлення атак LDDoS у мережах на базі SDN.

Мета дослідження – запропонувати модель виявлення вторгнень, адаптовану для SDN-мереж, з використанням онлайн-класифікатора пасивно-агресивного навчання (PA). Для досягнення поставленої мети були визначені наступні завдання:

– розробити онлайн-модель для виявлення атак LDDoS у мережах на базі SDN;
– оцінити ефективність запропонованої моделі у виявленні атак LDDoS при підтримці низького рівня хибних спрацювань, використовуючи різні набори даних, включаючи спеціально змодельовані сценарії трафіку;
– продемонструвати переваги запропонованої моделі порівняно з існуючими методами у виявленні та пом'якшенні атак LDDoS.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Атаки розподіленої відмови в обслуговуванні з низьким рівнем трафіку (LDDoS) стали значною загрозою для безпеки мереж через їхню здатність обходити традиційні методи виявлення DDoS-атак [13]. LDDoS-атаки працюють на низьких рівнях трафіку, що дозволяє їм уникати виявлення традиційними методами. Наскільки нам відомо, обмежена кількість досліджень була проведена щодо виявлення LDDoS-атак у мережах на базі SDN. Попередні дослідження розглядали різні підходи, включаючи методи на основі машинного навчання, статистичні техніки та гібридні підходи. Однак наявна література в цій конкретній області є досить обмеженою.

Підходи на основі машинного навчання показали обнадійливі результати у виявленні LDDoS-атак завдяки їхній здатності навчатися на історичних шаблонах трафіку і виявляти аномалії. Наприклад, Cheng та ін. [14] пропонують підхід на основі машинного навчання для виявлення LDDoS-атак у мережах IoT на базі SDN. Запропонований метод використовує алгоритми машинного навчання для виявлення LDDoS-атак, які є особливо складними для виявлення через їхню схожість із легітимним мережевим трафіком. Використовуючи програмовану архітектуру SDN та централізоване управління, модель обробляє великі обсяги даних у режимі реального часу, що робить її придатною для мереж IoT з різноманітними шаблонами трафіку. Експериментальні результати демонструють ефективність підходу у точному виявленні низькошвидкісних DDoS-атак у мережах IoT на базі SDN. Однак запропонований метод є неефективним за

умов мінливих мереж IoT, таких як зміна шаблонів трафіку та динамічні топології мереж, що впливає на продуктивність моделі.

Nadeem та ін. [15] вирішили проблему виявлення LDDoS-атак у середовищах SDN. Запропонований метод базується на рекурентних нейронних мережах (RNN) для інтелектуального виявлення LDDoS-атак. RNN використовує особливості правил потоку для виявлення і інтегрована в SDN-контролер, а її розгортання у віртуально-реальному мережевому середовищі за допомогою контролера Ryu та Mininet демонструє її ефективність. Однак дослідження використовувало обмежений набір даних і оцінювало підхід лише у змодельованому середовищі, що може не відображати точно реальні сценарії.

Tang та ін. [16] пропонують легку і реальну часову систему під назвою "Продуктивність та Особливості" (P&F). P&F використовує машинне навчання для аналізу особливостей трафіку, отриманих за допомогою OpenFlow, і класифікує їх на дві категорії. Система визначає ефективність атак LDoS на основі продуктивності нормального трафіку у станах атаки (P) і виявляє джерела атак та жертв, використовуючи особливості потоків (F) на основі частотно-часового аналізу. P&F встановлює відповідні схеми пом'якшення на основі результатів виявлення та локалізації. Експериментальні результати демонструють, що P&F досягає високих показників виявлення та низького рівня хибних спрацювань при виявленні атак LDoS. Однак дослідження використовувало обмежений набір даних і не оцінювало ефективність підходу проти атак "нульового дня". Крім того, підхід може бути не ефективним у реальних сценаріях, бо він базується на статистичних особливостях, які можуть не враховувати всю складність мережевого трафіку.

Таблиця 1 надає порівняння пов'язаних робіт. На відміну від інших підходів, запропонована модель з використанням онлайн-машинного навчання і пасивно-агресивного (PA) класифікатора може обробляти великі обсяги даних у режимі реального часу та створювати інтерпретовану модель з високою точністю, без обмежень інших підходів.

Таблиця 1

Порівняння пов'язаних робіт, обговорених у цьому розділі

Автори	Підхід до дослідження	Метрологія виявлення	Обмеження
Cheng та ін. [14]	Підхід на основі машинного навчання	Використання алгоритмів машинного навчання	Неефективність у змінних умовах IoT-мереж, обмежена оцінка реальних сценаріїв
Nadeem та ін. [15]	Підхід на основі RNN	Використання особливостей правил потоку та RNN	Потребує великої кількості навчальних даних і обчислювальних ресурсів, обмежене використання набору даних, можлива неточність у реальних умовах
Tang та ін. [16]	Продуктивність та особливості фреймворку	Машинне навчання з використанням особливостей OpenFlow	Обмежене використання набору даних, відсутня оцінка для атак нульового дня, може не враховувати складність мереж у реальних умовах
Запропонований підхід	Онлайн машинне навчання	Аналіз трафіку на основі потоків і пакетів, PA-класифікатор.	–

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У цьому розділі надається огляд програмно-визначених мереж (SDN), низькошвидкісних DDoS-атак та пасивно-агресивного класифікатора (PA).

Програмно-визначені мережі (SDN). SDN – це революційна архітектура, яка вирішує обмеження традиційних мереж. Вона відокремлює площини управління та передачі даних, дозволяючи централізоване управління через SDN-контролер. Це забезпечує більшу гнучкість, масштабованість і спрощене управління мережею. Адміністратори можуть легко розгортати пристрої від різних виробників і динамічно налаштовувати конфігурації відповідно до змінних вимог [17].

Архітектура SDN складається з трьох рівнів (шарів): інфраструктура, управління та застосування, що відповідають моделі OSI.

SDN-контролер приймає рішення, які виконуються на рівні передачі даних у всіх пристроях. Application Layer виконує специфічні функції, що відповідають вимогам IoT, та сприяє виконанню завдань, таких як хмарне зберігання даних і підключення за схемою "клієнт-сервер". Тобто SDN забезпечує комплексний огляд мережі, що дозволяє легко та ефективно керувати нею.

Атака розподіленої відмови в обслуговуванні з низьким рівнем трафіку (LDDoS). LDDoS є різновидом DDoS-атаки, що використовує інший метод. Замість того, щоб перевантажувати ціль великим потоком даних, LDDoS спрямовує невелику кількість шкідливого трафіку, що складає лише 20% або менше від загального мережевого трафіку. Такий низький рівень атаки дозволяє їй приховуватися серед нормального трафіку, що ускладнює її виявлення [18, 19]. Для вирішення проблеми виявлення LDDoS-атак дослідники запропонували різні методи. У дослідженні [5] представлено глибокий аналіз виявлення LDDoS-атак у програмно-визначених мережах.

Сучасні методи виявлення поділяються на три категорії: виявлення за ознаками, виявлення у часовій області та виявлення у частотній області. Виявлення за ознаками створює набір даних із відомими характеристиками LDDoS-атак і оцінює поточні потоки на наявність можливих атак. Методи у частотній області використовують мультифрактальні ознаки та техніки, як-от спектральний аналіз і вейвлет-перетворення, для виявлення змін у частотній області, що вказують на LDDoS-атаку. Виявлення у часовій області порівнює обчислені значення з пороговими значеннями, використовуючи алгоритми, як-от автокореляція, для виявлення атакуючих потоків [20].

Онлайн машинне навчання. Онлайн машинне навчання – це тип машинного навчання, у якому модель навчається на даних, які безперервно надходять у систему. У процесі онлайн-навчання модель отримує послідовність нових даних і оновлює свої прогнози або дії на основі нової інформації. Цей процес повторюється з часом, коли модель отримує більше даних, що дозволяє їй адаптуватися та покращувати свою продуктивність [21].

Онлайн навчання часто використовується в застосунках, де дані постійно створюються/оновлюються, як-от потоки даних у реальному часі, і де неможливо дочекатися повного набору даних для початку навчання. Однією з головних переваг онлайн-навчання є те, що воно може бути більш ефективним і масштабованим, ніж традиційне офлайн навчання, оскільки модель може почати навчатися і робити прогнози майже одразу, замість того, щоб чекати на всі дані [22].

Як показано на рисунку 1а, офлайн навчання передбачає навчання моделі на всіх доступних даних із подальшим її збереженням і розгортанням без подальшого навчання. Цей процес може зайняти багато часу, особливо при роботі з великими обсягами даних. Модель навчається і тестується на доступних їй даних, після чого розгортається. Після розгортання модель може бути оновлена, але вона не буде продовжувати навчатися на нових даних. При оновленні моделі навчання партіями важливо враховувати час, необхідний для навчання.

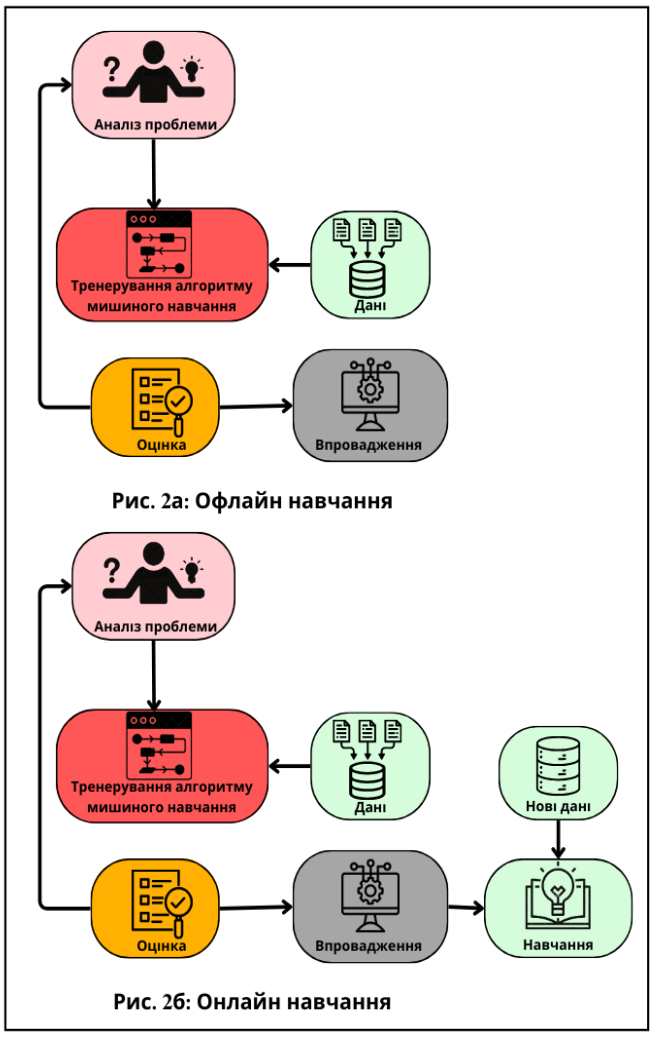

Рис. 1. Офлайн/Онлайн машинне навчання

Дивлячись на рисунку 1б, онлайн-навчання – це тип машинного навчання, у якому модель постійно оновлюється невеликими обсягами нових даних, коли вони стають доступними. Це дозволяє моделі постійно навчатися і адаптуватися до змін у патернах даних. Ось основні кроки в онлайн-навчанні:

– Модель навчається і розгортається з невеликою кількістю даних.

– Коли нові дані стають доступними, модель оновлюється невеликими обсягами цих даних, це можуть бути як окремі точки даних, так і міні-пакети.

– Модель продовжує навчатися і адаптуватися до змін у патернах даних навіть після її розгортання.

Онлайн-навчання особливо корисне у ситуаціях, коли дані, що обробляються, постійно змінюються, наприклад, при виявленні DDoS-атак. Система виявлення DDoS-атак повинна бути здатна швидко адаптуватися до нового трафіку, тому модель навчання, яке може постійно оновлюватися, є надзвичайно важливою та корисною. Необхідно враховувати дані, що надходять, і те, як їх можна використовувати для оновлення моделі в режимі реального часу.

Класифікатор Passive Aggressive (PA). Класифікатор Passive Aggressive (PA) – це алгоритм машинного навчання, що використовується для задач бінарної класифікації, зокрема для виявлення DDoS-атак. Він відмінно підходить для онлайн-навчання, постійно оновлюючи свою модель у міру надходження нових даних. Класифікатор PA агресивно оновлює модель, коли вона робить неправильні прогнози, водночас підтримуючи пасивний підхід до навчання [23]. Він ідеально підходить для виявлення DDoS-атак у реальному часі, оскільки ефективно адаптується до змін у мережевих патернах. Класифікатор використовує вектори ознак, що представляють атрибути мережевого трафіку, і оцінює, чи відповідає вхідний потік нормальному трафіку або атаці DDoS.

У контексті виявлення LDDoS-атак у програмно-визначених мережах (SDN), класифікатор PA пропонує кілька переваг. Він дозволяє здійснювати обробку в реальному часі та ефективно використовувати обчислювальні ресурси, що робить його придатним для обробки великих обсягів мережевого трафіку.

Дане дослідження представляє новий підхід до онлайн-виявлення LDDoS-атак у SDN-мережах. Запропонована модель базується на онлайн-класифікаторі Passive Aggressive (PA), що дозволяє точно та ефективно виявляти LDDoS-атаки.

Архітектура моделі. Запропонована модель онлайн-навчання використовує класифікатор PA для ефективного виявлення LDDoS-атак у SDN-мережах. Модель розроблена для обробки великих обсягів мережевого трафіку в режимі реального часу та поступового оновлення своїх параметрів. Запропонований алгоритм, зображений на рисунку 2, що включає наступні етапи:

1. *Збір даних*. Збір даних з двох джерел. По-перше, використовуємо набори даних, такі як CICDDoS2019, InSDN та slow-read-DDoS, які містять різні типи DDoS-атак. Ці набори даних включають як легітимні, так і зловмисні записи, що дозволяє забезпечити комплексне розуміння нормальної поведінки системи і виявлення як відомих, так і нових шаблонів атак. По-друге, створюємо власний набір даних мережевого трафіку в SDN-мережах, включаючи звичайний трафік і LDDoS-атаки. Для збору даних симулюємо SDN-середовище за допомогою Mininet і контролера Ryu.

2. *Обробка даних*. Для забезпечення точності моделі проводимо обробку зібраних даних, видаляючи нерелевантні ознаки та нормалізуючи їх. Також виконуємо дослідницький аналіз даних для підготовки даних до класифікатора PA. Етапи обробки включають роботу з відсутніми даними та колонками, трансформацію сирих даних у вдосконалені набори і встановлення єдиних типів ознак для всіх наборів даних.

3. *Навчання моделі*. Модель онлайн-навчання складається з двох етапів: онлайн-навчання і офлайн-навчання. На етапі офлайн-навчання основні набори даних використовуються для навчання моделі та створення первинної бази даних з вже обробленим трафіком. Етап онлайн-навчання постійно навчає модель на нових даних або трафіку, по одному зразку за раз. Оптимізатор PA поступово оновлює параметри моделі, що дозволяє в реальному часі розпізнавати нові дані.

4. *Оцінка моделі*. Запропонована модель була оцінена з використанням різних наборів даних, включаючи CICDDoS2019, InSDN, slow-read-DDoS і власний набір даних. Для оцінки продуктивності моделі використовуює такі характеристики, як точність, рівень втрат, точність (precision), повнота (recall) і F1-міра. Процес оцінки дозволяє приймати практичні рішення на основі результатів моделі.

5. *Розгортання*. Модель розгортається в SDN-мережі для виявлення LDDoS-атак в реальному часі. Інтеграція в мережеву інфраструктуру включає налаштування моделі для моніторингу мережевого трафіку з метою виявлення LDDoS-атак. Тестування і налаштування моделі забезпечують її ефективність у реальному середовищі. Безперервний моніторинг і оновлення підтримують ефективність моделі у виявленні LDDoS-атак.

6. *Інкрементальне навчання*. Для ефективного використання обчислювальних ресурсів і навчання моделі на передбачуваних LDDoS-атаках необхідно було поступово оновлювати її параметри з використанням нових даних. Це дозволяє обробляти дані в реальному часі та забезпечує еволюцію моделі

ISSN 2219-9365

шляхом поступового навчання на послідовних випадках даних, що дозволяє швидко виявляти LDDoS-атаки у реальному часі.

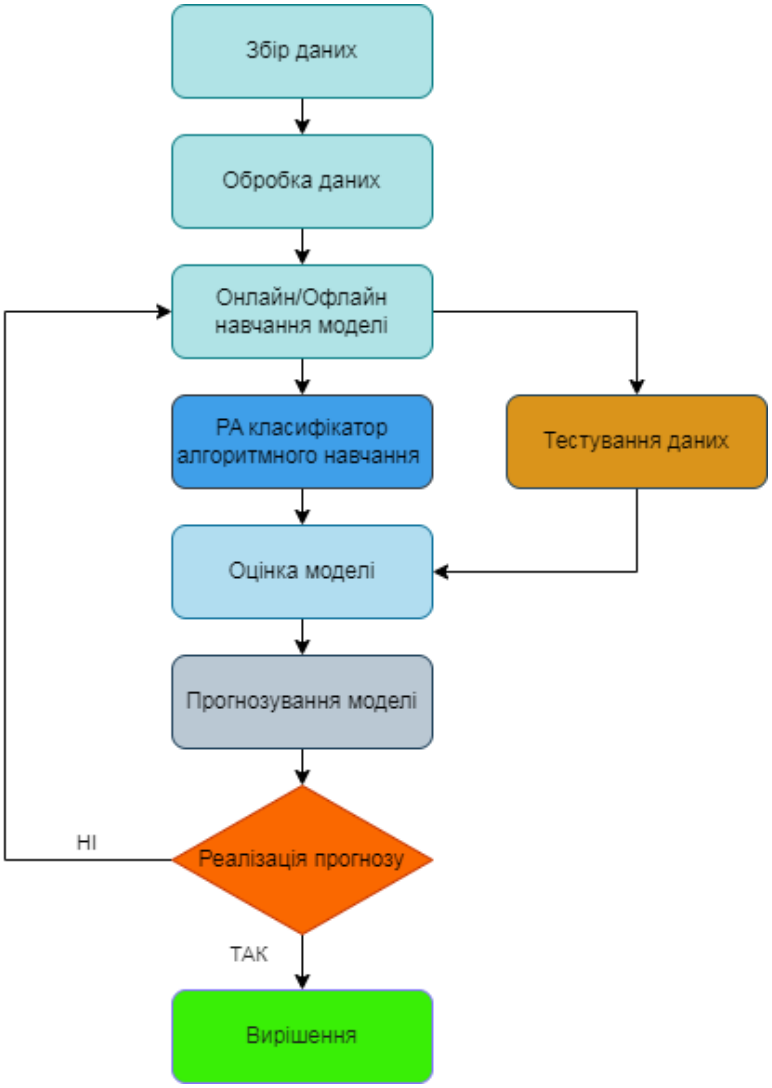

Рис. 2. Запропонований алгоритм

Онлайн-навчання запропонованої моделі. Після завершення етапу офлайн-навчання, що включає навчання моделі на основних наборах даних і створення первинної бази даних з обробленим трафіком, модель онлайн-навчання бере на себе подальшу роботу. Рисунок 3 ілюструє псевдокод для процесу онлайн-навчання класифікатора PA .

У псевдокоді дані представляють вхідні вектори ознак, а мітки представляють відповідні правильні мітки (1 для позитивного класу, -1 для негативного класу). Параметр регуляризації контролює агресивність оновлень, а max_iterations визначає кількість проходів через увесь набір даних.

Під час процесу онлайн-навчання класифікатор PA поступово оновлює вектор ваг **w** і зміщення *b* для кожного екземпляра в наборі даних. Якщо екземпляр класифіковано неправильно, модель виконує агресивне оновлення, щоб виправити помилку. Швидкість навчання *alpha* обчислюється на основі втрат і параметрів регуляризації, що забезпечує правильне коригування ваг і зміщень моделі. Процес онлайн-навчання дозволяє класифікатору PA адаптуватися до нових даних і постійно покращувати свою продуктивність з надходженням нових екземплярів у модель.

```
Function online_PA_training(data, labels,
regularization_parameter, max_iterations):
  Initialize weight vector w with zeros or small random values
  Initialize bias term b to 0
  for iteration in range(max_iterations):
    for i in range(len(data)):
      instance = data[i]
      true_label = labels[i]
      prediction = sign(w • instance + b)
      loss = max(0, 1 - true_label * (w • instance + b))
      if loss > 0:
        alpha = loss / (||instance||^2 + 1 / (2 *
regularization_parameter))
        w = w + alpha * true_label * instance
        b = b + alpha * true_label
  return w, b
```

Рис. 3. Псевдокод процесу онлайн-навчання PA

Результати та обговорення

У цьому розділі описуються експериментальні налаштування та результати, отримані від запропонованої онлайн-моделі машинного навчання з використанням класифікатора PA для виявлення атак LDDoS у мережах на базі SDN.

Експериментальні налаштування. Провівши експерименти в симуляторі Mininet було створено топологію мережі Fat-tree за допомогою API на Python, як показано на рисунку 4. Топологія складалася з одного контролера Ryu (C_1), десяти комутаторів OpenFlow $(S_{1...10})$ і вісімдесяти хостів $(h_{1...80})$. Пропускні здатності були налаштовані на 10 Мбіт/с і 100 Мбіт/с, що відповідає Ethernet та Fast Ethernet підключенням. Та було згенерувано нормальний трафік за допомогою Ping і атаки LDDoS за допомогою Scapy.

Python та scikit-learn було використано для реалізації запропонованої моделі. Алгоритм AP було задіяно для онлайн-навчання моделі. Тренувальний набір даних складався з 100 000 зразків, причому 70% використовували для навчання і 30% для тестування. Нормалізацію було застосовано за допомогою методу мінімально-максимальної нормалізації, як показано у рівнянні:

$$x_i' = \frac{x_i - \min x_i}{\max x_i - \min x_i}. \quad (1)$$

Метрики продуктивності. При оцінці продуктивності моделі були використані наступні характеристики:

Точність (accuracy) вимірює пропорцію правильно класифікованих екземплярів і служить метрикою оцінки в цьому дослідженні. Продуктивність класифікаційної моделі оцінювалася за різними параметрами, зосереджуючись на точності для вимірювання однокласової точності моделі. Точність запропонованої онлайн-моделі визначається за допомогою рівняння:

$$Точність = \frac{(tp + tn)}{(tp + fp + tn + fn)}, \quad (2)$$

Де, символи *tp*, *tn*, *fp* та *fn* позначають:

1. *tp* (true positive) – істинно позитивні: кількість правильно класифікованих позитивних випадків (наприклад, атаки, які правильно ідентифіковані як атаки).
2. *tn* (true negative) – істинно негативні: кількість правильно класифікованих негативних випадків (наприклад, нормальний трафік, який правильно ідентифікований як нормальний).
3. *fp* (false positive) – хибно позитивні: кількість нормальних випадків, помилково класифікованих як атаки.
4. *fn* (false negative) – хибно негативні: кількість атак, помилково класифікованих як нормальний трафік.

Ці показники використовуються для розрахунку таких характеристик, як точність, повнота та F1-міра, що допомагають оцінити якість моделі.

Точність *класифікації* ***(Precision)*** визначається як частка істинно позитивних випадків (true positives) серед усіх передбачених позитивних випадків. Для запропонованої онлайн-моделі точність розраховувалася за рівнянням:

$$Точність = \frac{(tp + tn)}{(tp + fp + tn + fn)}. \quad (3)$$

Повнота *(recall),* також відома як чутливість або істинно позитивний рівень, вимірює пропорцію істинно позитивних результатів серед усіх фактичних позитивних. У контексті запропонованої онлайн-моделі повнота обчислюється за допомогою рівняння:

$$Повнота = \frac{tp}{(tp + fn)'}. \quad (4)$$

F1-міра є збалансованою мірою продуктивності, яка обчислюється як гармонійне середнє між точністю та повнотою. У випадку запропонованої онлайн-моделі F1-міра отримується за допомогою рівняння:

$$F1-міра = \frac{2 \times Точність \times Повнота}{Точність + Повнота}. \quad (5)$$

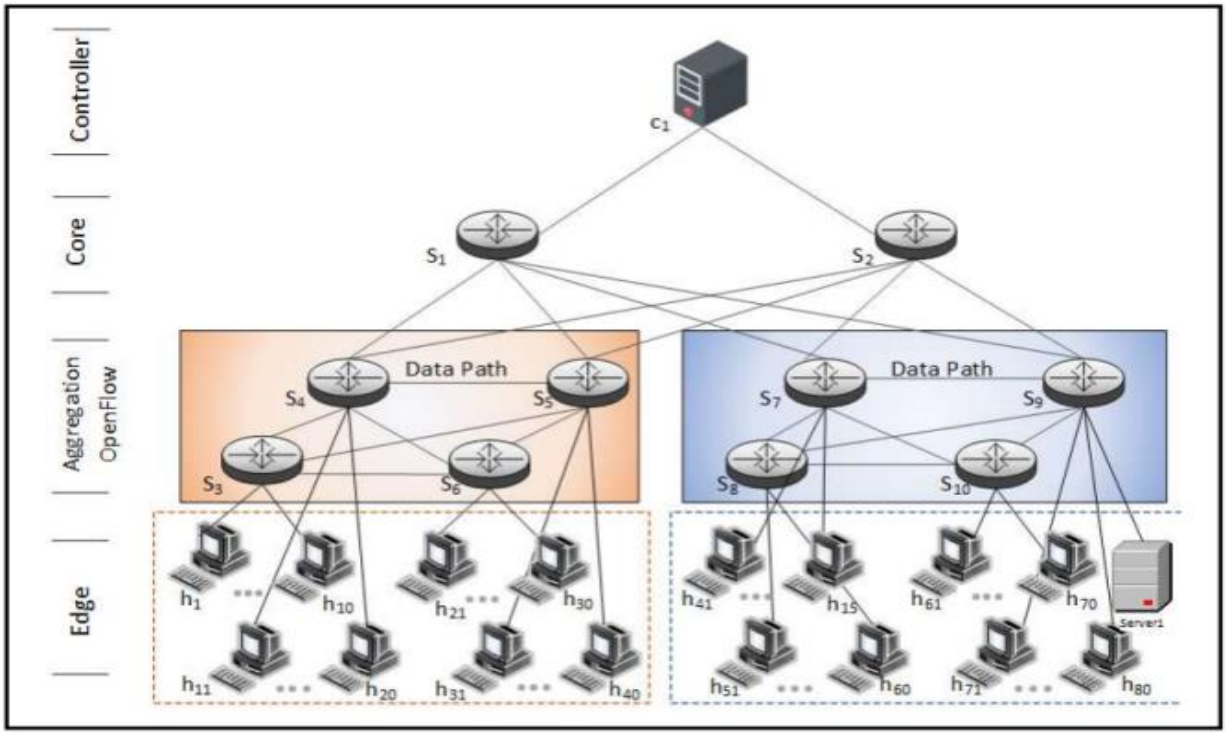

Рис. 4. Топологія мережі використаної в експерименті

Розглянемо характеристики продуктивності запропонованої моделі на навчальних і валідаційних даних для чотирьох наборів даних: **CICDDoS2019, InSDN, slow-read-DDoS** і власного набору даних. Оцінені метрики включають точність (accuracy), рівень втрат (loss rate), точність клас. (precision), повноту

(recall) та F1-міру (F1-score). Результати продуктивності методу, використаного в цьому дослідженні, візуалізовані на Рисунку 5.

Результати запропонованої онлайн-моделі на навчальних даних **CICIDS2019** досягли точності 99% при низькому рівні втрат 0.25%. Модель також показала високу точність (0.975), повноту (0.966) та F1-міру (0.969), що відображено на рисунку 5а. Подібним чином, на навчальних даних **InSDN** модель досягла високої точності (98%) і низького рівня втрат (0.325%), з показниками точності, повноти та F1-міри 0.987, 0.985 і 0.98 відповідно, як показано на рисунку 5б.

На навчальних даних набору даних **slow-read-DDoS** запропонована онлайн-модель ЕВМ досягла високої точності (97%) і низького рівня втрат (0.22%). Модель показала високу точність (0.989), повноту (0.942) і F1-міру (0.929), як показано на рисунку 5в. Результати на навчальних даних власного набору даних були ще кращими: висока точність (99%), низький рівень втрат (0.12%), точність (0.979), повнота (0.992) та F1-міра (0.989), що показано на рисунку 5г.

Результати валідації запропонованої моделі були узгодженими з результатами навчання, що свідчить про те, що модель добре узагальнює нові дані. Продуктивність моделі також була конкурентоспроможною порівняно з іншими сучасними моделями, описаними в літературі. Загалом, експериментальні результати показують, що запропонована онлайн-модель машинного навчання є ефективною для виявлення LDDoS-атак у мережах на базі SDN з високою точністю та низьким рівнем хибно-позитивних спрацьовувань.

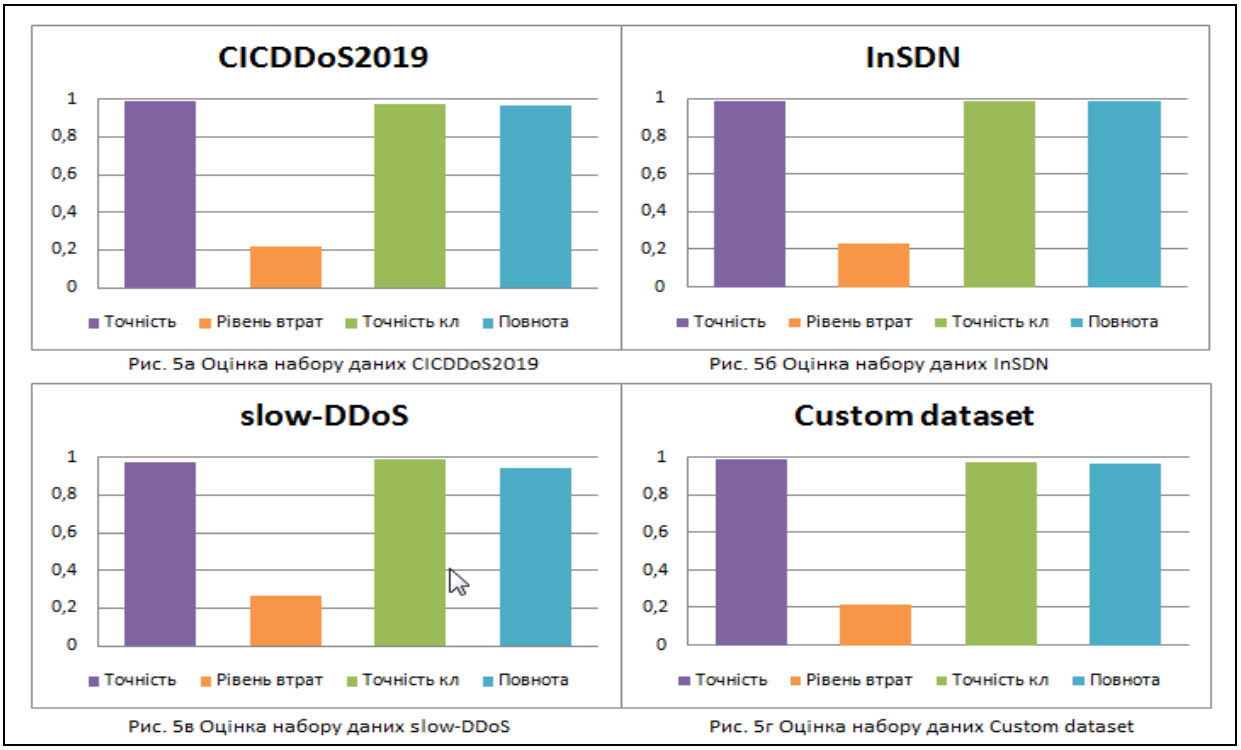

Рис. 5а Оцінка набору даних CICDDoS2019

Рис. 5б Оцінка набору даних InSDN

Рис. 5в Оцінка набору даних slow-DDoS

Рис. 5г Оцінка набору даних Custom dataset

Рис. 5. Характеристики продуктивності запропонованої моделі

Порівнявши продуктивність запропонованої моделі з існуючими методами, описаними в літературі, робимо висновок, що запропонована модель перевершила існуючі методи за точністю, повнотою, точністю та F1-мірою.

Запропонована модель досягла високої точності, низького рівня втрат, а також високих значень precision, recall та F1-міра на навчальних даних. Крім того, здатність моделі безперервно навчатися на нових вхідних даних і адаптуватися до змін у мережі робить її більш придатною для використання в динамічних мережевих середовищах у порівнянні з традиційними методами машинного навчання, які потребують періодичного перенавчання.

У порівнянні з іншими методами на основі машинного навчання, такими як дерево рішень, KNN та SVM, запропонована модель має переваги в точності та інтерпретованості. Також, модель можна навчати за допомогою алгоритму PA, який є поширеним і ефективним методом оптимізації, що підходить для великих наборів даних.

Одним із можливих обмежень моделі є те, що для її навчання та використання може знадобитися більше обчислювальних ресурсів у порівнянні з простішими методами, такими як дерево рішень або KNN.

Однак це компенсується тим, що модель може працювати в режимі онлайн-навчання, що дозволяє їй адаптуватися до змін у мережевих умовах без необхідності періодичного перенавчання.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У цій статті було запропоновано унікальну модель онлайн машинного навчання, використовуючи класифікатор PA, для виявлення LDDoS-атак у мережах на основі SDN. Запропонована модель досягла високої точності та низької втрати на тренувальних даних. У порівнянні з іншими дослідженнями, модель показала значні переваги щодо точності та ефективності. Проте, є деякі обмеження. По-перше, модель тестувалася в симульованому середовищі за допомогою Mininet, що може не повністю відображати складність реальних SDN-мереж. По-друге, модель оцінювалася лише на LDDoS-атаках, але вона може показати і інші результати для різних типів атак.

У майбутніх дослідженнях планується протестувати дану модель у реальному середовищі та оцінити її продуктивність на ширшому діапазоні атак. Також потрібно дослідити використання інших алгоритмів онлайн машинного навчання та можливі переваги комбінування кількох алгоритмів для підвищення точності та ефективності. Додатково, потрібно дослідити інтеграцію моделі з існуючими системами безпеки у SDN-мережах.

Отже, запропонована структура демонструє багатообіцяючі результати у виявленні LDDoS-атак у мережах на основі SDN. Дана модель сприятиме розвитку ефективних механізмів виявлення та реагування на такі атаки в SDN мережах.

Література

1. D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S.Azodolmolky,andS.Uhlig,"Software-defined networking:A comprehensive survey,"*Proceedings of the IEEE,* vol. 103, no.1, pp. 14-76, 2014.
2. L. Zhu *et al.,* "SDN controllers: A comprehensive analysis andperformance evaluation study,"*ACM Computing Surveys(CSUR),* vol. 53, no. 6, pp. 1-40, 2020.
3. A.A.Alashhab,M.S.M.Zahid,A.A.Barka,andA.M.Albaboh,"Experimenting and evaluating the impact of DoS attacks ondifferent SDN controllers," in *2021 IEEE 1st InternationalMaghrebMeetingoftheConferenceonSciencesandTechniquesofAutomaticControlandComputerEngineeringMI-STA*,2021:IEEE, pp. 722-727.
4. F.S.DantasSilva,E.Silva,E.P.Neto,M.Lemos,A.J.VenancioNeto, and F. Esposito, "A taxonomy of DDoS attack mitigationapproaches featured by SDN technologies in IoT scenarios,"*Sensors,* vol. 20, no. 11, p. 3078, 2020.
5. A. A. Alashhab, M. S. M. Zahid, M. A. Azim, M. Y. Daha, B.Isyaku, and S. Ali, "A Survey of Low Rate DDoS DetectionTechniques Based on Machine Learning in Software-DefinedNetworks,"*Symmetry,* vol. 14, no. 8, p. 1563, 2022.
6. N.Tantalaki,S.Souravlas,andM.Roumeliotis,"Areviewonbigdata real-time stream processing and its scheduling techniques,"*International Journal of Parallel, Emergent and DistributedSystems,* vol. 35, no. 5, pp. 571-601, 2020.
7. K. Crammer, O. Dekel, J. Keshet, S. Shalev-Shwartz, and Y.Singer, "Online passive aggressive algorithms," 2006.
8. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani,"Developingrealisticdistributeddenialofservice(DDoS)attackdataset and taxonomy," in *2019 International CarnahanConferenceonSecurityTechnology(ICCST)*,2019:IEEE,pp.1-8.
9. M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: Anovel SDN intrusion dataset,"*Ieee Access,* vol. 8, pp. 165263-165284,2020.
10. N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Pérez-Díaz,and D. F. Carrera, "A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcementlearning,"*Journal of Network and Computer Applications,* vol.205, p. 103444, 2022.
11. N. Handigol, B. Heller, V. Jeyakumar, B. Lantz, and N.McKeown,"Reproduciblenetworkexperimentsusingcontainer-based emulation," in *Proceedings of the 8th internationalconference on Emerging networking experiments andtechnologies*, 2012, pp. 253-264.
12. S. Asadollahi, B. Goswami, and M. Sameer, "Ryu controller'sscalability experimenton softwaredefined networks," in*2018 IEEE international conference on current trends in advancedcomputing (ICCTAC)*, 2018: IEEE, pp. 1-5.
13. M. Chen,J. Chen, X. Wei, and B. Chen, "Is low-rate distributeddenialofserviceagreatthreattothe Internet?,"*IETInformationSecurity,* vol. 15, no. 5, pp. 351-363, 2021.
14. H.Cheng,J.Liu,T.Xu,B.Ren,J.Mao,andW.Zhang,"Machinelearningbasedlow-rate DDoS attackdetection for SDNenabledIoT networks,"*International Journal of Sensor Networks,* vol.34, no. 1, pp. 56-69, 2020.
15. M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, "ARecurrent Neural Network based Method for Low-Rate DDoSAttackDetectioninSDN,"in*20223rdInternationalConferenceon Artificial Intelligence and Data Sciences (AiDAS)*, 2022:IEEE, pp. 13-18.
16. D. Tang, Y. Yan, S. Zhang, J. Chen, and Z. Qin, "Performanceand features: Mitigating the low-rate TCP-targeted DoS attackvia SDN,"*IEEE Journal on Selected Areasin Communications,*vol. 40, no. 1, pp. 428-444, 2021.
17. D.KumarandJ.Thakur,"HandlingSecurityIssuesinSoftware-defined Networks (SDNs) Using Machine Learning," in*Computational Vision and Bio-Inspired Computing*: Springer,2022, pp. 263-277.
18. A. Shevtekar, K. Anantharam, and N. Ansari, "Low rate TCPdenial-of-service attack detection at edge routers,"*IEEECommunications Letters,* vol. 9, no. 4, pp. 363-365, 2005.
19. A. A. Alashhab,M. S. M. Zahid, A. Muneer, and M. Abdullahi,"Low-rateDDoSattackDetectionusingDeepLearningforSDN-enabled IoT Networks,"*International Journal of AdvancedComputer Science and Applications,* vol. 13, no. 11, 2022.
20. C. Zhang, J. Yin, Z. Cai, and W. Chen, "RRED: robust REDalgorithm to counter low-rate denial-of-service attacks,"*IEEECommunications Letters,* vol. 14, no. 5, pp. 489-491, 2010.
21. Ó.Fontenla-Romero,B.Guijarro-Berdiñas,D.Martinez-Rego, B. Pérez-Sánchez, and D. Peteiro-Barral, "Online machinelearning," in *Efficiency and Scalability Methods forComputational Intellect*: IGI global, 2013, pp. 27-54.
22. C. S. Lee and A. Y. Lee, "Clinical applications of continuallearningmachinelearning,"*TheLancetDigitalHealth*,vol.2,no.6, pp. e279-e281, 2020.
23. S. Ifzarne, H. Tabbaa, I. Hafidi, and N. Lamghari, "Anomalydetection using machine learning techniques in wireless sensornetworks," in *Journal of Physics: Conference Series*, 2021, vol.1743, no. 1: IOP Publishing, p. 012021.