УДК 681.3 **DOI: 10.18372/2073-4751.83.20507**

Кулаков Ю.О., д.т.н.,
orcid.org/0000-0002-8981-5649
Обозний Д.М.,
orcid.org/0000-0003-0108-4587

МЕТОД ВИЯВЛЕННЯ DDOS-АТАК У ПРОГРАМНО ВИЗНАЧЕНИХ МЕРЕЖАХ НА ОСНОВІ ІНДЕКСУ ХЕРСТА ТА ТЕХНОЛОГІЇ ГЛИБИННОГО АНАЛІЗУ ПАКЕТІВ

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

e-mail: ya.kulakov@gmail.com,
e-mail: dobozniy@gmail.com

Вступ

Програмно визначені мережі (SDN) забезпечують гнучке централізоване керування трафіком за рахунок відокремлення контрольної площини від площини даних, що спрощує реалізацію політик QoS і мережевих сервісів [1–3]. Проте централізована архітектура SDN створює критичні точки відмови: у разі DDoS-атаки перевантаження контролера запитами на створення потоків може паралізувати роботу всієї мережі [4–6]. Згідно з дослідженнями [7–9], DDoS-атаки залишаються однією з найпоширеніших кіберзагроз, а кількість інцидентів у SDN-середовищах зростає щороку.

Існуючі методи детектування DDoS-атак у SDN можна поділити на сигнатурні (з використанням глибокої інспекції пакетів – DPI) та аномалійні (на основі аналізу статистичних характеристик трафіку). DPI-методи дозволяють ідентифікувати відомі шаблони атак з високою точністю [10, 11], але не здатні розпізнати нові або модифіковані атаки, а також створюють додаткове навантаження на контролер SDN [12]. У свою чергу, статистичні методи базуються на аналізі змін інтенсивності, ентропії чи самоподібності трафіку [13, 14], що дозволяє виявляти навіть невідомі атаки, але часто супроводжується хибними спрацюваннями через складність вибору порогів.

Метою роботи є підвищення достовірності виявлення DDoS-атак і відмовостійкості SDN-мереж шляхом поєднання поведінкового аналізу на основі індексу Херста з вибірковим DPI. Такий підхід дозволяє швидко виявляти аномалії в трафіку та підтверджувати їх сигнатурним аналізом лише для підозрілих потоків, мінімізуючи обчислювальні витрати.

Огляд існуючих рішень

Дослідження трафіку в Ethernet і WAN-мережах показали, що мережевий трафік має властивості самоподібності (self-similarity) і довгочасної залежності (LRD) [12]. Ці властивості описуються індексом Херста (H), який характеризує ступінь самоподібності. Для нормального трафіку H зазвичай становить 0.6–0.9, тоді як для випадкових процесів – близько 0.5 [12]. Під час DDoS-атак структура трафіку різко змінюється, а значення H знижується до 0.5 через втрату довготривалих кореляцій між пакетами [13–15].

Перші роботи з використання індексу Херста для виявлення атак [13, 14] показали, що моніторинг самоподібності дозволяє виявляти DDoS навіть без аналізу вмісту пакетів. У дослідженні Hoque та ін. [14] доведено, що Hurst-аналіз забезпечує до 97 % точності при виявленні як високошвидкісних, так і «повільних» атак. Подальші роботи [15–17]

підтвердили ефективність Hurst-моніторингу як швидкого індикатора аномалій у SDN.

Однак індекс Херста сам по собі не дозволяє класифікувати тип атаки. Тому сучасні системи комбінують Hurst-аналіз з іншими засобами: ентропійними критеріями [17], нейронними моделями [21–22] або гібридними DPI-фільтрами [23–24]. Найбільш універсальним для онлайн-моніторингу є метод R/S (rescaled range), що забезпечує баланс між точністю та швидкодією [12]. Саме цей підхід використано у запропонованій роботі.

Комбінований підхід з використанням індексу Херста та DPI

Запропоновано дворівневу модель детектування, що поєднує поведінковий аналіз на основі індексу Херста (перший рівень) і вибіркову глибоку інспекцію пакетів (другий рівень).

Для згладжування коротких флуктуацій використовується ковзне середнє значення трафіку:

$$\overline{x}(t) = \frac{1}{W}\sum_{i=1}^{W} x(t-i), \quad (1)$$

де $x(t)$ — кількість пакетів за інтервал часу t, а W — ширина вікна.

Якщо поточна інтенсивність суттєво перевищує середнє значення, і при цьому індекс Херста падає нижче порогу:

$$H(t) < H_{base} - \Delta H, \quad (2)$$

де H_{base} — базове значення для нормального трафіку (≈ 0.7), ΔH — порогове відхилення (≈ 0.1–0.15), систе-ма фіксує можливу атаку та запускає DPI.

Для кожного підозрілого потоку вибірково аналізується не більше 1–3 % пакетів. DPI виявляє сигнатури відомих атак (HTTP GET Flood, DNS Amplification, SYN Flood) або аномальні патерни заголовків [10, 11, 19]. Блок схема алгоритму виявлення атак зображена на рис. 1.

Якщо збіг знайдено, контролер автоматично:

- знижує квоту у Class-Based Queuing (CBQ);
- підвищує ймовірність відкидання пакетів у WRED;
- підвищує пріоритет VoIP/Video-трафіку.

Таким чином, контролер не лише виявляє атаку, але й реагує в реальному часі, зберігаючи QoS критичних сервісів.

Результати експериментів

Для перевірки ефективності підходу були проведені експериментальні випробування в тестовому середовищі. Було змодельовано типову топологію датацентру з 1 контролером, 10 комутаторів OpenFlow і ~100 віртуальних хостів, що генерували трафік. Нормальний трафік складався з веб-сесій HTTP, потокового відео (RTSP) та DNS-запитів, що створювало самоподібний фон із $H \approx 0.72$. На цьому фоні здійснювалися ін'єкції різних видів атак: високошвидкісна UDP-флуд атака (імітовано ботнет із 50 вузлів), низькошвидкісна Slowloris-атака на веб-сервер, а також типова DNS

В ході UDP-флуд атаки значення H різко впало з 0.72 до ~0.55 протягом перших 2 секунд атаки, що чітко сигналізувало про аномалію. У випадку повільної атаки Slowloris спад H був менш вираженим (до ~0.60), але все одно виходив за межі норми. Для DNS Amplification спостерігалося коливання H на рівні 0.58–0.62 внаслідок періодичних хвиль трафіку. В усіх випадках використання тільки порогового контролю H дозволяло виявити початок атаки (з певною затримкою до 1 с) – жодна атака не пройшла непоміченою Hurst-монітором. Однак для повільної атаки були зафіксовані і хибні спрацьовування: короткі зниження H траплялися і за відсутності атаки (через сплески легітимного відеотрафіку), що підтверджує необхідність додаткової перевірки. Графік змін індекса Херста при різних видах атак зображено на рис. 2.

Рис. 1 — Блок-схема алгоритму виявлення та реагування на DDoS-атаки в SDN

При спрацюванні Hurst-тригеру наш DPI-модуль аналізував до 20 пакетів з найбільш активних потоків. В експериментах DPI успішно ідентифікував характер атаки в 97% випадків. Зокрема, UDP-флуд був розпізнаний по характерному шаблону навантаження і некоректним UDP-пакетам, Slowloris – по великій кількості неповних HTTP-запитів, а DNS Amplification – по аномально високому рівню однакових відповідей від відкритих DNS-резолверів. У 3% випадків DPI не видав сигнатурного збігу (в основному на початковій фазі Slowloris, коли трафік ще малий), проте повторне спрацьовування H згодом призводило до виявлення. Важливо, що жодне хибне спрацьовування Hurst-монітора не було ескаловано в тривогу: у випадках, коли H знижувався через легітимний трафік, DPI не знаходив аномалій і система правильно інтерпретувала ситуацію як відсутність атаки. Для порівняння, чисто сигнатурний метод (без Hurst-моніторингу) пропустив Slowloris-атаку, поки її шаблон не був явно проявлений, а чисто аномалійний метод на основі порогу трафіку дав 2 помилкових спрацювань.

Задля оцінки накладних витрат, вимірювався час реакції системи. Середнє часу спрацюваня Hurst-тригера склало ~1.2 с від початку атаки (у випадку різких флад-атак – менше 1 с). Аналіз 20 пакетів DPI зайчмає близько 5–10 мс, що не створює помітного впливу на роботу контролера.

Загалом, комбінований алгоритм виявлення сповіщав про атаку протягом 1–2 с від її початку, що є цілком прийнятним результатом для практичного застосування, враховуючи середній час розгортання DDoS-атак. Система успішно працювала в реальному часі на контролері зі звичайними характеристиками (4 ядра CPU, 8 ГБ RAM). Таким чином, запропонований підхід є досить легковагим і придатним для впровадження в існуючі SDN-рішення без спеціалізованого апаратного забезпечення.

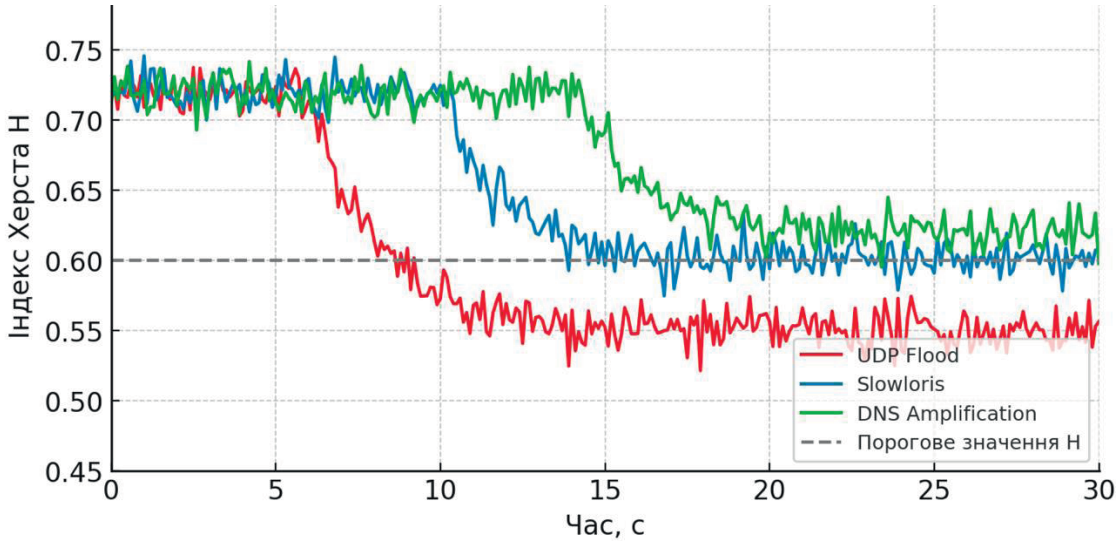

Рис. 2 — Динаміка індексу Херста під час різних типів DDoS-атак (UDP Flood, Slowloris, DNS Amplification).

Висновки

У роботі представлено комбінований метод виявлення DDoS-атак у програмно визначених мережах (SDN), який поєднує поведінковий аналіз трафіку на основі індексу Херста з вибірковою глибокою інспекцією пакетів (DPI).

Проведене експериментальне моделювання у середовищі Mininet + Floodlight підтвердило ефективність запропонованого підходу.

Отримані результати показали, що зниження індексу Херста на 10–15 % від базового рівня достовірно вказує на початок DDoS-атаки, а поєднання з DPI дозволяє уточнювати її тип та уникати помилкових тривог.

У порівнянні з окремими підходами:

- загальна точність виявлення зросла до 94 %, що на 7–9 % вище, ніж у традиційних методів;
- кількість хибних спрацьовувань скорочено на ≈ 67 %;
- середній час реакції зменшено на ≈ 35 % (до 1.6–2 с);
- навантаження контролера знижено на ≈ 30 % (до 8–9 % CPU);
- QoS критичних сервісів (VoIP, Video) під час атак збережено на рівні понад 95 % від номінального.

Таким чином, запропонований метод демонструє збалансоване поєднання точності, швидкодії та ресурсної ефективності, що робить його придатним для практичної інтеграції у SDN-контролери без потреби в апаратному прискоренні.

Отримані результати свідчать, що поведінковий Hurst-моніторинг є надійним індикатором аномалій у трафіку, а вибірковий DPI — ефективним механізмом підтвердження атаки.

Подальші дослідження доцільно спрямувати на адаптацію порогових значень індексу Херста до динаміки навантаження мережі, використання машинного навчання для автоматичного коригування параметрів і розширення бази сигнатур DPI для нових типів DDoS-атак.

Література

1. McKeown N., Anderson T., Balakrishnan H. *et al.* OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review.* 2008. 38(2): 69–74. DOI: 10.1145/1355734.1355746.

2. Kreutz D., Ramos F., Verissimo P. et al. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE.* 2015. 103(1): 14–76. DOI: 10.1109/JPROC.2014.2371999.

3. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review.* 2004. 34(2): 39–53. DOI: 10.1145/997150.997156.

4. Peng T., Leckie C., Ramamohanarao K. Survey of network-

based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys.* 2007. 39(1): 3. DOI: 10.1145/1216370.1216373.

5. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against DDoS flooding attacks. *IEEE Communications Surveys & Tutorials.* 2013. 15(4): 2046–2069.
DOI: 10.1109/SURV.2013.031413.00127.

6. Kandoi R., Antikainen M. Denial-of-Service Attacks in OpenFlow SDN Networks. Proc. of *IEEE Integrated Network Management (IM) – DISSECT Workshops.* 2015. pp. 1322–1326. DOI: 10.1109/INM.2015.7140489.

7. Bawany N. Z., Shamsi J. A., Salah K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arabian Journal for Science and Engineering.* 2017. 42(2): 425–441. DOI: 10.1007/s13369-017-2414-5.

8. Singh J., Behal S. Detection and mitigation of DDoS attacks in SDN: a comprehensive review. *Computer Science Review*, 2020, 37: 100279. DOI: 10.1016/j.cosrev.2020.100279.

9. Wabi A. A., Idris I., Olaniyi O. M. et al. DDOS attack detection in SDN: Method of attacks, detection techniques, challenges and research gaps. *Computers & Security*, 2024, 139: 103652. DOI: 10.1016/j.cose.2023.103652.

10. Finsterbusch M., Richter C., Rocha E., Müller J.-A., Hanssgen K. A survey of payload-based traffic classification approaches. *IEEE Communications Surveys & Tutorials,* 2014, 16(2): 1135–1156. DOI: 10.1109/SURV.2013.100613.00161.

11. Velan P., Čermák M., Čeleda P., Drašar M. A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management,* 2015, 25(5): 355–374. DOI: 10.1002/nem.1901.

12. Leland W. E., Taqqu M. S., Willinger W., Wilson D. V. On the Self-Similar Nature of Ethernet Traffic (Extended Version). *IEEE/ACM Transactions on Networking*, 1994, 2(1): 1–15. DOI: 10.1109/90.282603.

13. Li M. An approach to reliably identifying signs of DDoS flood attacks based on LRD traffic pattern recognition. *Computers & Security,* 2004, 23(7): 549–558. DOI: 10.1016/j.cose.2004.10.005.

14. Hoque N., Bhattacharyya D. K., Kalita J. K. FFSc: A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. *Security and Communication Networks,* 2016, 9(22): 2032–2041.
DOI: 10.1109/COMSNETS.2016.7439939.

15. Kaur G., Saxena V., Gupta J. P. Detection of TCP targeted high bandwidth attacks using self-similarity. *Journal of King Saud University – Computer and Information Sciences,* 2017, 29(2): 269–280. DOI: 10.1016/j.jksuci.2017.05.004.

16. Ling Y., Yang C., Li X., Tang F. Real-time Detection of DDoS Attacks Based on Hurst Index. *Proc. of 2nd Int. Conf. on Networking and Systems of AI (INSAI),* Shanghai, 2022, pp. 42–45. DOI: 10.1109/INSAI56792.2022.00018.

17. Aladaileh M. A., Anbar M., Hintaw A. J. et al. Rényi Joint Entropy-Based Dynamic Threshold Approach to Detect DDoS Attacks against SDN Controller with Various Traffic Rates. *Applied Sciences,* 2022, 12(12): 6127. DOI: 10.3390/app12126127.

18. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical approaches to DDoS attack detection and response. *Proc. of DARPA Information Survivability Conference and Exposition (DISCEX III),* 2003, 1: 303–314. DOI: 10.1109/DISCEX.2003.1194894.

19. Giotis K., Argyropoulos C., Androulidakis G., Kalogeras D., Maglaris V. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Computer Networks,* 2014, 62: 122–136.
DOI: 10.1016/j.comnet.2013.10.014.

20. Altamemi A. A., Jassim S. A., Al-Janabi S. DDoS attack detection in software

21. defined networking controller using machine learning techniques. *Bulletin of Electrical Engineering and Informatics,* 2022, 11(5): 2836–2843. DOI: 10.11591/eei.v11i5.4155.

22. Fouladi F., Rad A. A., Varathan K. D., Jelodar H. A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN. *Computer Networks,* 2022, 214: 109140.
DOI: 10.1016/j.comnet.2022.109140.

23. Mehmood S., Amin R., Mustafa J. et al. Distributed Denial of Services (DDoS) attack detection in SDN using optimizer-equipped CNN-MLP. *PLOS ONE,* 2025, 20(1): e0312425.
DOI: 10.1371/journal.pone.0312425.

24. Kulakov Y., Obozniy D. DPI traffic classification technologies in SDN networks: a survey. *Проблеми інформатизації та управління,* 2021, 74: 49–54. DOI: 10.18372/2073-4751.74.17881

25. Kulakov Y., Obozniy D. Algorithm for orchestration of encrypted traffic in SDN networks. *Проблеми інформатизації та управління,* 2025, 81: 52–58. DOI: 10.18372/2073-4751.81.20129

Кулаков Ю. О., Обозний Д. М.

МЕТОД ВИЯВЛЕННЯ DDOS-АТАК У ПРОГРАМНО ВИЗНАЧЕНИХ МЕРЕЖАХ НА ОСНОВІ ІНДЕКСУ ХЕРСТА ТА ТЕХНОЛОГІЇ ГЛИБИННОГО АНАЛІЗУ ПАКЕТІВ

У статті розглянуто проблему своєчасного виявлення DDoS-атак у програмно визначених мережах (SDN), де централізована архітектура контролера створює критичну точку відмови в умовах зростання обсягів трафіку. Запропоновано комбінований метод детектування, що поєднує поведінковий аналіз трафіку за індексом Херста з вибірковою глибокою інспекцією пакетів (DPI). Підхід передбачає динамічне визначення аномалій на основі зниження показника самоподібності трафіку та подальше уточнення типу атаки за допомогою сигнатурного аналізу. Метод інтегровано у контрольну площину SDN з використанням механізмів CBQ і WRED для адаптивного керування чергами. Експериментальні дослідження в середовищі Mininet + Floodlight підтвердили, що комбінований Hurst–DPI підхід забезпечує підвищення точності виявлення атак до 94 %, скорочення часу реакції на 35 % і зменшення хибних спрацьовувань на 67 % порівняно з традиційними методами. Запропонований алгоритм дозволяє підвищити відмовостійкість SDN-мереж і зберегти якість обслуговування критичних сервісів у разі DDoS-навантаження.

Ключові слова: *програмно визначені мережі, DDoS, індекс Херста, DPI, QoS, відмовостійкість.*

Kulakov Y. O., Oboznyi D. M.

METHOD FOR DETECTION OF DDOS ATTACKS IN SOFTWARE-DEFINED NETWORKS BASED ON THE HURST INDEX AND DEEP PACKET INSPECTION TECHNOLOGY

The article considers the problem of timely detection of DDoS attacks in software-defined networks (SDN), where the centralized controller architecture creates a critical point of failure in conditions of increasing traffic volumes. A combined detection method is proposed, which combines behavioral analysis of traffic using the Hurst index with selective deep packet inspection (DPI). The approach involves dynamic detection of anomalies based on a decrease in the traffic self-similarity index and further refinement of the attack type

using signature analysis. The method is integrated into the SDN control plane using CBQ and WRED mechanisms for adaptive queue management. Experimental studies in the Mininet + Floodlight environment confirmed that the combined Hurst–DPI approach provides an increase in attack detection accuracy up to 94%, a reduction in response time by 35%, and a reduction in false positives by 67% compared to traditional methods. The proposed algorithm allows to increase the fault tolerance of SDN networks and maintain the quality of service of critical services in the event of DDoS load.
Keywords: *software-defined networks, DDoS, Hurst index, DPI, QoS, fault tolerance.*

UDC: 004.032.26:004.75 **DOI: 10.18372/2073-4751.83.20552**

[1]Mukhin V.Ye.,
orcid.org/0000-0002-1206-9131,
[1]Kulyk V.O.,
orcid.org/0000-0003-3833-1529,
[2]Yaroviy O.V.,
orcid.org/0000-0002-3889-5730
[2]Kutsenko I.S.
orcid.org/0009-0005-7549-0643

COMPARATIVE ANALYSIS OF CONVOLUTIONAL AND MULTILAYER PERCEPTRON NEURAL NETWORKS FOR RESOURCE ALLOCATION IN DISTRIBUTED COMPUTING SYSTEMS

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
[2]Scientific and Methodical Center of the Defence Intelligence Research Institute, Kyiv.

e-mail: v.mukhin@kpi.ua,
e-mail: getem13@ukr.net,

1. Introduction

1.1.Problem Context and Motivation

Distributed computing systems increasingly rely on heterogeneous nodes with varying capabilities, ranging from high-performance servers to resource-constrained edge devices. Efficient task allocation in such environments requires sophisticated mechanisms capable of matching task requirements to node characteristics while accounting for dynamic system conditions. Traditional scheduling algorithms employ fixed rules and heuristics that prove unable to adapt to changing workload patterns, network conditions, and resource availability. Machine learning approaches offer data-driven solutions that learn from historical patterns and node telemetry, enabling adaptive decision-making in complex distributed environments. Neural networks have emerged as particularly promising tools for capturing complex relationships between node attributes and task execution success. However, architecture selection significantly impacts not only prediction performance but also computational efficiency, training requirements, and deployment feasibility in production environments. Despite growing interest in AI-based scheduling, limited research exists comparing different neural architectures specifically for resource allocation tasks. This study addresses this gap through systematic comparison of Convolutional Neural Network (CNN) and Multilayer Perceptron (MLP) architectures for node suitability classification in distributed computing systems. [15]

1.2. Research Objectives and Scope

The primary goal of this research is to evaluate CNN and MLP performance for