УДК 681.3 DOI: 10.18372/2073-4751.85.21094

Кулаков Ю. О., д.т.н.,
orcid.org/0000-0002-8981-5649,
ya.kulakov@gmail.com,
Чередник В. Ю.,
cherednyk.v.yu.-io51f@edu.kpi.ua

МЕТОДИ ВИЯВЛЕННЯ DDOS-АТАК У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ: ПОРІВНЯЛЬНИЙ АНАЛІЗ КЛАСИЧНИХ ТА СУЧАСНИХ ПІДХОДІВ НА ОСНОВІ МАШИННОГО ТА ГЛИБОКОГО НАВЧАННЯ

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Вступ

Розвиток хмарних обчислень, Інтернету речей та технологій 5G/6G супроводжується різким зростанням складності та масштабів мережевої інфраструктури. У цьому контексті програмно-конфігуровані мережі (Software-Defined Networking, SDN) набули широкого поширення завдяки відділенню площини управління від площини даних, що забезпечує централізований контроль, гнучке програмування та динамічне застосування мережевих політик [1].

Водночас централізована архітектура SDN має одну важливу вразливість: SDN-контролер стає єдиною точкою відмови та пріоритетною ціллю для DDoS-атак. Такі атаки здатні вивести з ладу весь сегмент мережі шляхом насичення контролера запитами або вичерпання ресурсів таблиць потоків OpenFlow [2]. За даними звітів NETSCOUT Threat Intelligence, кількість DDoS-атак у мережах нового покоління щороку зростає на 10–15%, а їх складність значно ускладнює традиційне виявлення.

Протягом тривалого часу захист від DDoS-атак в SDN мережах ґрунтувався на традиційних підходах: статистичному аналізі трафіку, порогових методах і системах правил. Однак сучасні атаки – зокрема *slow DDoS*, *low-rate DDoS*, шифровані флуд-атаки та адаптивні ботнет-атаки – дедалі частіше обходять ці механізми захисту. Наявні дослідження на дану тематику [3,4] підтверджують, що сигнатурні й ентропійні методи демонструють критичне падіння точності при нових векторах атак. Це зумовлює необхідність переходу до інтелектуальних систем виявлення на основі машинного та глибокого навчання.

Справжня актуальність проблеми підкреслюється і специфікою SDN: на відміну від традиційних мереж, тут атака спрямована не лише проти конкретного сервера, а проти всієї інфраструктури управління, що робить наслідки значно критичними. Це пояснює інтенсивний розвиток галузі досліджень, присвячених методам машинного та глибокого навчання для виявлення DDoS-атак саме в SDN-середовищах.

Мета дослідження

Мета дослідження — провести систематизований порівняльний аналіз методів виявлення DDoS-атак у SDN-мережах: від класичних підходів до сучасних рішень на основі машинного та глибокого навчання, виявити їхні обмеження та сформулювати рекомендації щодо їх подальшого вдосконалення.

Класичні методи виявлення DDoS-атак в SDN та їхні обмеження

Для аналізу сучасних рішень, було окреслено контекст: чому традиційні методи захисту виявляються недостатніми і які недоліки змушують звертатися до складніших підходів виявлення DDoS-атак. При аналізі класичних методів виявлення DDoS-атак в програмно-конфігурованих мережах було виявлено чотири основні категорії.

Фундаментальною роботою в даній галузі є дослідження [3], в якому систематизовано підходи до виявлення DDoS-атак в SDN-мережах та встановлено, що системи, які базуються на правилах та статистичні методи не можуть ефективно виявляти динамічні атаки. Огляд [4], що базується на матеріалі датасетів CIC-IDS2017 та CICDDoS2019 показав, що класичні одноалгоритмні класифікатори (SVM, Decision Tree, Naive Bayes) при оцінюванні на реальних SDN-потоках демонструють точність на рівні 85–94%, тоді як на атаках нульового дня — нижче 70%. Аналогічного висновку було досягнуто авторами роботи [5], що статичні механізми мітигації позбавлені адаптивності та неефективні проти ботнет-кампаній, що постійно змінюють свою сигнатуру. Також авторами дослідження [6] було доведено, що сигнатурні системи виявлення атак ідентифікують зашифрований трафік менш ніж у 40% випадків.

Таблиця 1. Класичні методи виявлення DDoS в SDN: переваги та обмеження

Клас методів	Типові представники	Точність / ефективність	Ключові обмеження
Статистичні та ентропійні методи [3], [7]	Шенонова ентропія IP-адрес, k-means, аналіз розподілу пакетів	70–88% (залежно від типу атаки)	+ Не потребують навчальних даних; низькі обчислювальні витрати. – Висока частота хибних спрацьовувань; не виявляють slow DDoS та low-rate атаки; вимагають ручного налаштування порогів.
Правилові та порогові системи [5], [6]	OpenFlow rate-limiting, статичні ACL, SNORT-правила	65–82% при адаптивних атаках	+ Мінімальна затримка спрацьовування; проста реалізація. – Жорстко фіксовані сигнатури не адаптуються до нових векторів; adversarial-атаки легко обходять правила; непридатні для шифрованого трафіку.
Класичні алгоритми	SVM, Decision Tree,	85–94% на стандартних датасетах	+ Відносна інтерпретованість; помірна обчислювальна складність.

машинного навчання [4], [8]	Naive Bayes, k-NN		– Слабкі результати на складних патернах і незбалансованих датасетах; SVM погано масштабується при великих обсягах трафіку SDN; потребують ручного інжинірингу ознак.
Гібридні IDS на базі сигнатур та аномалій [9], [10]	Snort + Bro IDS, Suricata + ML-модулі	88–94%, але з відставанням на нових атаках	+ Комбінований захист відомих і відхилень від норми. – Висока хибнопозитивна частка при аномальному виявленні; потребують постійного оновлення сигнатурних баз; не враховують SDN-специфіку.

Проаналізувавши дані з таблиці 1, було встановлено, що всі класичні підходи мають спільний системний недолік: вони реагують на відомі патерни, але не здатні адаптуватися до адаптивних загроз. Більш фундаментальна проблема полягає в тому, що ці методи не враховують специфіки SDN-архітектури: вразливості площини управління, атак на таблиці потоків та динаміки топології. Саме це відкриває простір для застосування методів машинного та глибокого навчання, здатних виявляти складні поведінкові аномалії без явного задання правил.

Сучасні рішення на основі ML та DL: аналіз актуальних досліджень

Обмеженість класичних підходів зумовила науковців вести активний розвиток напряму інтелектуального виявлення DDoS-атак у програмно-конфігурованих мережах. Було здійснено аналіз актуальних публікацій, що представляють різні підходи до вирішення проблеми – від ансамблевих методів машинного навчання до гібридних архітектур глибокого навчання та adversarial-стійких систем.

Найширший контекст для аналізу надають автори в огляді [11], де систематизовано публікації 2021–2025 років, класифікуючи методи за трьома парадигмами навчання. Встановлено, що методи Random Forest і XGBoost демонструють стабільні результати серед класичних класифікаторів машинного навчання із точністю 98–99%. Серед гібридних архітектур глибокого навчання найбільш перспективними було визнано CNN-LSTM та CNN-GRU. Федеративне навчання виокремлюється як ключовий напрям для вирішення проблеми конфіденційності даних у розподілених SDN-середовищах. Водночас зафіксовано брак єдиних метрик оцінювання та нестачу досліджень у контексті шифрованих DDoS-атак та мультиконтролерних SDN.

Автори публікації [12] вказують на критичну проблему, яку ігнорують більшість дослідників у своїх роботах, а саме вразливість систем виявлення вторгнень до навмисно спотворених вхідних даних (adversarial-атак). Представлена авторами розроблена система поєднує три компоненти: Deep Belief Network (DBN) для зменшення

розмірності ознак потоку (CICFlowMeter + датасет CICDDoS2019), LSTM для захоплення часових залежностей у послідовностях пакетів та генеративно-змагальну мережу (GAN) для генерації adversarial-прикладів під час навчання. Механізм реакції побудовано на правилах Event-Condition-Action (ECA), інтегрованих у площину застосувань SDN. Головне обмеження розробленого методу — оцінювання проводилося виключно офлайн, без інтеграції в реальне SDN-середовище. Висока обчислювальна складність adversarial-тренування може бути суттєвим недоліком для практичного застосування.

Інший підхід запропоновано авторами дослідження [13], який полягає в перетворенні числових ознак мережевого потоку на двовимірні зображення для подальшої класифікації згортковими нейронними мережами. Це дозволяє задіяти потужні CNN-архітектури для виявлення просторових патернів у структурі трафіку.

Кращого результату було досягнуто за допомогою моделі Stacked Auto-Encoder MLP (SAE-MLP), а саме більше 99% точності на власному датасеті, що є підтвердженням відтворюваності дослідження. Однак критичним недоліком є час виявлення — більше 3 хвилин, що робить неможливим застосування підходу для сценаріїв виявлення в реальному часі та фактично виключає його з розгляду для практичного захисту SDN-мереж.

Автори публікації [14] представляють систематичне порівняння шести DL-моделей на збалансованому SDN-датасеті. Запропонована гібридна CNN-GRU модель поєднує: одновимірний CNN-шар для вилучення локальних просторових патернів у ознаках потоку; GRU-шар для темпорального моделювання послідовностей; повнозв'язні шари з Dropout для регуляризації; оптимізатор Adam з ранньою зупинкою для запобігання перенавчанню. Ключова перевага GRU над LSTM — менша кількість параметрів при схожій здатності моделювати часові залежності, що знижує обчислювальні витрати без суттєвої втрати точності. Модель досягла близько 100% точності на тестовій вибірці. Гібридна модель продемонструвала найвищу стабільність порівняно зі звичайними згортковими нейронними мережами чи рекурентними мережами.

У дослідженні [15] наведено результати експериментів, що проводилися науковцями у реальному тестовому середовищі Mininet з контролером OpenDayLight, з автентичними інструментами HTTP-атак (GoldenEye, Slowloris, HULK, Slowhttptest, XerXes). Особливою науковою цінністю дослідження є порівняння двох інструментів генерації ознак: CICFlowMeter та NTLFlowLyzer. Більший обсяг даних NTLFlowLyzer корелює з кращою стабільністю моделей. За підсумками тестування було виявлено, що модель Random Forest показує кращі результати на обох датасетах, ніж XGBoost.

Дослідники у своїй роботі [16] представили розробку end-to-end фреймворку, що охоплює не лише виявлення, а й автоматизовану мітигацію атак. Середовище реалізовано на двох віртуальних машинах: Ryu SDN-контролер та Mininet-емулятор (топологія spine-leaf, 18 хостів, 7 комутаторів).

Ключовим внеском є розробка чотирьох SDN-специфічних ознак: Unique Source Counts (кількість унікальних IP-джерел за секунду — маркер ботнет-атак), Flow Counts (кількість потоків до призначення — маркер об'ємних атак), Packet/Byte Rate (інтенсивність потоків — маркер amplification-атак), SYN Flag Count (лічильник TCP SYN-пакетів — маркер SYN-флуд атак). Виявлено високу кореляцію цих ознак із мітками атак, що

свідчить про їхню високу інформативність.

З чотирьох розглянутих у роботі методів Random Forest показав найвищий результат, перевершивши CNN, Gradient Boosting та SVM. Також розроблений модуль мітигації використовує OpenFlow-правила для блокування або перенаправлення шкідливого трафіку в реальному часі та безперервно адаптується до нових передбачень ML-моделі.

Порівняльний аналіз сучасних підходів

Результати детального аналізу кожного підходу систематизовано та наведено в таблиці 2. Наведені дані дозволяють зробити обґрунтовані висновки щодо відносних переваг і обмежень розглянутих рішень.

Таблиця 2. Загальна характеристика аналізованих сучасних підходів

Підхід / Архітектура	**Датасет**	**SDN-середовище**	**Найкраща точність**	**Ключова новизна**
ML / DL / FL (систематичний огляд) [11]	CICDDoS2019, InSDN та ін.	Mininet, Ryu, ODL (різні)	до 99%+	Комплексна класифікація методів за парадигмами; огляд FL для SDN; аналіз 50+ публікацій
GAN + DBN + LSTM (adversarial) [12]	CICDDoS2019 (88 ознак)	Офлайн оцінювання	99%+ / 91.23% (adv.)	Захист від adversarial-атак через GAN-навчання; ECA-механізм мітигації в SDN
SAE-MLP, CNN (image-based) [13]	Власний SDN-датасет (Mendeley) + CIC	Програмне SDN-середовище	99.75%	Перетворення ознак потоку на зображення для CNN; відкритий датасет (Mendeley Data)
Гібрид CNN-GRU (1D-CNN + GRU + Dense) [14]	SDN-датасет після SMOTE (24 500 семплів)	Програмне SDN-середовище	100% / CV: 99.70%	Поєднання CNN (просторові ознаки) + GRU (темпоральні); SMOTE-балансування; 5-fold CV оцінювання
RF, XGBoost + вибір ознак [15]	CICFlowMeter та NTLFlowLyzer (два датасети)	Mininet + OpenDayLight (реальне середовище SDN)	RF: 99.97–99.99%	Порівняння CICFlowMeter vs NTLFlowLyzer; HTTP-атаки (Slowloris); реальне SDN-середовище
RF, CNN, GB, SVM + 4 SDN-ознаки [16]	Синтетичний (Mininet/hping3)	Mininet + Ryu (spine-leaf, 2 VM)	RF: 95.3%	4 SDN-специфічні ознаки (USC, FC, PR, SFC); end-to-end фреймворк із динамічним OpenFlow-мітигатором

Проведений аналіз даних з таблиці 2 дозволяє виділити різні типи підходів. Одні методи показують високу ефективність в точності виявлення атак [14], інші методи демонструють високу стійкість до adversarial-атак [12], а решта методів орієнтовані на практичній реалізованості в реальному SDN-середовищі [15][16]. Наявність таких різних підходів дозволяє розглядати їх не як конкуруючі, а як взаємодоповнюючі компоненти майбутньої комплексної системи захисту від DDoS-атак.

Таблиця 3. Порівняння метрик ефективності виявлення по моделях

Модель	Точність, %	Precision, %	Recall, %	F1, %
Random Forest [15]	99.97–99.99	~99.9	~99.9	~99.9
CNN-GRU [14]	100.0	100.0	100.0	100.0
GRU [14]	100.0	~100.0	~100.0	~100.0
1D-CNN [14]	100.0	~100.0	~100.0	~100.0
SAE-MLP [13]	99.75	~99.7	~99.7	~99.7
LSTM [14]	99.0	~99.0	~98.5	~98.7
XGBoost [15]	97.61–99.48	~98.0	~98.0	~98.0
Random Forest [16]	95.3	94.8	95.9	95.3
CNN [16]	93.1	92.5	93.8	93.1
Gradient Boosting [16]	92.4	91.8	93.0	92.4
SVM [16]	89.6	88.4	90.1	89.2
DBN-LSTM+GAN [12]	99%+ / 91.23%*	н/д	н/д	н/д
RNN [14]	98.0	~97.5	~97.0	~97.2

Аналіз даних з таблиці 3 показав тенденції сучасних досліджень, що гібридні моделі глибокого навчання досягають майже ідеальних метрик точності виявлення, однак ці результати часто отримані на штучно збалансованих датасетах у контрольованих умовах. Порівняно нижча точність описаного методу у дослідженні [16] пояснюється більш реалістичними умовами — синтетичним трафіком у реальному SDN-середовищі без штучного балансування, що робить цей результат більш показовим для практичного застосування.

Таблиця 4. Якісне порівняння підходів за практичними критеріями

Джерело	Реальне SDN	Автоматична мітигація	Захист від adversarial-атак	Реальний час	Публічний датасет	Масштабованість
[16]	Так (Mininet+ Ryu)	Так (OpenFlow)	Ні	Так	Ні	Середня
[12]	Ні (офлайн)	Так (ECA)	Так (GAN)	Частково	Так (CIC)	Низька
[13]	Частково	Ні	Ні	Ні (216 с)	Так (Mendeley)	Середня
[14]	Ні	Ні	Ні	Потенційно	Частково	Висока
[15]	Так (Mininet+ ODL)	Ні	Ні	Частково	Так (CIC+NTL)	Середня
[11]	н/з	н/з	Згадано	н/з	Різні	н/з

Згідно аналізу отриманих даних з таблиці 4 виявлено суттєву нерівномірність, що підходи, які демонструють найвищу точність [14], не мають реалізації мітигаційного модуля та перевірки роботи в реальному SDN-середовищі. Натомість у дослідженнях, де описано практичну реалізацію розроблених методів [15][16], отримали дещо нижчі значення метрик ефективності виявлення атак. Однак такі підходи є ближчими до реального практичного застосування. Розглянуті підходи не забезпечують одночасно всіх ключових якостей, що вказує на необхідність комплексного рішення.

Виявлені недоліки та можливі шляхи вдосконалення

Синтез проведеного аналізу дозволяє виявити системні проблеми, що характерні для більшості аналізованих підходів, та сформулювати конкретні рекомендації щодо їх усунення.

1. У більшості досліджень використовуються синтетичні або застарілі датасети (наприклад, CICDDoS2019), які не відображають сучасних патернів атак — зокрема шифрованих DDoS-атак, повільних HTTP-атак та багатовекторних атак. Винятком є розроблений метод в дослідженні [15], де трафік генерується у реальному середовищі з актуальними HTTP-інструментами.

Можливим рішенням даної проблеми є розробка та публікація нових SDN-специфічних датасетів, що охоплюють повільні DDoS-атаки, шифровані флуд-атаки та мережі 5G/SDN-IoT. Рекомендується використання інструменту генерації трафіку NTLFlowLyzer, що генерує більш деталізовані ознаки, ніж CICFlowMeter. Варто зазначити, що публікація датасетів є важливою умовою для перевірки відтворюваності результатів.

2. Результати дослідження [12] доводять те, що без спеціального adversarial-тренування стандартні моделі

глибокого навчання виявляють DDoS-атаки такого типу з низькою точністю. На практиці це означає, що зловмисник, знаючи про існування системи виявлення атак, що базується на алгоритмах машинного чи глибокого навчання, може тривіально обійти більшість таких сучасних систем шляхом незначних модифікацій трафіку.

У якості можливого рішення пропонується інтегрувати змагальне навчання у стандартний пайплайн навчання моделей. Також рекомендується використовувати гарантований захист (certified defenses) та ансамблеві підходи для підвищення стійкості без значного збільшення обчислювальної складності.

3. Більшість підходів з глибоким навчанням обмежується лише виявленням атак, без використання автоматизованої мітигації. Тільки в двох розглянутих дослідженнях [12][16] реалізовано повний цикл виявлення-реагування.

Можливим варіантом для удосконалення є розробка інтегрованого фреймворка, де результати класифікатора безпосередньо ініціюють динамічні OpenFlow-правила (блокування, rate-limiting, перенаправлення потоків на honeypot). Механізм ECA [12] є перспективною основою для такої інтеграції.

4. Довготривалий час виявлення атак моделі SAE-MLP та висока обчислювальна вартість змагального тренування DBN-LSTM є неприйнятними для SDN-мереж, де швидкість реагування на атаки є критично важливою.

Пропонується дослідити дворівневу архітектуру:

1) швидкий ML-фільтр (Random Forest або XGBoost) для первинного скринінгу потоків із затримкою менше 1 мс;

2) точна DL-модель (CNN-GRU) для детального аналізу підозрілих потоків, ідентифікованих на першому рівні.

Також є можливість застосування квантизації моделей та апаратної акселерації (FPGA).

5. Тестування розглянутих рішень здійснювалося в одноконтролерних SDN-середовищах, тоді як реальні промислові мережі використовують розподілену мультиконтролерну архітектуру, де трафік між контролерами суттєво ускладнює централізований аналіз.

У якості можливого рішення цієї проблеми може бути впровадження федеративного навчання для мультиконтролерних SDN, де локальні моделі навчаються на кожному контролері без передачі сирих даних трафіку. Це допоможе одночасно вирішити проблеми конфіденційності, масштабованості та адаптованості до розподіленої архітектури.

Висновки

Проведений аналіз існуючих підходів до виявлення DDoS-атак в програмно-конфігурованих мережах дозволяє сформулювати такі ключові висновки.

По-перше, класичні методи захисту від DDoS-атак в програмно-конфігурованих мережах – статистичні, засновані на правилах та класичні методи машинного навчання – демонструють системні обмеження в умовах сучасних адаптивних атак. Їх ефективність знижується до 65–88% при повільних, зашифрованих та adversarial-атаках, що обґрунтовує необхідність переходу до більш складних підходів.

По-друге, сучасні методи машинного та глибокого навчання показують досить високі показники точності виявлення атак: Random Forest досягає 99.97–99.99% у реальних SDN-середовищах, гібридні моделі CNN-GRU показують 99.70% при крос-валідації. Разом із тим ці показники часто досягаються в штучних умовах без реального тестування в SDN-

середовищі, і реальна ефективність в умовах практичного застосування потребує додаткової верифікації.

По-третє, жоден із аналізованих підходів не задовольняє всі потреби для ефективного виявлення DDoS-атак. Методи, що забезпечують найвищу точність виявлення атак, не мають реалізації мітигаційного модуля та не перевірені в реальному SDN-середовищі, тоді як практично орієнтовані рішення мають порівняно нижчу точність виявлення атак. Це вказує на необхідність комплексного фреймворку, що одночасно забезпечує точне виявлення, стійкість до атак на моделі машинного чи глибокого навчання, автоматизовану мітигацію, масштабованість та відтворюваність.

По-четверте, можна виділити наступні пріоритетні напрями для майбутніх досліджень: розробка трансформерних архітектур для складних патернів, федеративне навчання для мультиконтролерних SDN, онлайн навчання для адаптації до дрейфу концепції (concept drift) та дворівневі фреймворки машинного та глибокого навчання для балансування між точністю та затримкою виявлення.

Література

1. Ahmed N. et al. Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis // Sensors. — 2022. — Vol. 22, No. 20. — Art. 7896. DOI: 10.3390/s22207896

2. Abubakar R. et al. An Effective Mechanism to Mitigate Real-Time DDoS Attack // IEEE Access. — 2020. — Vol. 8. — P. 126215–126227. DOI: 10.1109/ACCESS.2020.3007638

3. Swami R. et al. Software-Defined Networking-Based DDoS Defense Mechanisms // ACM Computing Surveys. — 2019. — Vol. 52, No. 2. — Art. 28. DOI: 10.1145/3301614

4. Ahmed N. et al. Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms // Sensors. — 2022. — Vol. 22, No. 20. — P. 7896.

5. Bawany N.Z. et al. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions // Arabian Journal for Science and Engineering. — 2017. — Vol. 42, No. 2. — P. 425–441. DOI: 10.1007/s13369-017-2414-5

6. Zhang F. et al. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems // IEEE Transactions on Industrial Informatics. — 2019. — Vol. 15, No. 7. — P. 4362–4369.

7. Mousavi S.M., St-Hilaire M. Early Detection of DDoS Attacks against SDN Controllers // IEEE CCECE. — 2015. DOI: 10.1109/CCECE.2015.7129521

8. El Sayed M.S. et al. A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs // IEEE Trans. Cogn. Commun. Netw. — 2022. — Vol. 8, No. 4. — P. 1862–1880.

9. Zhang F. et al. Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection // IEEE Access. — 2022. — Vol. 10. — P. 900–913.

10. Garg S. et al. Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN // IEEE Transactions on Multimedia. — 2019. — Vol. 21, No. 3. — P. 566–578.

11. Batool, S.; Aslam, M.; Akpokodje, E.; Jilani, S.F. A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives. Electronics 2025, 14, 4222. https://doi.org/10.3390/electronics14214222

12. Chen L., Wang Z., Huo R., Huang T. An Adversarial DBN-LSTM Method for Detecting and Defending against DDoS Attacks in SDN Environments // Algorithms. — 2023. — Vol. 16, No. 4. — Art. 197. https://doi.org/10.3390/a16040197

13. Boby Clinton, Urikhimbam & Hoque, Nazrul & Robindro, Khumukcham. Classification of DDoS Attack Traffic on SDN Network Environment Using Deep Learning // Cybersecurity (SpringerNature). — 2024. https://www.researchgate.net/publication/382830855

14. Elshewey A.M., Abbas S., Osman A.M. et al. DDoS Classification of Network Traffic in Software Defined Networking SDN Using a Hybrid Convolutional and Gated Recurrent Neural Network // Scientific Reports. — 2025. — Vol. 15. — Art. 29122. https://doi.org/10.1038/s41598-025-13754-1

15. Estupiñán Cuesta, E.P.; Martínez Quintero, J.C.; Avilés Palma, J.D. DDoS Attacks Detection in SDN Through Network Traffic Feature Selection and Machine Learning Models. Telecom 2025, 6, 69. https://doi.org/10.3390/telecom6030069

16. Gayantha N., Rajapakse C., Senanayake J. Advanced DDoS Attack Detection and Mitigation in Software-Defined Networking (SDN) Environments: An Integrated Machine Learning Approach // IEEE SCSE 2025. — Colombo: IEEE, 2025. — P. 1–6. https://doi.org/10.1109/SCSE65633.2025.11030982

Кулаков Ю.О., Чередник В.Ю.

МЕТОДИ ВИЯВЛЕННЯ DDOS-АТАК У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ: ПОРІВНЯЛЬНИЙ АНАЛІЗ КЛАСИЧНИХ ТА СУЧАСНИХ ПІДХОДІВ НА ОСНОВІ МАШИННОГО ТА ГЛИБОКОГО НАВЧАННЯ

У даній роботі розглянуто методи виявлення DDoS-атак у програмно-конфігурованих мережах. Метою роботи є порівняльний аналіз та систематизація класичних і сучасних підходів до виявлення атак в SDN-середовищах.

Проаналізовано традиційні методи захисту, зокрема статистичний аналіз ентропії, порогові та правилові системи, а також традиційні алгоритми машинного навчання, виявлено їх обмеження в умовах сучасних адаптивних атак. Досліджено сучасні підходи на основі машинного та глибокого навчання, включаючи ансамблеві методи, гібридні архітектури, adversarial-стійкі моделі та федеративне навчання, їх переваги та недоліки. Порівняно точність та ефективність різних методів на основі актуальних опублікованих результатів досліджень.

У статті запропоновано подальше дослідження дворівневих архітектур на основі машинного та глибокого навчання та федеративного навчання в програмно-конфігурованих мережах з метою підвищення точності виявлення атак, adversarial-стійкості та адаптивності до змін у мережевому середовищі. Наведено результати порівняння методів з акцентом на їх ефективність у реальних SDN-середовищах.

Ключові слова: *програмно-конфігуровані мережі; DDoS-атаки; машинне навчання; глибоке навчання; OpenFlow; змагальне навчання; федеративне навчання.*

Kulakov Y.O., Cherednyk V.Y.

DDOS ATTACK DETECTION METHODS IN SOFTWARE-DEFINED NETWORKS (SDN): A COMPARATIVE ANALYSIS OF CLASSICAL AND MODERN MACHINE LEARNING AND DEEP LEARNING APPROACHES

This paper examines DDoS attack detection methods in software-defined networks (SDN). The aim of the study is a comparative analysis and systematization of classical and modern approaches to attack detection in SDN environments.

Traditional protection methods are analyzed, including entropy-based statistical analysis, threshold and rule-based systems, and conventional machine learning algorithms, with their limitations under modern adaptive attacks identified. Modern machine learning and deep learning approaches are investigated, including ensemble methods, hybrid architectures, adversarially robust models, and federated learning, along with their respective advantages and drawbacks. The accuracy and efficiency of various methods are compared on the basis of current published research results.

The paper proposes further investigation of two-tier machine learning and deep learning architectures and federated learning in software-defined networks, with the aim of improving attack detection accuracy, adversarial robustness, and adaptability to changes in the network environment. Results of the method comparison are presented with emphasis on their effectiveness in real SDN deployments.

Keywords: *software-defined networking; DDoS attacks; machine learning; deep learning; OpenFlow; adversarial training; federated learning.*

Стаття подана до редакції: 25/03/2026
Стаття прийнята до опублікування: 30/03/2026
Стаття опублікована: 27/04/2026