September 5, 2025;
Boston, USA

SECTION 14.
INFORMATION TECHNOLOGIES AND SYSTEMS

DOI 10.36074/logos-05.09.2025.029

ВИКОРИСТАННЯ ОНЛАЙН-НАВЧАННЯ ДЛЯ АДАПТИВНОГО ВИЯВЛЕННЯ DDOS-АТАК У МЕРЕЖЕВОМУ ТРАФІКУ

Бородай Денис Юрійович[1]

1. аспірант факультету інформаційних технологій
Київський національний університет імені Тараса Шевченка, УКРАЇНА

DDoS-атаки залишаються однією з найбільш критичних загроз для сучасних комп'ютерних мереж, оскільки здатні вивести з ладу критичні сервіси та інфраструктуру. Зростання обсягів трафіку, кількості та масовості DDoS-атак[4], широке впровадження шифрування та поява нових, раніше невідомих типів атак суттєво ускладнюють застосування традиційних методів виявлення, які ґрунтуються на сигнатурному аналізі та статичних моделях. Такі методи виявляють атаки лише за заздалегідь відомими шаблонами та не здатні адаптуватися до зміни характеристик трафіку та появи нових атак. Це обумовлює необхідність розробки підходів, здатних до адаптації в режимі реального часу та ефективної роботи у потокових середовищах.

Метою роботи є розробка та оцінка підходу до виявлення DDoS-атак у потоковому мережевому трафіку на основі алгоритмів онлайн-навчання, здатних адаптуватися до дрейфу даних та забезпечувати високу точність класифікації за обмеженого набору характеристик, що доступні навіть у разі шифрування трафіку.

Для реалізації підходу використано алгоритм Adaptive Random Forest (ARF)[1] у поєднанні з механізмом Drift Detection Method (DDM)[3] для своєчасного виявлення змін у характеристиках та типах атак. ARF складається з ансамблю дерев рішень, кожне з яких навчається на різних підмножинах даних за рахунок застосування техніки online bagging. У разі виявлення концептуального дрейфу окремі дерева можуть бути замінені на нові, що забезпечує здатність моделі адаптуватися до змін у трафіку без повного перенавчання [1]. Задача класифікації була зведена до бінарної: усі класи атак були об'єднані в один клас, що забезпечує наявність двох класів «атака» та

«норма». Це знижує обчислювальні витрати та дозволяє застосовувати метрики, які менш чутливі до дисбалансу класів.

Для дослідження було використано датасет CIC-DDoS2019, який містить широкий спектр DDoS-атак [2]. Навчання проводилося на даних першого дня, що включає обмежений набір атак, тоді як тестування виконувалося на даних другого дня, де присутні нові типи атак і відмінні IP-адреси. Такий підхід дозволяє оцінити здатність моделі узагальнювати знання та виявляти атаки, які раніше не зустрічалися. Стратегія навчання відповідала класичній парадигмі онлайн-обробки: кожен екземпляр оброблявся один раз, під час його обробки спочатку здійснювався прогноз, а потім оновлення моделі. Для відбору інформативних ознак попередньо навчався класичний Random Forest, після чого на основі важливості відбирались ознаки, які потім використовувалися в досліджуваній моделі.

Запропонований підхід продемонстрував високу точність у потоковому середовищі та стійкість до дрейфу даних (табл. 1).

Таблиця 1

Результат роботи моделі

Метрика	Результат на тренувальній вибірці (1-й день)	Результат на тестовій вибірці (2-й день)
Точність	>99,99%	>99,99%
Влучність	99,57%	99,77%
Повнота	99,78%	99,89%
F_1-міра	99,67%	99,83%

Модель ефективно виявляла атаки навіть за умови використання лише загальних характеристик трафіку (метаданих), що робить її придатною для аналізу зашифрованого трафіку, де неможливо застосувати глибинний аналіз пакетів. Використання ARF у поєднанні з DDM забезпечило динамічну адаптацію до нових умов та типів атак і запобігло деградації якості моделі під час появи нових типів атак.

Таким чином, розроблений підхід дозволяє здійснювати адаптивне виявлення DDoS-атак у потоковому трафіку в режимі реального часу, демонструючи високу ефективність навіть за умов обмежених даних і шифрування. У подальшому планується дослідити застосування даного підходу для виявлення інших типів атак, а також протестувати його у реальних мережах, зокрема в мережах SDN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Adaptive random forests for evolving data stream classification / H. M. Gomes et al. Machine learning. 2017. Vol. 106, no. 9-10. P. 1469–1495. URL: https://doi.org/10.1007/s10994-017-5642-8.
[2] DDoS evaluation dataset (CIC-DDoS2019). Canadian Institute for Cybersecurity. URL: https://www.unb.ca/cic/datasets/ddos-2019.html.
[3] Learning with drift detection / J. Gama et al. Intelligent data analysis. 2004. P. 286–295. URL: https://doi.org/10.1007/978-3-540-28645-5_29.
[4] Targeted by 20.5 million ddos attacks, up 358% year-over-year: cloudflare's 2025 Q1 ddos threat report. The Cloudflare Blog. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/.