ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ПОНОЧОВНИЙ ПЕТРО МИХАЙЛОВИЧ

УДК 004.05(045)

ДИСЕРТАЦІЯ
СИСТЕМА ПРОТИДІЇ УПЕРЕДЖЕННЯ НИЗЬКОШВИДКІСНИХ HTTP DDOS-АТАК НА ВЕБ-РЕСУРСИ

Спеціальність 125 – Кібербезпека
Галузь знань 12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Петро ПОНОЧОВНИЙ

Наукові керівники: ПЕПА Юрій Володимирович
к.т.н., доцент, професор кафедри
технічного захисту інформації;

ІВАНЧЕНКО Ігор Сергійович
к.т.н., доцент, професор кафедри
технічного захисту інформації;

Київ - 2025

АНОТАЦІЯ

Поночовний П.М. Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека» (12 – Інформаційні технології). - Державний університет інформаційно-комунікаційних технологій, м. Київ, 2025.

Дисертаційна робота присвячена підвищенню надійності серверів з використанням системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси.

Об'єктом дослідження дисертаційної роботи є процес захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак. *Предметом* дослідження дисертаційної роботи є системи захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак.

В дисертаційній роботі проведено аналіз існуючих та сучасних методів, моделей та систем протидії низькошвидкісним HTTP DDoS-атакам. Встановлено, що традиційні підходи, такі як обмеження трафіку або сигнатурний аналіз, недостатньо ефективні через динамічний характер атак, що використовують легальні HTTP-запити. На основі цього сформульовано вимоги до системи, зокрема необхідність аналізу груп пакетів та аномалій на рівні мережевої взаємодії.

Метою дослідження є зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси.

В процесі досягнення зазначеної мети та вирішення наукового завдання у роботі одержано основні наукові результати:

- *вперше* розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача, яка за рахунок виявлення

аномального потоку, алгоритму фільтрації трафіку, модуля пам’яті, дозволить передувати та протидіяти низькошвидкісним HTTP DDoS-атакам на рівні кінцевого користувача;

- *вперше* розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, який за рахунок умов фільтрації трафіку, а саме обмеження кількості запитів з одного IP/підмережі, блокування трафіку з регіонів, де немає клієнтів, тривалості запиту, дає можливість зменшити навантаження на сервер від 40 до 60 % і підтримати цілісність системи.

- *вперше* розроблено систему протидії низькошвидкісним HTTP DDOS-атакам на веб-ресурси з урахуванням аномалій в пакетах, яка за рахунок розроблених моделі та методу, дає можливість упередженню та покращенню захисту від низькошвидкісних HTTP DDoS-атак на 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей.

Дані особливості порівнюються з вхідним трафіком (відбувається онлайн виявлення), під час якого виявлені аномалії, та низькошвидкісні HTTP DDoS-атаки передаються для «Навчання ШІ» після опрацювання передаються до блоку «Даних про навчання». Історія навчань використовується при наступних виявленнях загроз.

Експериментальна оцінка ефективності розробленої системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси показала, що розроблена система знижує навантаження на сервер на 40–60% порівняно з базовими рішеннями. Точність виявлення атак становить 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей.

У вступі обґрунтовано актуальність теми дисертації, сформульовано мету і завдання дослідження, визначено наукову та практичну цінність отриманих результатів і особистий внесок автора у спільних публікаціях.

У першому розділі проаналізовано методи, моделі та системи упередження низькошвидкісних HTTP DDoS-атак. Проаналізовано системи протидії DDoS атакам які застосовуються на території України, враховано всі особливості, та сформульовано обґрунтований напрям наукового вирішення проблеми. Системи які було проаналізовані наведені в табл. 1.1 з урахуванням їх особливостей за 10 основними характеристиками безпеки.

У другому розділі запропоновано модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача. Досліджено та вдосконалено модель за допомогою фільтрування особливостей пакетів з використанням Штучного інтелекту. Розроблено комплексну модель виявлення аномального потоку, яка враховує наступні особливості:

- наявність пустих пакетів;
- час тривалості запиту;
- кодування регіону.

Для оцінки захищеності користувачів використовуються попередньо згадані особливості, при виявлені аномалій дані опрацьовуються ШІ та передаються для блоку «Дані про навчання». Аномалії, які виявлені таким шляхом будуть враховані при наступному колі фільтрації вхідного трафіку. Також у даному розділі удосконалено алгорим роботи методу раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак на основі аналізу обробки пакетних груп. Що забезпечує ретельніший захист кінцевого користувача від аномалій, поведінка яких схожа на низькошвидкісні HTTP DDoS-атаки. Наступним кроком даного розділу було вперше розроблено та представлено Систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси. Яка складається з моделі упередження низькошвидкісних HTTP DDoS-атак з використанням штучного інтелекту, алгоритму фітрації та модуля виснаження пам’яті при DDoS-атаці. Складові які входять у систему протидії низькошвидкісним

HTTP DDoS-атакам на веб-ресурси є ефективним рішенням, та забезпечують безпеку кінцевих користувачів.

У третьому розділі проведено апробацію розробленої Системи протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси. Проведено оцінку вхідного трафіку за допомогою виявлення аномалій враховуючи особливості, та моніторивши навантаження на систему сервера. Отримані дані показали, система виконує свої задачі та швидко навчається відсіюючи шкідливий/аномальний трафік.

Дисертаційну роботу виконано відповідно до напряму науково-дослідної роботи “Моделювання кібератак на промислові об’єкти, створення розумних систем моніторингу” (№ держ. реєстрації 0123U100245, ДУІКТ, м. Київ). Результати наукових досліджень були використані на кафедрі технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій.

Також результати наукових досліджень прийняті до впровадження в діяльність ТОВ “ СІТОН ДІДЖИТАЛ”, ТОВ “ЛУЧ” та ТОВ “А.А.Г.”.

Ключові слова: низькошвидкісні HTTP DDoS-атаки, система протидії DDoS, аналіз мережевого трафіку, аномалії в пакетах, раннє виявлення атак, модель упередження атак, наліз пакетних груп, динамічні особливості трафіку, фільтрація трафіку, кібербезпека, оцінка ризиків, критична інфраструктура, машинне навчання, захист веб-ресурсів, виявлення загроз.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Лук’яненко Т.Ю. (Lukyanenko T. Yu.), Поночовний П.М. (Ponochovnyy P. M.), Легомінова С.В. (Lehominova S. V.), Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу // *Сучасний захист інформації*, 2022. – № 2. – 15-21. Режим доступу: https://doi.org/10.31673/2409-7292.2022.021521

2. Поночовний П.М. Інформаційна безпека сьогодні// II Всеукраїнської науково-практичної конференції пам’яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського, 29 червня, Київ, 2022 р – С. 77 – 79, покликання на матеріал: https://enpuir.npu.edu.ua/bitstream/handle/123456789/37971/book_2022.pdf?sequence=1&isAllowed=y

3. Опанасенко М.І., Поночовний П.М., Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // *Сучасний захист інформації*, 2023. – № 1. – С.72-78. Режим доступу: https://doi.org/10.31673/2409-7292.2023.010010

4. Прокопенко А.Г., Лаврінець К.Г., Поночовний П.М., Оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення // *Зв'язок*, 2024. – № 4. – С.19-23. Режим доступу: https://doi.org/10.31673/2412-9070.2024.041923

5. Савченко В.А., Поночовний П.М., Аверічев І.М. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. // *Прикладні проблеми комп`ютерних наук, безпеки та математики*. Луцьк: Волинський національний університет імені Лесі Українки, 2024. №3. – С.71-76. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127

6. Поночовний П.М. Модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача // Електронне фахове наукове видання *Кібербезпека: освіта, наука, техніка.* Київ: Київський столичний університет імені Бориса Грінченка, 2024. Том 2 № 26. – С.291-304. Режим доступу: https://doi.org/10.28925/2663-4023.2024.26.695

7. Поночовний П.М., Іванченко І.С. Метод раннього виявлення та захисту від мінливих DDoS атак на основі аналізу обробки пакетних груп // *Наукові записки ДУІКТ* – 2024. No2. – С.153-164. Режим доступу: https://doi.org/10.31673/2786-8362.2024.027035

8. Поночовний П.М., Пепа Ю.В. Реалізація системи захисту серверівз урахуванням аномалій в пакетах // *Вимірювальна та обчислювальна техніка в технологічних процесах*, 2025, №2. м. Хмельницький – С.44-51. Режим доступу: https://doi.org/10.31891/2219-9365-2025-81-6

9. Рижаков М.М., Поночовний П.М. Модель трансформації на основі штучного інтелекту з елементами захисту від DDoS-атак // *Прикладні проблеми комп'ютерних наук, безпеки та математики*. 2025, №4 м. Луцьк – С. 14-32. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128

10. Поночовний П.М., Пепа Ю.В. Система реалізації захисту серверів з урахуванням аномалій в пакетах // *Український журнал досліджень інформаційної безпеки*. 2025, Том 26, №2. м. Київ С. 270-277. Режим доступу: https://doi.org/10.18372/2410-7840.26.20018

11. Поночовний П.М. Автоматизоване реагування на кіберінциденти за допомогою ШІ: міф чи реальність сучасних SOC? // XIIV Міжнародна науково-технічна ITSec-2025 Безпека інформаційних технологій, 2025, м. Тернопіль – с.156-159. Режим доступу: https://drive.google.com/drive/u/0/folders/1f_WDoOIyqDmVMa5eJZDJ-ABFERbSdEWG

12. Ponochovnyy P. M., Pepa Yu. V. Method for determining vulnerabilities to ddos attacks on content management systems // The IV International Conference on emerging technology trends on the smart industry and the internet of things “TTSIIT - 2025”, Kyiv National University of Construction and Architecture -january 30-31, 2025, Ukraine-Iraq-Poland pp. – 95-100. Access mode: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

13. Поночовний П.М. Впровадження систем штучного інтелекту у сфери безпеки і оборони, науки і освіти, економіки, медицини // С34 Системи та засоби штучного інтелекту: тези доповідей Міжнародної наукової молодіжної школи. – Київ: ІПШІ «Наука і освіта», 2023. – С. 30-33. Режим доступу: https://www.ipai.net.ua/docs/AIIS-2023-school.pdf

14. Поночовний П.М. Використання штучного інтелекту в освіті // IV Всеукраїнська науково-практична конференція «Модернізація змісту професійної освіти в умовах євроінтеграції України – 2024», 2024, м. Київ – С.437-439. Режим доступу: https://drive.google.com/file/d/18Jhvyz_tMht0tu7wjcuRpeXN86R3ony4/view

15. Пепа Ю.В., Поночовний П.М., Вплив сторонніх факторів на обробку сигналів // XIII міжнародна науково-практична конференція *«Математика. Інформаційні технології. Освіта»*, 2024, м. Луцьк – с.157-159. Режим доступу: https://drive.google.com/file/d/16GSq2WkNNsnEs6KRBkfCGdcYCKwi1bwO/view

16. Поночовний П.М., Ігор Аверічев І.М., Критерії виявлення повільних DDoS-атак // XIII Міжнародна науково-технічна ITSec-2024 Безпека інформаційних технологій, 2024, м. Львів – с.175-176. Режим доступу: https://drive.google.com/file/d/1N1orbCGW37_pIRTzbHWuEgO3M8lw9B6r/view?usp=drive_link

17. Пепа Ю.В., Поночовний П.М., Інтегральне оцінювання стійкості систем управління // Науково-практична конференція «перспективи та проблематика Інтелектуальних систем», 2024, м. Київ – с.3-4. Режим доступу: https://duikt.edu.ua/uploads/p_2661_35995256.pdf

18. Поночовний П.М., Пепа Ю.В., "Захист освітнього сервера від повільних DDoS-атак" // IV Всеукраїнська науково-практична конференція пам’яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського «Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук», 2024, м. Київ – с.159 – 162. Режим доступу: https://drive.google.com/file/d/1zYSEg2O2x88H3_NHh27EFyTwjRg7mGt6/view

19. Поночовний П.М. "Кіберзагрози в епоху цифровізації: моделювання та захист від DDoS-атак" // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.85 – 86. Режим доступу: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

20. Куліш Є.О., Поночовний П.М., Пепа Ю.В. Оцінка ефективності систем раннього виявлення DDoS-атак // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.17 – 20. Режим доступу: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

21. Поночовний П.М., Іванченко І.С. Експериментальне дослідження системи реалізації захисту серверів з урахуванням аномалій в пакетах // ІІ міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024, м. Київ – С. 173 – 177. Режим доступу: https://duikt.edu.ua/uploads/p_2661_99635945.pdf

ABSTRACT

Ponomochovnyi P.M. System for Counteracting the Anticipation of Low-Rate HTTP DDoS Attacks on Web Resources. - Qualification scientific work on the rights of manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 125 - "Cybersecurity" (12 - Information Technology). - State University of Information and Communication Technologies, Kyiv, 2025.

The dissertation is devoted to improving the reliability of servers through the implementation of a system to counter the impact of low-rate HTTP DDoS attacks on web resources.

The object of the dissertation research is the process of protecting web resources from low-rate HTTP DDoS attacks. *The subject* of the study is systems for protecting web resources against low-rate HTTP DDoS attacks.

The dissertation analyzes existing and modern methods, models, and systems for countering low-rate HTTP DDoS attacks. It is established that traditional approaches—such as traffic limiting or signature-based analysis—are insufficiently effective due to the dynamic nature of attacks that exploit legitimate HTTP requests. Based on this, system requirements were formulated, particularly the need for packet group analysis and anomaly detection at the network interaction level.

The aim of the research is to reduce the effectiveness of low-rate HTTP DDoS attacks on web resources.

To achieve this goal and solve the scientific problem, the dissertation presents the following main scientific results:

For the first time, a model was developed to preempt low-rate HTTP DDoS attacks at the end-user level, enabling early detection and mitigation of such attacks through traffic anomaly detection, filtering algorithms, and memory modules.

For the first time, a method for early detection and protection against low-rate HTTP DDoS attacks was developed. By applying specific filtering conditions—such as limiting the number of requests from a single IP/subnet, blocking traffic from regions without clients, and measuring request duration—the server load can be reduced by 40–60% while preserving system integrity.

For the first time, a system was designed to counter low-rate HTTP DDoS attacks on web resources, taking into account packet anomalies. This system, based on the developed model and method, improves detection and mitigation by 73% through a combination of packet group analysis and dynamic traffic characteristics.

These characteristics are compared to incoming traffic (real-time detection), and the identified anomalies and low-rate HTTP DDoS attacks are transmitted to the "AI Training" module. After processing, data is stored in the "Training Data" block. The training history is used for subsequent threat detections.

Experimental evaluation of the developed system showed a 40–60% reduction in server load compared to baseline solutions. Attack detection accuracy reached 73% due to the combination of packet group analysis and traffic dynamics.

The introduction justifies the relevance of the dissertation topic, outlines the aim and objectives of the study, defines the scientific and practical value of the obtained results, and specifies the author’s personal contribution to joint publications.

Chapter One analyzes methods, models, and systems for preempting low-rate HTTP DDoS attacks. It examines DDoS countermeasures used in Ukraine, considers their specific features, and formulates a scientifically justified approach to solving the problem. The analyzed systems are summarized in Table 1.1 based on 10 key cybersecurity characteristics.

Chapter Two proposes a model for preempting low-rate HTTP DDoS attacks at the end-user level. The model is enhanced through packet feature filtering using artificial intelligence. A comprehensive model for detecting anomalous traffic was developed, taking into account:

- the presence of empty packets;
- request duration;
- region-based encoding.

These features are used to assess user protection. Upon detecting anomalies, the data is processed by AI and transferred to the “Training Data” module. These anomalies will be considered in the next round of input traffic filtering. The chapter also improves the early detection method based on packet group analysis to better protect end-users from behavior resembling low-rate HTTP DDoS attacks.

Furthermore, a System for Countering Low-Rate HTTP DDoS Attacks was designed for the first time. It includes a model based on AI, a traffic filtering algorithm, and a memory exhaustion protection module. These components form an effective solution for securing end users.

Chapter Three presents the validation of the developed system. It evaluates incoming traffic using anomaly detection methods and monitors server load. The results show that the system performs its tasks effectively and adapts rapidly by filtering out malicious/anomalous traffic.

The dissertation was carried out under the scientific research program "Modeling cyberattacks on industrial facilities, creation of intelligent monitoring systems" (State Reg. No. 0123U100245, State University of Telecommunications, Kyiv). The research results have been applied at the Department of Technical Cyber Defense Systems at the State University of Telecommunications.

Also, the results of scientific research have been accepted for implementation in the activities of LLC "SITON DIGITAL", LLC "LUCH" and LLC "A.A.G.".

Keywords: Low-rate HTTP DDoS attacks, DDoS countermeasure system, network traffic analysis, anomalies in packets, early attack detection, attack anticipation model, packet group analysis, dynamic traffic features, traffic filtering, cybersecurity, risk assessment, critical infrastructure, machine learning, web resource protection, threat detection.

LIST OF PUBLICATIONS OF THE APPLICANT

Scientific papers in which the main scientific results of the dissertation are published:

1. Lukyanenko T. Yu., Ponochovnyy P. M., Lehominova S. V., Method for detecting network intrusions and signs of computer attacks based on an empirical approach // Modern Information Security, 2022. – No. 2. – 15-21. Access mode: https://doi.org/10.31673/2409-7292.2022.021521

2. Ponochovnyy P. M. Information security today // II All-Ukrainian Scientific and Practical Conference in memory of Academician of the Academy of Sciences of Higher Education, Professor Anatoliy Volodymyrovych Kaspersky, June 29, Kyiv, 2022 - P. 77 - 79, reference to the material: https://enpuir.npu.edu.ua/bitstream/handle/123456789/37971/book_2022.pdf?sequence=1&isAllowed=y

3. Opanasenko M. I., Ponochovnyy P. M., Technology for ensuring cybersecurity of the cloud environment based on the Cisco Cloudlock solution // Modern Information Security, 2023. – No. 1. – P.72-78. Access mode: https://doi.org/10.31673/2409-7292.2023.010010

4. Prokopenko A. G., Lavrinets K. G., Ponochovnyy P. M., Evaluation of the quality of the technical condition monitoring system of telecommunication networks for special purposes // Communication, 2024. – No. 4. – P.19-23. Access mode: https://doi.org/10.31673/2412-9070.2024.041923

5. Savchenko V. A., Ponochovnyy P. M., Averichev I. M. Detection of DDOS-attack on a high-speed network: survey. // Applied Problems of Computer Science, Security and Mathematics. Lutsk: Lesya Ukrainka Volyn National University, 2024. No. 3. – P.71-76. Access mode: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127

6. Ponochovnyy P. M. Model of prevention of low-speed HTTP DDoS attacks on the end user // Electronic professional scientific publication

Cybersecurity: education, science, technology. Kyiv: Borys Grinchenko Kyiv Metropolitan University, 2024. Volume 2 No. 26. – P.291-304. Access mode: https://doi.org/10.28925/2663-4023.2024.26.695

7. Ponochovnyy P. M., Ivanchenko I. S. Method of early detection and protection against changing DDoS attacks based on the analysis of packet group processing // Scientific notes of DUIKT – 2024. No. 2. – P.153-164. Access mode: https://doi.org/10.31673/2786-8362.2024.027035

8. Ponochovnyy P. M., Pepa Yu. V. Implementation of a server protection system taking into account anomalies in packets // Measuring and computing equipment in technological processes, 2025, No. 2. Khmelnytskyi - P.44-51. Access mode: https://doi.org/10.31891/2219-9365-2025-81-6

9. Ryzhakov M. M., Ponochovnyy P. M. Model of transformation based on artificial intelligence with elements of protection against DDoS attacks // Applied Problems of Computer Science, Security and Mathematics. 2025, No. 4 Lutsk – P. 14-32. Access mode: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128

10. Ponochovnyy P. M., Pepa Yu. V. System for implementing server protection taking into account anomalies in packets // Ukrainian Journal of Information Security Research. 2025, Volume 26, No. 2. Kyiv P. 270-277. Access mode: https://doi.org/10.18372/2410-7840.26.20018

11. Ponochovnyy P.M. Automated response to cyber incidents using AI: a myth or a reality of modern SOCs? // XIV International Scientific and Technical ITSec-2025 Information Technology Security, 2025, Ternopil – pp. 156-159. Access mode: https://drive.google.com/drive/u/0/folders/1f_WDoOIyqDmVMa5eJZDJ-ABFERbSdEWG

12. Ponochovnyy P. M., Pepa Yu. V. Method for determining vulnerabilities to ddos attacks on content management systems // The IV International Conference on emerging technology trends on the smart industry

and the internet of things “TTSIIT - 2025”, Kyiv National University of Construction and Architecture -january 30-31, 2025, Ukraine-Iraq-Poland pp. – 95-100. Access mode: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

13. Ponochnovnyy P.M. Implementation of artificial intelligence systems in the areas of security and defense, science and education, economics, medicine // C34 Systems and means of artificial intelligence: abstracts of reports of the International Scientific Youth School. – Kyiv: ISAI "Science and Education", 2023. – pp. 30-33. Access mode: https://www.ipai.net.ua/docs/AIIS-2023-school.pdf

14. Ponochnovny P.M. The use of artificial intelligence in education // IV All-Ukrainian Scientific and Practical Conference "Modernization of the content of professional education in the conditions of European integration of Ukraine - 2024", 2024, Kyiv - pp.437-439. Access mode: https://drive.google.com/file/d/18Jhvyz_tMht0tu7wjcuRpeXN86R3ony4/view

15. Pepa Yu.V., Ponochnovny P.M., Influence of external factors on signal processing // XIII International Scientific and Practical Conference "Mathematics. Information Technology. Education, 2024, Lutsk - pp.157-159. Access mode: https://drive.google.com/file/d/16GSq2WkNNsnEs6KRBkfCGdcYCKwi1bwO/view

16. Ponochnovny P.M., Igor Averichev I.M., Criteria for detecting slow DDoS attacks // XIII International Scientific and Technical ITSec-2024 Information Technology Security, 2024, Lviv - pp.175-176. Access mode: https://drive.google.com/file/d/1N1orbCGW37_pIRTzbHWuEgO3M8lw9B6r/view?usp=drive_link

17. Pepa Yu.V., Ponochnovny P.M., Integral assessment of the sustainability of control systems // Scientific and practical conference "Prospects

and problems of Intelligent systems", 2024, Kyiv - pp.3-4. Access mode: https://duikt.edu.ua/uploads/p_2661_35995256.pdf

18. Ponochnovny P.M., Pepa Yu.V., "Protection of the educational server from slow DDoS attacks" // IV All-Ukrainian scientific and practical conference in memory of the academician of the Academy of Sciences of Higher Education, Professor Anatoliy Volodymyrovych Kaspersky "Actual problems and prospects for the development of fundamental, applied, general technical and security sciences", 2024, Kyiv - pp.159-162. Access mode: https://drive.google.com/file/d/1zYSEg2O2x88H3_NHh27EFyTwjRg7mGt6/view

19. Ponochnovny P.M. "Cyber threats in the era of digitalization: modeling and protection against DDoS attacks" // All-Ukrainian scientific and practical conference "Actual problems of security of information and telecommunication systems", 2024, Kyiv - pp.85-86. Access mode: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

20. Kulish E.O., Ponochnovnyy P.M., Pepa Yu.V. Evaluation of the effectiveness of early detection systems for DDoS attacks // All-Ukrainian scientific and practical conference "Actual problems of security of information and telecommunication systems", 2024, Kyiv - pp.17-20. Access mode: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

21. Ponochnovnyy P.M., Ivanchenko I.S. Experimental study of the system for implementing server protection, taking into account anomalies in packets // II International Scientific and Practical Conference "Modern aspects of digitalization and informatization in software and computer engineering", 2024, Kyiv - pp. 173-177. Access mode: https://duikt.edu.ua/uploads/p_2661_99635945.pdf

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DDoS	–	Distributed Denial of Service (Розподілена атака відмови в обслуговуванні)
HTTP	–	Hyper Text Transfer Protocol (Протокол передавання гіпертексту)
IP	–	Internet Protocol address (унікальний числовий ідентифікатор мережевого рівня)
ICMP	–	Internet Control Message Protocol (міжмережевий протокол керуючих повідомлень)
IRC	–	Internet Relay Chat
WAF	–	Web Application Firewall (Мережевий екран веб-застосунків)
IPS	–	Intrusion Prevention System (Система запобігання вторгненням)
IDS	–	Intrusion Detection System (Система виявлення вторгнень)
AI	–	Artificial Intelligence (Штучний інтелект)
ML	–	Machine Learning (Машинне навчання)
DoS	–	Denial of Service (Атака відмови в обслуговуванні)
TCP	–	Transmission Control Protocol (Протокол керування передаванням)
TLS	–	Transport Layer Security (Протокол захисту транспортного рівня)
API	–	Application Programming Interface (Програмний інтерфейс застосунку)
CDN	–	Content Delivery Network (Мережа доставки контенту)
QoS	–	Quality of Service (Якість обслуговування)

CAPTCHA	–	Completely Automated Public Turing test to tell Computers and Humans Apart (Автоматизований тест Тюринга для відокремлення людей і комп’ютерів)
SOC	–	Security Operations Center операційні центри безпеки
RPS	–	Requests Per Second (Кількість запитів на секунду)
ОС	–	Операційна система
CPU	–	Central Processing Unit
RAM	–	Random Access Memory
VM	–	Virtual Machine
NGFW	–	Next-Generation Firewall
VPC	–	Virtual Private Cloud
VPS	–	Virtual Private Server
VDS	–	Virtual Dedicated Server
C&C	–	командування і контроль

ВСТУП

Зростання залежності сучасних бізнесів від веб-ресурсів та хмарних технологій призвело до активізації кіберзагроз, серед яких особливе місце займають низькошвидкісні HTTP DDoS-атаки. На відміну від класичних DDoS-атак з високим трафіком, ці атаки діють непомітно, імітуючи легальних користувачів та поступово виснажуючи ресурси сервера. Забезпечення ефективного захисту від таких атак стає критичним для підтримки доступності та продуктивності веб-сервісів.

Основними проблемами, які потребують вирішення, є:

- складність виявлення атак через низьку інтенсивність трафіку, що унеможливлює використання традиційних методів аналізу;

- необхідність балансу між блокуванням шкідливих запитів і збереженням доступності для справжніх користувачів;

- вразливість хмарних інфраструктур через розподілену природу сервісів та залежність від автоматизованих налаштувань;

- відсутність універсальних інструментів для аналізу поведінки користувачів у реальному часі та адаптації до змін у тактиці атак;

Створення спеціалізованої системи протидії низькошвидкісним HTTP DDoS-атакам має враховувати інтеграцію з сучасними технологіями, використання машинного навчання для ідентифікації аномалій, а також постійне оновлення захисних механізмів у відповідь на еволюцію кіберзагроз.

Актуальність:

Сучасні зловмисники все частіше використовують низькошвидкісні HTTP DDoS-атаки, які важко виявити через їхню схожість із легальним трафіком. Такі атаки націлені на довгострокове паралізування веб-ресурсів, що становить загрозу для доступності критичних сервісів (наприклад, електронних урядів або фінансових платформ).

Дослідженням підходів до виявлення та прогнозування низькошвидкісних DDoS-атак займаються як закордонні, так і вітчизняні вчені. Спеціалізація, аналіз поведінки мережевого трафіку, методи виявлення повільних DDoS-атак, Лукова-Чуйко Н.В. [1]. Базова модель параметрів для побудування систем виявлення атак, Корченко А.О. [2]. Класифікація DDoS-атак, включаючи низькоінтенсивні методи, Mirkovic J., & Reiher P. [3, 4]. Механізми виявлення атак на основі часових характеристик трафіку, S. M. Specht, R. B. Lee [5, 6]. Розробка алгоритмів для ідентифікації "повільних" атак на веб-сервери, D. Kagir [7]. Аналіз вразливостей HTTP/HTTPS-протоколів до DDoS із низькою швидкістю, Asosheh A., & Ranezani N. [8, 9]. Дослідження, комбінація машинного навчання та сигнатурного аналізу для блокування DdoS-атак, Douligeris C., & Mitrokotsa A. [10, 11]. Розробка моделі системи виявлення кіберзагроз з підтримкою та оновленням правил виявлення атаки О. Шпур [12]. Системи моніторингу на основі аналізу сесійних даних HTTP, K. Salah [13]. Дослідження механізмів "shrew attacks" та їх впливу на веб-інфраструктуру, A. Kuzmanovic [14]. Вплив перехоплення HTTPS на безпеку, V. Paxson [15].

Аналіз робіт зарубіжних та відчизняних авторів дає змогу зробити висновок, що на сьогодні проблема низькошвидкісних HTTP DDoS-атак досліджена вкрай недостатньо.

Низькошвидкісні HTTP DDoS-атаки порушують роботу серверів, що призводить до втрат доходів, репутаційних збитків та порушення функціонування інфраструктури. Забезпечення стабільності веб-ресурсів є пріоритетом для організацій, які працюють з великою кількістю користувачів.

Існуючі системи захисту часто не розрізняють низькошвидкісні DDoS-атаки та звичайний трафік, що призводить до запізнілого реагування або помилкових блокувань. Це створює потребу в спеціалізованих

рішеннях, орієнтованих на аналіз поведінки користувачів та аномалій у HTTP-запитах.

Традиційні методи блокування DDoS (наприклад, блокування лишень за IP) неефективні проти низькошвидкісних атак, які використовують розподілені джерела та імітують легальних користувачів. Необхідність у розумних алгоритмах, здатних навчатися на нових типах загроз, робить тему дослідження критично важливою для кібербезпеки.

Отже, зважаючи на зв’язок теми дисертації з актуальними науковими та практичними завданнями, вважаємо її вибір обґрунтованим, а саму тему актуальною.

Зв’язок роботи з науковими програмами, планами та темами.

Спрямованість дисертаційного дослідження пов'язана з виконанням Законів України “Про основні засади забезпечення кібербезпеки України” [16], “Про захист інформації в інформаційно-комунікаційних системах” [17], “Про інформацію” [18], “Про захист персональних даних” [19], “Про національну безпеку України” [20].

Дисертаційна робота виконана за планами наукових і науково-технічних робіт Державного університету інформаційно-комунікаційних технологій та в рамках науково-дослідної роботи “Моделювання кібератак на промислові об’єкти, створення розумних систем моніторингу” (№ держ. реєстрації 0123U100245, ДУІКТ, м. Київ).. (внесок автора, пошуку ризиків, пов'язаних із захистом безпеки сервера, що є важливою частина роботи, наступним кроком якої є розробка методів виявлення та пом'якшення цих загроз.).

Метою дослідження кваліфікаційної роботи є зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси.

Для своєчасного виявлення прихованих кіберзагроз необхідно вирішити наступні **задачі**:

- проаналізувати системи захисту від низькошвидкісних HTTP DDoS-атак та їх ефективності;
- розробити модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача для запобігання кіберінцидентам в кіберпросторі;
- розробити метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак шляхом аналізу обробки пакетних груп;
- розробити систему протидії низькошвидкісним HTTP DDOS-атакам на веб-ресурси, яка враховує аномалії в пакетах для підвищення ефективності захисту від низькошвидкісних HTTP DDoS-атак;
- провести експериментальне дослідження розробленої системи протидії низькошвидкісним HTTP DDoS-атак на веб-ресурси.

Об`єктом дослідження процес захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак.

Предметом дослідження системи захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак.

Методи дослідження базуються за допомогою визначення груп пакетів в часовому вікні. Це надає можливість створити особливості, за допомогою яких забезпечується раннє виявлення та захист від низькошвидкісних HTTP DDoS-атак. Достовірність наукових результатів, висновків та рекомендацій, викладених у дисертаційній роботі, обґрунтовано правильним використанням математичного апарату, моделюванням на обчислювальних пристроях, а також аналізом впливу низькошвидкісних HTTP DDoS-атак на ймовірність успішних DDoS-атак. Результати теоретичних досліджень було підтверджено результатами симуляцій та експериментального моделювання в умовах різних сценаріїв визначення захищеності.

Наукова новизна одержаних результатів полягає у наступному:

- *вперше* розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача, яка за рахунок виявлення аномального потоку, алгоритму фільтрації трафіку, модуля пам’яті, дозволить передувати та протидіяти низькошвидкісним HTTP DDoS-атакам на рівні кінцевого користувача;

- *вперше* розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, який за рахунок умов фільтрації трафіку, а саме обмеження кількості запитів з одного IP/підмережі, блокування трафіку з регіонів, де немає клієнтів, тривалості запиту, дає можливість зменшити навантаження на сервер від 40 до 60 % і підтримати цілісність системи.

- *вперше* розроблено систему протидії низькошвидкісним HTTP DDOS-атакам на веб-ресурси з урахуванням аномалій в пакетах, яка за рахунок розроблених моделі та методу, дає можливість упередженню та покращенню захисту від низькошвидкісних HTTP DDoS-атак на 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей.

Практичне значення одержаних результатів:

- алгоритм роботи системи захисту серверів, який складається з адаптивної моделі штучного інтелекту. Результати дисертаційної роботи були використані на кафедрі Технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій під час виконання науково-дослідної роботи на тему «Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси» (ДУІКТ, м. Київ), та впроваджені у виробничий процес на підприємствах: ТОВ «СІТОН ДІДЖИТАЛ»; ТОВ «ЛУЧ»; ТОВ «А.А.Г.».

Особистий внесок здобувача складається з робіт, що опубліковані в співавторстві, де в дисертаційній роботі використано тількі результати

дослідження, що були отриманні виключно здобувачем. У роботах, опублікованих в співавторстві, автором: методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу [21]; технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock [22]; оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення [23]; виявлення DDoS-атаки на високошвидкісну мережу: опитування [24]; модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача [25]; метод раннього виявлення та захисту від мінливих DDoS-атак на основі аналізу обробки пакетних груп [26]; система реалізації захисту серверів з урахуванням аномалій в пакетах [27]; модель трансформації на основі штучного інтелекту з елементами захисту від DDoS -атак [28].

Апробація результатів дисертації. Результати дисертаційної роботи представлені та обговорені на міжнародних науково-технічних та науково-практичних конференціях: «Штучний інтелект та інтелектуальні системи AIIS`2023 XXIII міжнар. наук.-тех. конф.» (м. Київ, 2023) [29], «Математика. Інформаційні технології. Освіта XIII міжнар. наук.-практ. конф.» (м. Луцьк, 2024) [30], «ITSec-2024: Безпека інформаційних технологій: матеріали XIII міжнар. наук.-тех. конф.» (м. Львів, 2024) [31], «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії II міжнар. наук.-практ. конф.» (м. Київ, 2024) [32], «TTSIIT – 2025 The IV International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things» (Ukraine - Iraq – Poland, 2025) [33], «ITSec-2025: Безпека інформаційних технологій: матеріали XIV міжнар. наук.-тех. конф.» (м. Тернопіль, 2025) [34]

Публікації. Наукові результати дисертаційної роботи опубліковано у 21 науковій праці, із них: 9 наукових статей, надрукованих у відчизняних

фахових наукових виданнях, а також 12 тез доповідей на науково-практичних конференціях, 6 із них міжнародні.

Структура та обсяг дисертаційної роботи.

Дисертація складається із вступу, трьох розділів та висновків до них, а також бібліографії, що містить 145 посилань на 17 сторінках. Загальний обсяг роботи становить 183 сторінки, з них 132 сторінки основного тексту, 68 малюнків, 16 таблиць.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СИСТЕМ ПРОТИДІЇ НИЗЬКОШВИДКІСНИХ DDOS-АТАК

1.1. Аналіз методів упередження низькошвидкісних DDoS-атак

У період активного розвитку та впровадження інформаційних технологій у повсякденне життя важливу роль відіграє надійність комп’ютерних систем, що забезпечують доступ до інформації та її зберігання. Але разом із тим, як зростає важливість інформації, зростають і збитки, які виникають у результаті крадіжки, знищення або відсутності доступу до тієї чи іншої інформації.

Атака, що призводить до неможливості отримання інформації або неможливості подальшої роботи комп'ютерних систем без перевантаження, називається «атакою на відмову в обслуговуванні» DoS (Denial of Service). Цей тип атаки запобігає або повністю блокує відповіді служб законним користувачам.

На практиці набагато легше порушити роботу мережі або системи, ніж отримати несанкціонований доступ. Атака «відмова в обслуговуванні» істотно змінила Інтернет, показавши слабкі місця в захисті використовуваних технологій.

Характерною особливістю DoS і DDoS (Distributed DoS) атак є те, що їх запобігання неможливе без попередньої підготовки. Ще більш неприємний факт, що навіть за умови попередньої підготовки протидіяти їм важко. На жаль, більшість серверів в Інтернеті недостатньо захищені брандмауером або більш складним типом захисту від атак.

Необхідна система аналізу аномалій на основі штучного інтелекту з використанням математичних алгоритмів для вирішення проблеми перевантаження мережі. На практиці – це розробки численних інститутів, роки практичного вивчення DDoS-атак і результати десятків дисертацій.

Захист від DDoS - складна програма, яка потребує високої концентрації найновіших досягнень у галузі аналізу трафіка і автоматично реагує на атаку. Методи атак можуть динамічно змінюватися, і система повинна відстежувати та вживати відповідних заходів.

Незважаючи на те, що у світі проводиться велика кількість досліджень і розробок в галузі боротьби з DDoS-атаками, у більшості випадків вони не доводяться до широкої публіки, і спостерігається нестача публікацій про конкретні розробки.

Готова продукція різних компаній зазвичай недоступна для використання в умовах України через її високу ціну. В основному це стосується звичайних користувачів, які використовують сервери на базі GNU/Linux.

Різноманітність загроз, що наражають на небезпеку користувача, який працює в мережі, величезна. Частина з них є платою за використання складних інформаційних технологій, вразливих до зовнішніх впливів, інша частина пов'язана з діяльністю людини.

Низькошвидкісна FTTP DDoS-атака (або "низька і повільна" DDoS-атака в контексті волоконно-оптичного підключення, Fiber to the Premises) — це тип атаки на відмову в обслуговуванні, який використовує повний потік даних для встановлення ресурсів цільового сервера чи мережі, виявляючи традиційні методи захисту. Такі атаки спрямовані на відповідний рівень (Layer 7 моделі OSI) або транспортний рівень (Layer 4), використовуючи легітимний на вигляд трафік, що ускладнює їх розпізнавання.

Основні характеристики низькошвидкісних FTTP DDoS-атак:

Низька інтенсивність трафіку. На відміну від об'ємних DDoS-атак, які перевантажують пропускну здатність мережі величезною кількістю запитів, низькошвидкісні атаки надсилають невеликі обсяги даних із вільною швидкістю, щоб не викликати враження.

Тривале утримання з'єднань. Зловмисники встановлюють численні з'єднання з сервером і підтримують їх відкритими, надсилаючи дані дуже повно (наприклад, один байт кожні кілька хвилин), що визнає ресурси сервера, як кількість доступних з'єднань, пам'ять чи процесорний час.

Цільовий вплив. Атаки часто спрямовані на веб-сервери, які базуються на потоках (на основі потоків), де кожен вільний запит відвідує потік, блокуючи доступ легітимним користувачам.

Найпоширеніші типи низькошвидкісних DDoS-атак:

Slowloris зловмисник надсилає часткові HTTP-запити, не завершуючи їх, що змушує сервер отримати з'єднання відкритим, визнаючи його ресурси.

RUDY (RU-Dead-Yet) дана атака використовує вільне надсилання даних у HTTP POST-запитах, заповнюючи форми на сервері та перевантажуючи його.

Sockstress атака спрямована на експлуатацію вразливості в TCP/IP, створюючи незавершені з'єднання через маніпуляції з потрійним рукостисканням TCP.

Slow Read зловмисник надсилає легітимні запити, але читає відповіді дуже повно, утримуючи з'єднання відкритими та споживаючи ресурси сервера.

Slow Post дана атака відома тим, що надсилає легітимні HTTP POST-запитів із вільною передачею даних у тілі запиту, що вимагає сервер чекати завершення.

FTTP (Fiber to the Premises) забезпечує високу пропускну здатність і низьку затримку, що робить його привабливим для атакуючих, оскільки дозволяє точно керувати повними потоками даних. Однак низькошвидкісні атаки не залежать від швидкості мережі, а більша здатність підтримувати численні з'єднання. У FTTP-середовищі такі атаки можуть бути ефективними через:

Висока стабільність з'єднання. Волоконно-оптичні мережі рідко втрачають пакети, що дозволяють атакувати надійне з'єднання.

Велика кількість IoT-пристроїв. FTTP часто використовують для підключення розумних пристроїв, які можуть бути скомпрометовані для створення ботнетів, що беруть участь у низькошвидкісних атаках.

Атака «відмова в обслуговуванні» має багато різних визначень. Міжнародний консультативний комітет з телеграфу та телефонії (CCITT) у рекомендації X.800 описує відмову в обслуговуванні як «запобігання авторизованому доступу до ресурсів або затримку виконання критично важливих операцій». Комітет із систем національної безпеки додає примітку до цього визначення, що «критичним часом можуть бути мілісекунди або години, залежно від наданої послуги» [35, 36, 128, 134].

Аналіз поведінку низькошвидкісних HTTP DDoS-атак для їх виявлення потрібно звернути увагу на наступні порушення в роботі легітимного трафіку:

- порівняння нормального трафіку з позитивним, наприклад, якщо час виконання запитів (наприклад, заповнення форми) значно збільшується;
- моніторинг ресурсів, відстеження використання ЦП, пам'яті, таблиці з'єднань і потоків додатків у реальному часі;
- аномалії в трафіку, виявлення незвичних патернів, таких як велика кількість відкритих з'єднаних із низькою швидкістю передачі.

Тим часом Інститут розробки програмного забезпечення підкреслює мету атаки та визначає, що «основна мета атаки полягає в тому, щоб відмовити жертві (жертвам) у доступі до певного ресурсу». Словник загальноприйнятих термінів безпеки Bright Hub у визначенні «Відмова в обслуговуванні» також вказує на мету цієї атаки, однак у ньому додатково згадується, що «DoS-атака — це метод перевантаження мережі

запитами на підключення до справа в тому, що він не може нормально функціонувати» [37, 38].

Однак на практиці послуга може бути відмовлена не лише через перевантаження системних ресурсів, але й через використання вірусів, хробаків. У цій роботі не буде аналізу цієї частини відмови в обслуговуванні, а акцент буде зосереджено на атаках на відмову в обслуговуванні, коли зловмисник використовує величезну кількість надісланого трафіку, щоб атакувати жертву, викликаючи її відмову в обслуговуванні через надіслані обсяг трафіку [39].

Для досягнення більшого розміру трафіку атаки можна використовувати кілька джерел атаки. Техніка відмови в обслуговуванні, яка використовує численні хости для здійснення атаки, називається розподіленою відмовою в обслуговуванні (DDoS). Це не означає, що зловмисник володіє великою кількістю комп'ютерів для здійснення DDoS-атаки. Зазвичай цей тип атаки використовує армію пошкоджених і контрольованих хостів – ботнетів. Тому, щоб краще зрозуміти DDoS-атаки, слід знати принципи ботнету [40, 41].

Ботнет — це набір хостів, заражених шкідливим програмним забезпеченням (званим роботами, ботами або агентами), яке працює автономно й автоматично без відома власника машини. Інфікована машина передає свій контроль творцю бота (званому botheader або botmaster), тому творець може використовувати всі контрольовані машини для бажаних зловмисних цілей навіть без знання користувача контрольованої машини. Використовувати ботнет для зловмисників безпечніше та дешевше, ніж володіти такою ж кількістю реальних хостів [42, 43].

Аналізуючи життєвий цикл ботнету, можна виділити кілька основних етапів [39, 44, 45, 46]:

- сканування потенційно вразливих машин.
- компрометація обраних машин.

- доставка шкідливих програм.
- встановлення підключення до ботнету.

Сканування зазвичай виконується вже існуючими ботами в ботнеті, а не самим ботмайстром. Його мета — виявити якомога більше потенційно вразливих машин. Тому використовується кілька методів сканування [44, 45, 48]:

- випадкове сканування – довільно вибрані IP-адреси.
- сканування Hitlist – існуючий список вразливих IP-адрес.
- сканування на основі маршрутизації – збір інформації про наявні IP-адреси за допомогою префіксів маршрутизації BGP.
- розділяй і володарюй сканування – багато ботів сканують різні IP-простір.
- сканування локальних налаштувань – усі боти сканують IP-адреси з локальної мережі.
- топологічне сканування – збір інформації з даних ботів, залишених його користувачем і з використанням його машини.

Перестановка – усі боти спільно використовують загальну псевдовипадкову перестановку простору IP-адрес.

Сканування є одним із найважливіших етапів вербування ботнетів, тому різні хробаки використовують різні стратегії сканування [47, 48, 49]. Стратегії сканування, які використовують різні хробаки, підсумовано в табл. 1.1.

Коли список IP-адрес збирається (або навіть під час пошуку IP-адрес), усі IP-адреси перевіряються на наявність вразливостей, яким вони можуть бути подані. Якщо виявлені вразливості та IP-адреси піддаються їм, наступним кроком є завантаження шкідливого програмного забезпечення ботів.

Зазвичай експлойт і закодоване шкідливе програмне забезпечення упаковані в один сценарій і доставлені так само, як віруси, хробаки чи

тройські коні [50]. Однак Agabot почав розділяти доставку експлойтів і шкідливих програм. Спочатку надсилається експлойт, потім він відкриває оболонку на віддаленому хості та завантажує закодовану шкідливу програму через HTTP або FTP.

Таблиця 1.1.

Стратегії сканування, які використовують різні хробаки

Стратегія сканування / хробаки	випадковий	список хітів	на основі маршруту	розділяй і володарюй	місцеві переваги	топологія	перестановка
Slammer (Moore, D.)	✓						
CodeRed II (Moore, D.)	✓				✓		
Witty (Kuma, A.)	✓	✓					
Warhol (Weave, N.C.)		✓					✓
Flash (Zou, C.C.)		✓		✓			
Routing slammer worm (Zou, C.C.)			✓				
Morris (Eichin, M. and Rochlis, J.)						✓	

Вчений J. Mirkovic розрізняє два основних типи того, як шкідливе програмне забезпечення можна завантажувати за допомогою окремих експлойтів і шкідливих програм. Перший метод полягав би в тому, щоб вимагати код з оригінальної машини, яка заражає ціль. Однак, якщо було отримано джерело експлойту, можна відстежити інфіковану машину. З іншого боку, лише один бот буде відстежений, якщо інформацію про місце завантаження коду зловмисного програмного забезпечення буде видалено одразу після доставки коду зловмисного ПЗ. (рис. 1.1.). Другий спосіб передбачає використання центрального джерела, яке використовується лише для зберігання шкідливих програм. Це дозволяє захистити інформацію зловмисників, однак, якщо інформацію про центральне

джерело можна було б отримати, центральне джерело було б усунено, а поширення ботнету було б зупинено (рис. 1.2.).

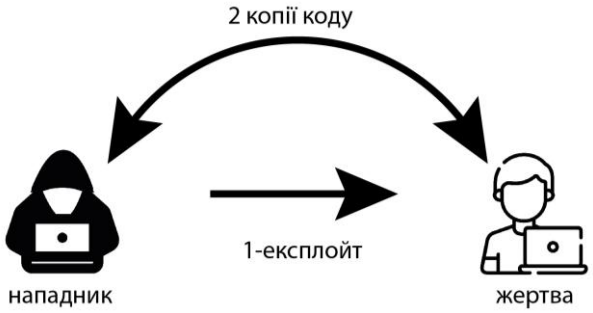


Рис. 1.1. Способи завантаження зловмисного ПЗ окремо від доставки експлойтів, коли код зловмисного ПЗ завантажується від зловмисника.

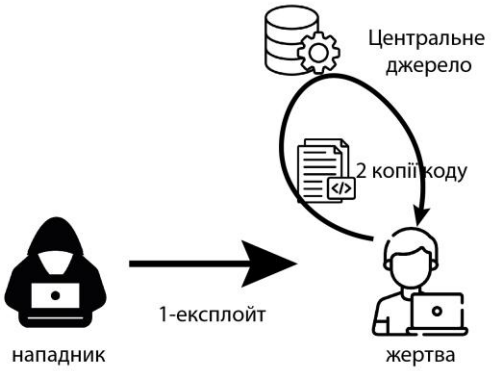


Рис. 1.2. Способи завантаження зловмисного ПЗ окремо від доставки експлойтів, коли код зловмисного ПЗ завантажується з центрального джерела.

Головною особливістю ботнету є можливість контролювати всі боти, щоб разом виконувати певне завдання [51]. Тому мережа керування повинна бути складена. Найпоширеніший механізм керування агентом називається командуванням і контролем (C&C) (див. рис. 1.3) [52]. Він використовує один або кілька хостів як центральну точку для прямого зв’язку з ботами. Ці командні сервери отримують команди від свого бот-майстра та пересилають їх іншим роботам у мережі [53].

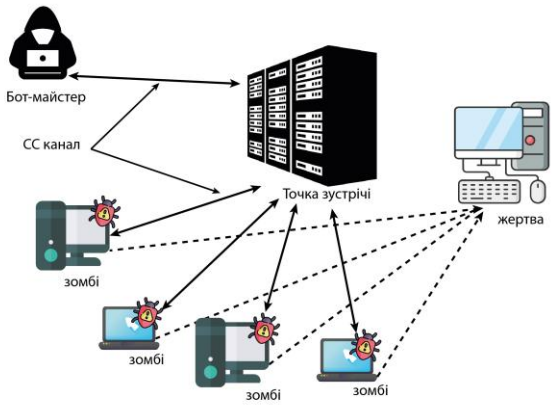


Рис. 1.3. Схема управління агентами командування та управління.

Зазвичай для керування ботами використовується протокол IRC (Internet Relay Chat). Botmaster надсилає команди на C&C сервер, який передає команди в кімнату діаграм, тоді як усі боти завжди чекають команд у цій кімнаті. Ця керуюча мережа має визначену структуру. Однак він досить вразливий через централізований механізм управління. Якщо сервери C&C були знайдені та нейтралізовані, уся комунікаційна мережа Botnet буде втрачена [54]. Для усунення цього недоліку можна використовувати інші комунікаційні архітектури – P2P (Peer-to-Peer). У цій архітектурі немає централізованої точки для C&C, оскільки всі вузли діють і як клієнт, і як сервер (див. рис. 1.4). Таким чином, якщо один бот нейтралізований, вплив на інших ботів дуже малий, і ботнет продовжує працювати належним чином [55].

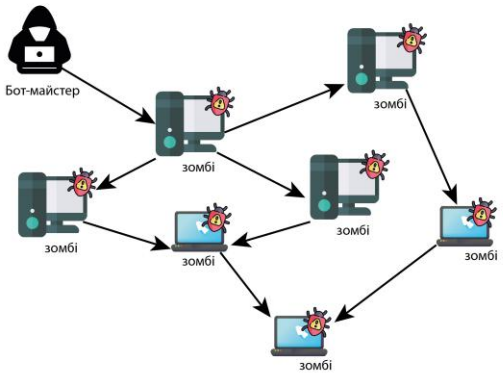


Рис.1.4. Схема керування одноранговим агентом.

Однак кібератаки не припиняють розвиватися, як і архітектури комунікаційних мереж Botnet. Wang J. пропонує гібридну комунікаційну архітектуру ботнету P2P. Він використовує P2P для зв'язку керуючих ботів, тоді як кожен керуючий бот спілкується з певною кількістю клієнтських ботів [51]. (див. Мал. 1.5).

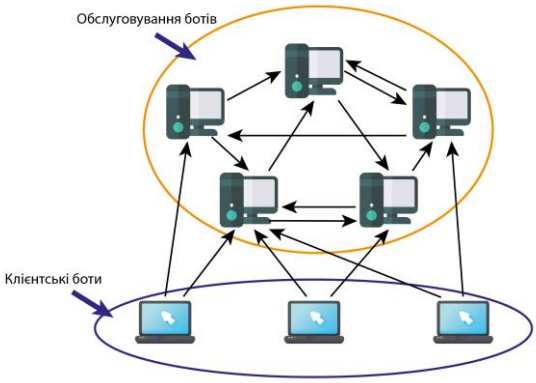


Рис.1.5. Гібридна однорангова схема керування агентом

Зазвичай зловмисник використовує кілька сходинок, щоб ускладнити відстеження. Тому на практиці слід використовувати більш складні схеми управління агентами.

Атака TCP SYN є однією з найвідоміших і використовуваних атак із виснаженням ресурсів. Атака SYN flood відбувається під час тристороннього рукостискання, яке позначає початок TCP-з'єднання. У тристоронньому рукостисканні клієнт запитує нове з'єднання, надсилаючи пакет SYN на сервер. Після цього сервер надсилає клієнту пакет SYN/ACK і поміщає запит на підключення в чергу. Нарешті, клієнт підтверджує пакет SYN/ACK.

Проте, якщо відбувається атака, зловмисник надсилає жертві велику кількість SYN-пакетів, змушуючи її відкривати багато TCP-з'єднань і відповідати на них. Тоді зловмисник не виконує третій крок тристороннього рукостискання, який слідує, роблячи жертву нездатною приймати будь-які нові вхідні з'єднання, оскільки її черга заповнена

напіввідкритими з'єднаннями TCP. Здебільшого зловмисник надсилає підроблений пакет жертві, що призводить до того, що пакет SYN/ACK повністю надсилається на інший хост, який не відповідає, оскільки не надсилав жодних пакетів SYN жертві [56, 117].

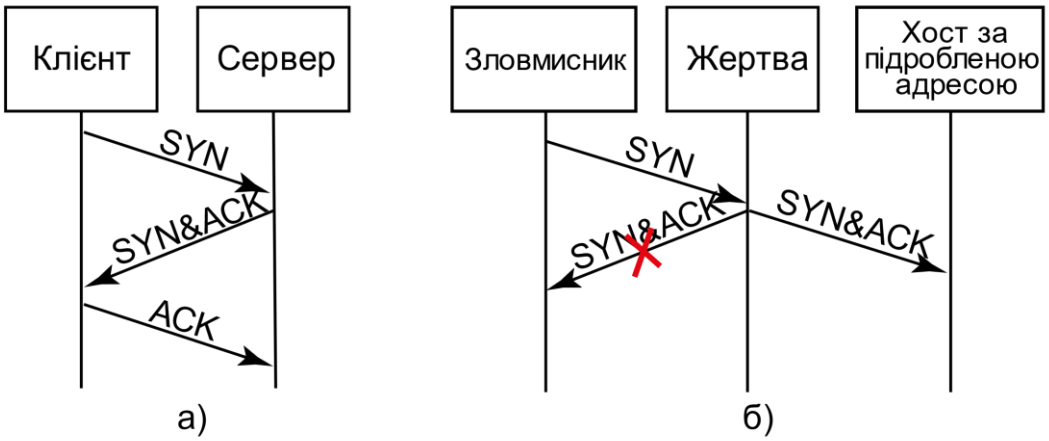


Рис. 1.6. Потік пакетів у тристоронньому рукостисканні (а) та атаці TCP SYN (б)

Стандартними діями для захисту системи є збільшення розміру буфера, зменшення періоду часу збереження незавершеного з'єднання в стані SYN RECEIVED у черзі, увімкнення вбудованих механізмів захисту [57]. Найвідомішими механізмами захисту є SYN-кеш, SYN cookie, Synkill тощо. Однак усі ці контрзаходи мають обмеження, і їх слід вибирати з розумом, щоб максимізувати стійкість до DDoS-атак [58, 59].

Атака Smurf використовує підроблену адресу. Він надсилає широкомовний пакет PING із фальшивою IP-адресою (яка встановлена як IP-адреса жертви) до певної мережі чи навіть багатьох мереж. Відповідно всі комп'ютери відповідають на цей пакет на надану IP-адресу, тому весь потік йде до одного хосту – жертви (див. рис. 1.7). Вхідний трафік може бути настільки великим, що жертва (хост або навіть мережа) не зможе обслуговувати весь трафік, оскільки його пропускна здатність вичерпана [60, 61, 62, 111].

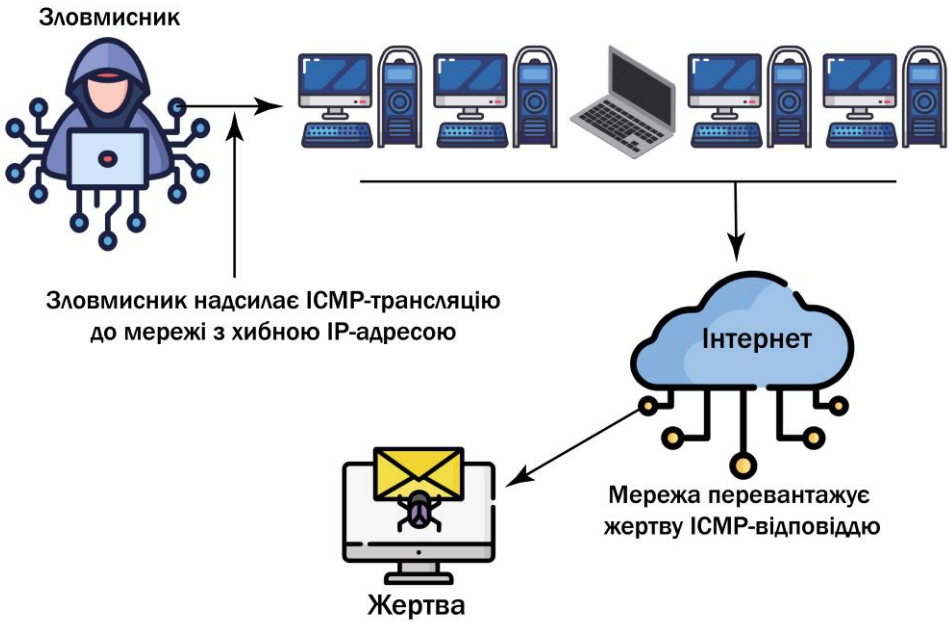


Рис. 1.7. Смурф атакує мережу

Згідно з дослідженням Інституту розробки програмного забезпечення (CERT 1998), можуть бути рішення для атаки Smurf на 3 рівнях для посередника, жертви та сайту, з якого походять атаки. Щоб запобігти вашій участі в атаці Smurf, можна вимкнути пряму IP-трансляцію та відповідь на пакети ICMP, надіслані на широкомовні IP-адреси. Однак для жертви та сайту, з якого походять атаки, немає настільки ефективних рішень, і вони можуть в основному покладатися на фільтрацію пакетів, яка в багатьох випадках не є достатньо ефективною.

Перша відома розподілена атака типу «відмова в обслуговуванні» сталася в 1996 році, коли Panix, один із найстаріших інтернет-провайдерів, був виведений з мережі на кілька днів через SYN-флуд – техніку, яка стала класичною DDoS-атакою. Протягом наступних кількох років DDoS-атаки стали поширеними, і Cisco прогнозує, що загальна кількість DDoS-атак подвоїться з 7,9 мільйона у 2018 році до чогось понад 15 мільйонів до 2023 року. Аналіз Cisco загальної історії та прогнозів DDoS-атак рис. 1.8.

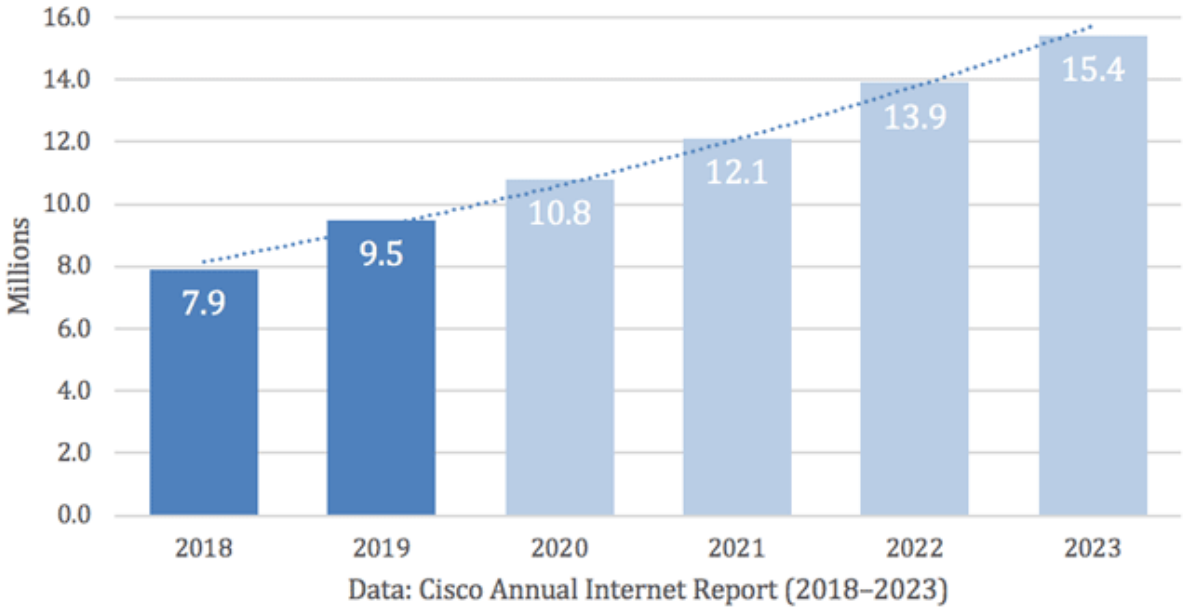


Рис. 1.8. Аналіз Cisco загальної історії та прогнозів DDoS-атак.

Однак, зростає не лише кількість DDoS-атак. Зловмисники створюють дедалі більші ботнети – армії зламаних пристроїв, які використовуються для генерації DDoS-трафіку. Зі збільшенням розмірів ботнетів зростає також масштаб DDoS-атак. Розподіленої атаки типу «відмова в обслуговуванні» зі швидкістю один гігабіт на секунду достатньо, щоб вивести більшість організацій з Інтернету, але зараз ми спостерігаємо пікові розміри атак, що перевищують один терабіт на секунду, що генеруються сотнями тисяч або навіть мільйонами підкуплених пристроїв.

Nuke — це одна з атак типу «відмова в обслуговуванні», які вже використовуються протягом найдовшого періоду. Він використовує модифіковані пакети ICMP і надсилає жертві, яка не здатна правильно обробити надіслане. Обробка модифікованої утиліти ping вимагає більше часу, тому система сповільнюється і навіть може повністю зупинитися.

Щоб досягти бажаного ефекту DoS за допомогою атаки Nuke, жертві слід надіслати багато модифікованих фрагментованих даних. Nuke-

атаки також можна здійснити в системах обміну миттєвими повідомленнями або онлайн-ігор [63, 124, 125, 126].

Деякі DoS-атаки можуть бути виконані на прикладному рівні і не вимагають від зловмисника знання протоколу чи структури пакету. Одним із таких прикладів є використання символів підстановки SQL для використання центрального процесора (CPU) на сервері бази даних. Як показує Mavituna, F., якщо веб-додаток використовує форму пошуку, де використовуються запити LIKE із символами підстановки, звичайний користувач може шукати рядок «_[aaaaaaaaa[! -z]@$!_» замість «foo», і це призведе до того, що сервер бази даних виконуватиме SQL-запит набагато довше. Якщо веб-програми використовують запити LIKE із кількома пошуковими термінами, виконання запиту sql може тривати навіть довше.

Що стосується цієї вразливості, навіть група користувачів, які виконують пошуки, що потребують багато часу, можуть спричинити проблеми для системи, і те саме можна сказати про величезну кількість агентів, які атакують одночасно.

Цей вид DoS-атак можна усунути, правильно проектуючи та реалізовуючи веб-програми: розробникам слід уникати використання символів узагальнення SQL для звичайних користувачів або використовувати додаткові елементи, як впровадження CAPTCHA або головоломки, щоб уповільнити роботу користувача та довести свою людяність [63].

Аналізуючи, чому DoS доступний, існує багато причин, чому DoS-атаки є успішними. Ефект DoS може бути викликаний навіть законними користувачами систем, навіть без поганих намірів. Одна з останніх відомих зустрічей, коли законні користувачі викликали відмову в системі обслуговування, стався 14 березня 2011 року, в перший день онлайн-продажу квітків на Євробаскет 2011. Усі користувачі намагалися якомога

швидше купити квітки та отримати найкращі місця. Проте система не змогла впоратися з такою величезною кількістю запитів.

Це вплинуло на час обслуговування, а іноді деякі користувачі взагалі не обслуговувалися. [64, 65].

Це лише один приклад того, коли відмова в обслуговуванні може статися без будь-якої форми зловмисного наміру. Аналізуючи, як може бути викликана DoS, їх багато. Але єдиного загальноприйнятого стандарту класифікації DDoS-атак і низькошвидкісних DDoS-атак не існує.

1.2. Дослідження моделей упередження низькошвидкісних DDoS-атак

Аналізуючи, як можна викликати DoS, існує багато різних способів. Однак єдиного стандарту класифікації DDoS-атак і низькошвидкісних DDoS-атак не існує.

Немає єдиного стандарту групування атак DoS і DDoS, тому наведемо кілька різних способів. У своїй роботі вчені Д. Каріг і Р. Лі по окремих DoS-атаках на п'ять категорій за місцем атаки:

- на рівнях мережевого пристрою;
- на рівні операційної системи;
- на рівні програми;
- потік даних;
- особливості протоколу.

Ця категорія є основною і показує, до якої категорії в класифікації належить об’єкт установки, тобто захист. Але він не деталізує всі властивості атаки, важливі для аналізу та вибору відповідних контрзаходів. Тому, що існує перезавантаження інформації, атака спрямована на функції протоколу та була фрагментована на менших частинах. Цього недостатньо, щоб описати повний сценарій DoS-атаки. Вчені A. Fadallallah і A. Serhrouchni [67] вибирають таксономію DoS-атаки, враховуючи кількість

комп’ютерів, які використовують для здійснення однієї атаки. Таксономія DoS-атак показана на рис. 1.9.

Аналізуючи структуру виникнення механізмів DDoS-атак, не може існувати єдиного стандарту для для класифікації даних видів кіберзагроз. Тому в дослідженні розглянуто декілька різних способів. Вчені Д. Каріг і Р. Лі у своїй дослідженнях класифікують DoS-атаки враховуючи низку особливостей, а саме на місце де відбувається атака. Поділяючи дані особливості на п’ять категорій [66]:

- атака зосереджена на виведення з ладу мережевих пристроїв;
- атака зосереджена на виведення з ладу операційної системи;
- атака відбувається на рівні прогарних застосунків;
- потік даних;
- особливості протоколу.

Така класифікація є напрочут простою, та дає можливість відразу визначити місце яке атакує кіберзлочинець, таким чином дає можливість захистити об'єкта, або клієнта мережі. Проте така класифікація не описує всіх можливих властивостей атаки, які є важливими для аналізу та боротьби з кіберінцидентами. Дана дія відбувається тому, що дані перенасичують технічні характеристики сервера так як низькошвидкісна DDoS-атака спрямована на особливості протоколу і поділяється на менші частини. Даної інформації недостатньо для того, щоб описати всю механіку DDoS-атаки.

Вчені А. Фадлаллах і А. Сергроучні [67] в своїх дослідженнях застосовують наступну класифікацію DoS-атак, враховуючи кількість комп’ютерів, які можуть бути застосовані для виконання однієї атаки. На рис. 1.9. наведено класифікація DoS-атак.

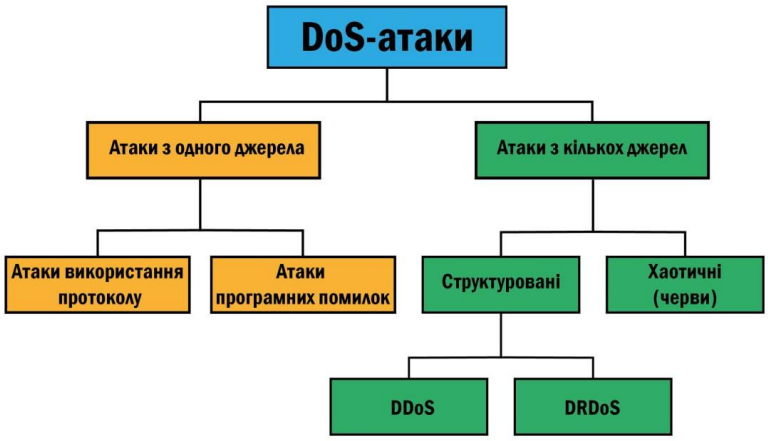


Рис. 1.9. Класифікація DoS-атак

Вони поділяють DoS-атаки на дві наступні категорії (рис. 1.9.):

- атаки, які відбуваються з одного ресурсу;
- атаки, які відбуваються одночасно з декількоє ресурсів.

Кількість помилок протоколу та програмного забезпечення додатково класифікуються на відміну від атак на обслуговування, розподілену відмову в атаках обслуговування та напади шарів додатків. У той же час напади з декількох ресурсів варто класифікувати на хаотичні та структуровані (розділяти їх за відмовами з одного джерела та проста розподілена відмова у обслуговуванні).

Ці DOS-атаки прості для розуміння та демонструють межі атаки DOS та DDOS. Проте не враховуються інші особливості атаки, наприклад тип використовуваної вразливості.

Посилання [66, 68], які виявляють відсутність таксономії DDoS-атаки, є більш детальними та сортують більше властивостей атаки.

Вчені К. Дулігерис та А. Мітрокоца не розрізняли цілі [69], в їх працях основна увага була приділена опису атаки за повним підходом (рис. 1.10.):

• ступінь автоматизації;

• використані уразливості;

• швидкість атаки та її динаміка;

• вплив.

Ця класифікація розглядає всі чотири групи та їхні підходи до опису кожної атаки. Це дозволить нам вибрати відповідне рішення з цих категорій та створити чітке рішення для даного різновиду кібератак.

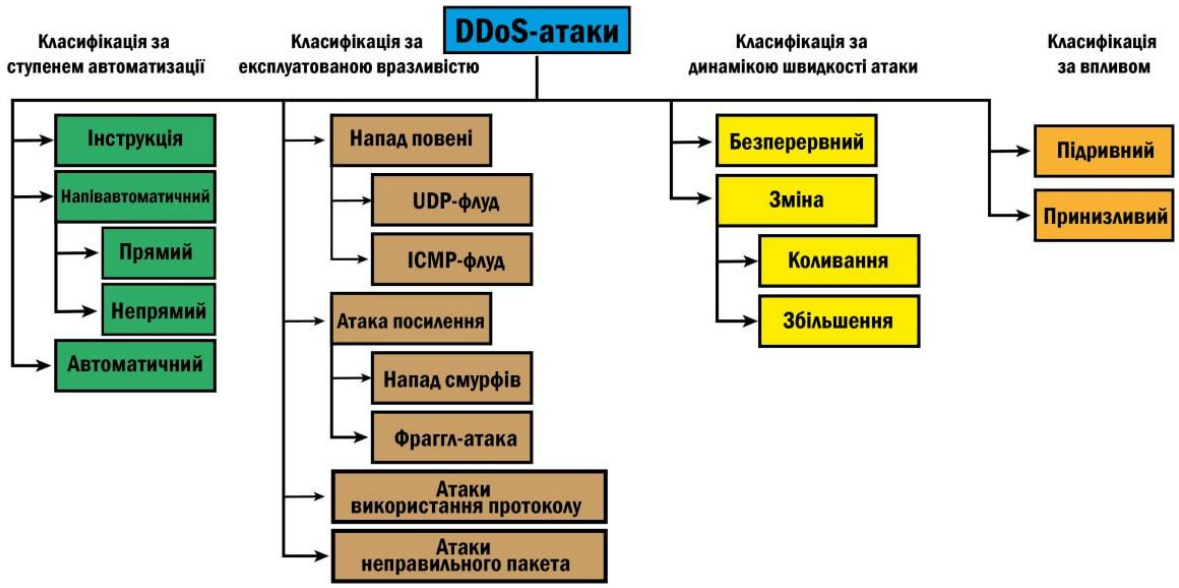


Рис. 1.10. Класифікація DoS-атак запропонована К. Дулігерис

Вчені Дж. Міркович та П. Рейхер [67] слідкують за аналогічною структурою класифікації DDoS-атак. Це дає можливість групувати методи DDoS-атаки на вісім різних типів. (рис. 1.11):

- автоматизація;
- експлуатована слабкість;
- достовірність адреси джерела;
- динаміка швидкості атаки;
- можливість характеристики;
- постійність набору агентів;
- тип жертви;
- вплив на потерпілого.

Ця класифікація зосереджена на описі DDoS-атаки з точки зору зловмисника. Даний опис досить повний і підходить для представлення DDoS-атаки, однак опис за усіма ознаками є дуже складним. Це пояснюється тим, що для нових модифікації DDoS-атак додатково необхідно проаналізувати та вивчати їх поведінку. Для того, щоб налаштувати деякі властивості, необхідні для створення нової класифікації.

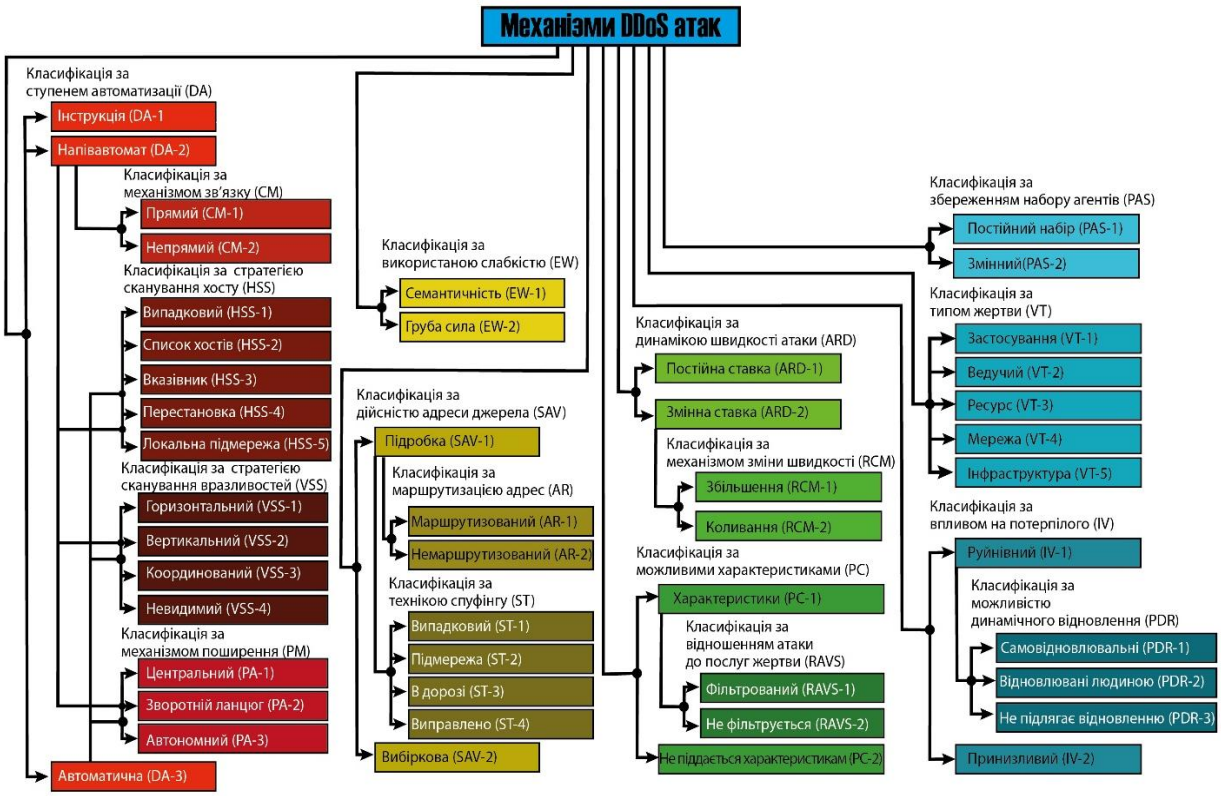


Рис. 1.11. Класифікація DoS-атак, запропонована Дж. Мірковичем

Більш орієнтованою на комплексне та миттєве визначення характеристик атаки є таксономія атак вчені S. Specht і R. Lee DDoS, описана в статті [70] (рис. 1.12.). Вони зосереджуються на тому, як відбувається атака та які слабкі сторони жертви використовуються (пропускна здатність або виснаження ресурсу). Але вони не врахували

додаткові властивості атаки, за винятком типу вразливості, яка використовується для виклику DoS-ефекту.

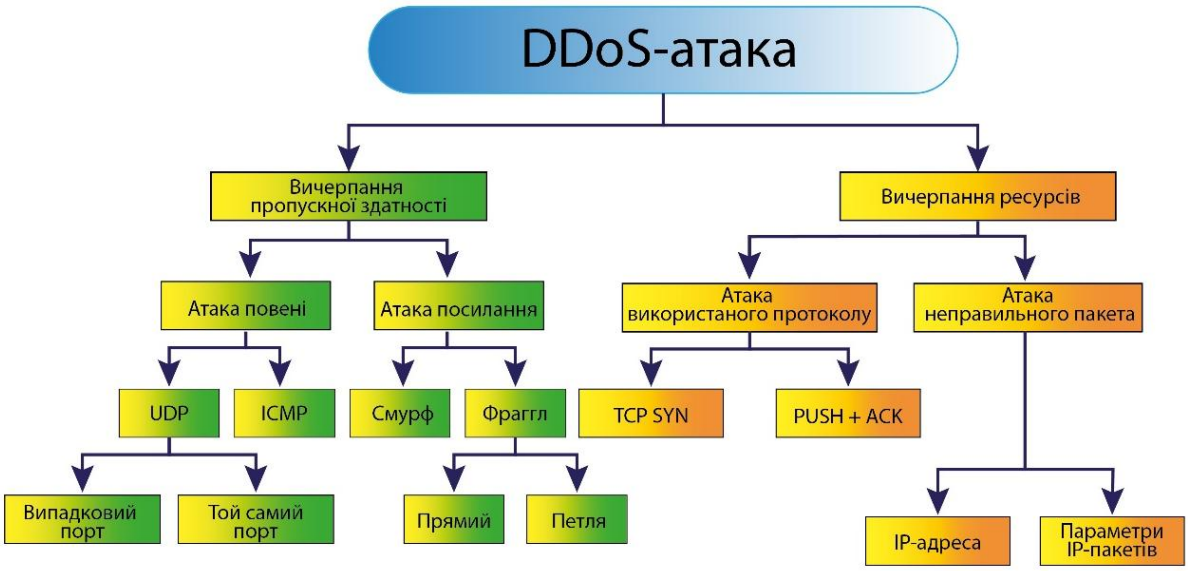


Рис. 1.12. Класифікація DoS-атак, запропонована С. Шпехтом

Усі проаналізовані класифікації DoS-атак мають особливі властивості. Найдокладнішу систематику запропонував вчений Я. Міркович [67].

Класифікація засобів протидії DoS-атакам

Оскільки типи DoS та DDoS є більш неоднорідними, багато різних типів контрзаходів можуть бути застосовані для боротьби з певними типоми DoS. Класифікація існуючих засобів протидії DoS є місцевою, оскільки вона не може чітко визначити механізми захисту та можливості вибору єдиного механізму захисту з усіх можливих методів, які можна застосувати. Вчений Д. Кагір [66] виділяє п’ять груп протидії DoS, які орієнтовані на тип жертви (рис. 1.13.):

- рівень мережевого пристрою;
- рівень ОС;
- рівень програми;
- стандартний рівень протоколу;

- реплікація, і балансування навантаження.

Для підкатегорій цих п'яти груп можна надати більш детальні описи. Однак, надалі в цих групах є дві основні підкатегорії, ітераційне обслуговування та додаткові системи використання, описи, ймовірно, будуть рідкісними.

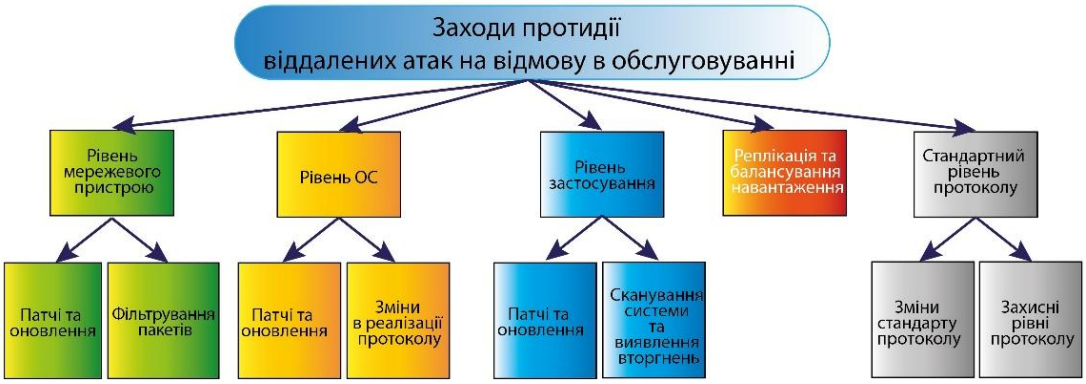


Рис. 1.13. Класифікація протидій DoS-атакам, яку пропонує Д. Кагір

Вчений А. Асоше запропонував класифікацію DDoS-атак, яка також фокусується на типі жертви, але більш детально. По-перше, є наступні категорії, які пропонують можливість фази контрзаходів (1.14) [68]:

- профільна;

- виявлення.

Дані категорії описують типи жертв, а саме цільову та проміжну мережі для обох фаз трафіку та додаткову вихідну мережу для фази виявлення. Кожна із цих підкатегорій розгалужується та надає нам детальну класифікацію.

Ця класифікація не дозволяє належним чином представити багато фаз контрзаходів. Вчений М. Шпехт [70] прагне кращого, він врахував і використовує шість фаз у своїй класифікації (рис. 1.15.):

• виявлення та знешкодження обробників;

• виявлення та попередження вторинних жертв;

• виявлення та попередження деяких атак;

• пом'якшення та припинення нападів;

• відбиття атак;

• післянападна криміналістика.

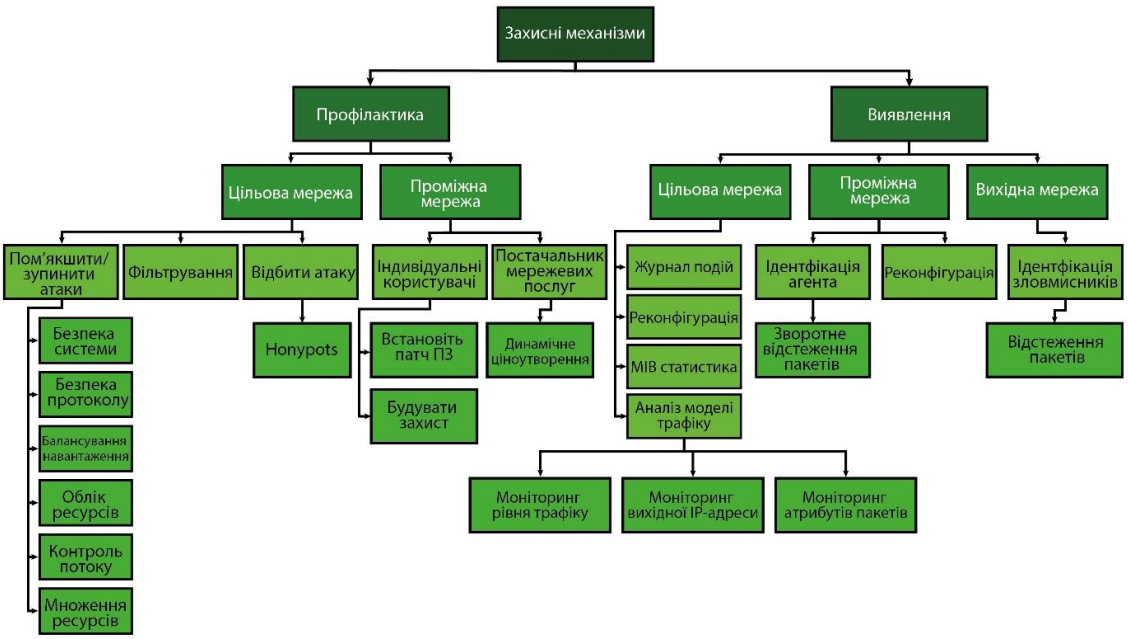


Рис. 1.14. Класифікація протидії DDoS-атак, яку пропонує А. Асоше

Більшість етапів складається з підкатегорій, призначених для більш детального опису заходів протидії DDoS-атакам. Однак ця фаза, як і всі інші зібрані класифікації протидії DDoS, зосереджується тільки на одній характеристиці, протидія DDoS може належати тільки до однієї категорії в цій класифікації.

Рис. 1.15. Вчений М. Шпехт пропонує наступну класифікацію протидії DDoS-атакам,

Критерії класифікації заходів протидії DDoS-атакам проілюстровано на рисунку 1.16 і можуть бути описані таким чином:

- за діяльністю, на якій вони засновані;

- за своїм розташуванням.

Другий спосіб раніше не згадувався, що може використовуватись у протидії низькошвидкісним HTTP DDoS-атакам, тобто в жертви можуть належати посередній чи вихідній мережі.

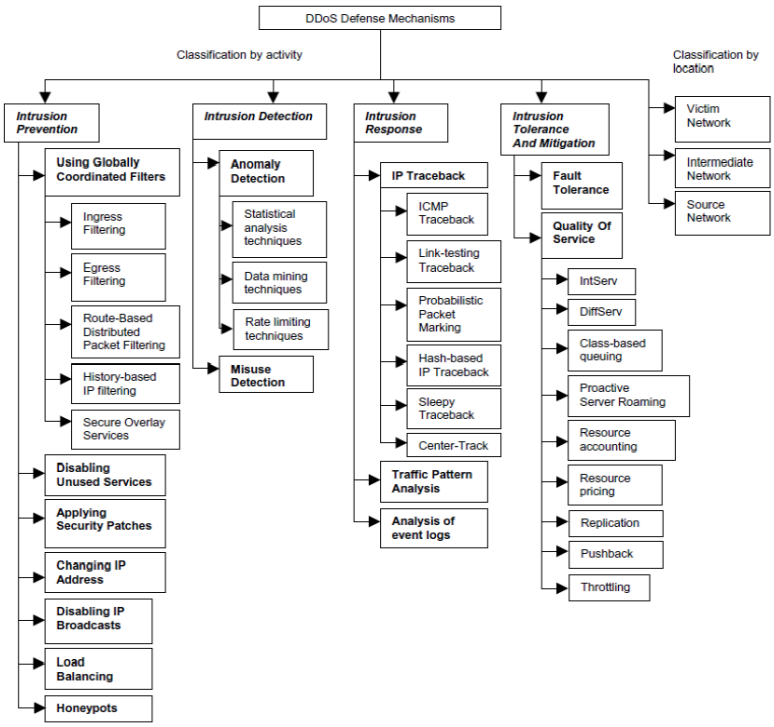


Рис. 1.16. Класифікація засобів протидії DoS-атакам

Вчені Дж. Міркович та А. Фадлаллах пропонують враховувати третій критерій у класифікації заходів протидії DoS, а саме класифікацію на основі ступеня співпраці [40, 67]:

• автономний;

• кооперативний;

• взаємозалежний.

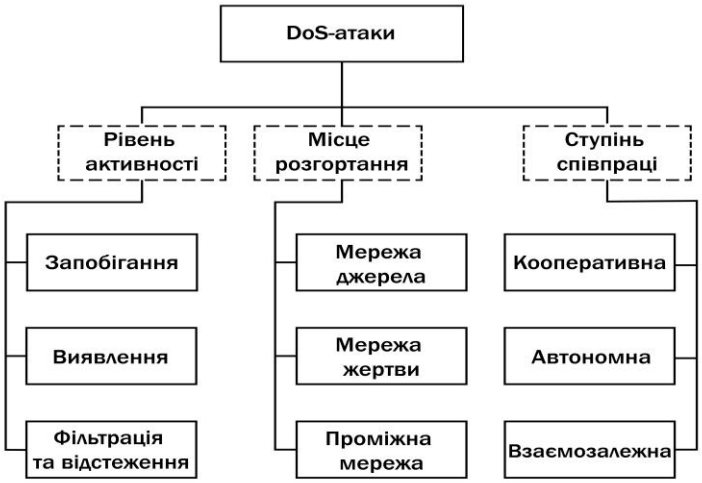


Рис. 1.17. Класифікація засобів протидії DoS-атак, запропонована вченим A. Fadlallah

Основною відмінністю двох класифікацій є різна повнота характеристик та критеріїв сфери застосування. Вчений А. Фадлаллах звертає увагу на декілька підкатегорій для всіх критеріїв. В той час як вчений Я. Міркович має критерії, які починають працювати вже на етапах започаткування DDoS-атак [40, 71].

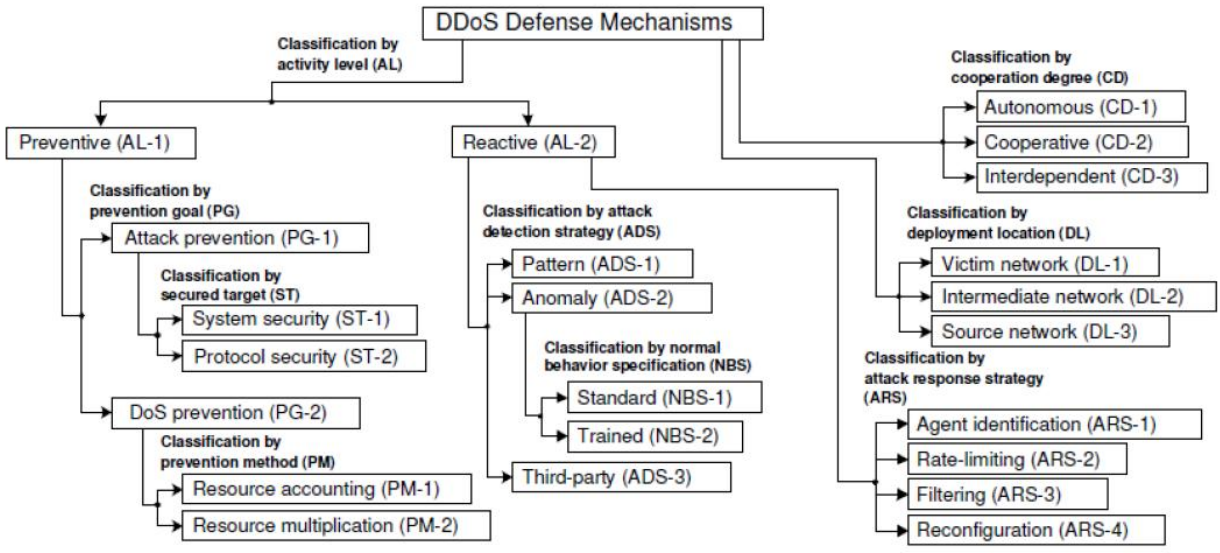


Рис. 1.18 Класифікації протидії DDoS-атакам запропоновані вченим J. Mirkovic

Таксономії DDoS більш сприйнятливі до старіння, як класифікації протидії DoS, оскільки ці властивості атаки мають більш специфічні протидії, тому створені нові ідеї протидії DoS не будуть відображені в поточній класифікації DDoS-атак.

1.3 Дослідження систем протидії низькошвидкісних DDoS-атак.

З постійним розвитком нових енергетичних систем інтелект розподільчих мереж значно покращився, а рівні мережевого та взаємозв'язкового з'єднання пристроїв на стороні користувача значно покращилися. Ґрунтуючись на цьому розвитку мереж, деякі вчені запропонували методи запобігання кібератак з використанням теорій оцінки стану, таких як оцінка стану розподільчої системи (DSSE) [72] та сліпі атаки з введенням хибних даних (FDIA) [73]. Однак, з цими досягненнями, проблеми безпеки мережі стали серйознішими, особливо розподілені атаки типу "відмова в обслуговуванні" (DDoS), які становлять значний ризик для безпечного функціонування розподільчих мереж [74, 127]. DDoS-атаки споживають ресурси цільової системи через велику кількість фальшивих запитів, роблячи її нездатною нормально функціонувати, тим самим впливаючи на стабільність та надійну роботу енергосистеми [75, 76, 77, 78]. Отже, дослідження та розробка ефективних механізмів захисту від низькошвидкісних HTTP DDoS-атак для забезпечення безпеки мережі пристроїв на стороні користувача в розподільчих мережах стали нагальною проблемою, яку необхідно вирішити.

У відповідь на механізми захисту від низькошвидкісних HTTP DDoS-атак у розподільчих мережах було проведено значні дослідження як в академічних колах, так і в промисловості. Серед них методи на основі ентропії відіграють вирішальну роль у виявленні низькошвидкісних HTTP

DDoS-атак. Як правило, методи ентропії виявляють аномальну поведінку, аналізуючи розподіл та зміну мережевого трафіку, тим самим ідентифікуючи та захищаючись від низькошвидкісних HTTP DDoS-атак [79, 80, 81, 82]. Лі та ін. [83] запропонували метод виявлення DDoS-атак на основі φ-ентропії для раннього виявлення низькошвидкісних HTTP DDoS-атак у SDN-мережах. Шляхом налаштування параметрів φ-ентропії цей метод підсилює відмінності між нормальними та аномальними характеристиками трафіку, що полегшує виявлення атак на ранніх стадіях формування низькошвидкісних HTTP DDoS-трафіку. Анчал та ін. [84] використовували ентропію Реньї для виявлення низькошвидкісних HTTP DDoS-атак, підвищуючи точність та ефективність виявлення шляхом вибору відповідних порогів.

Методи, засновані на цінності довіри, також відіграють важливу роль у виявленні низькошвидкісних HTTP DDoS-атак. Ці методи оцінюють поведінку та історію взаємодії вузлів, щоб визначити їхню надійність, тим самим виявляючи та захищаючись від шкідливих атак [85, 86]. Наприклад, вчений Магдіч та ін. [87] запропонували модель управління довірою, яка не тільки ідентифікує довірені вузли, але й застосовує методи машинного навчання для їх виявлення та запобігання шкідливим атакам шляхом вивчення характеристик поведінки шкідливих вузлів. В іншому дослідженні вчений Вафа та ін. [88] запропонували модель управління довірою, яка аналізує поведінку взаємодії вузлів та призначає розумні значення довіри для виявлення атак. Крім того, вчений Хуан та ін. [89] використовували математичні моделі та статистичний аналіз для виявлення аномального трафіку, тоді як вчений Баскар [90] поєднав методи аналізу великих даних для точної ідентифікації та захисту від складних DDoS-атак.

Хоча ці методи продемонстрували відмінну ефективність у виявленні DDoS-атак, вони все ще мають деякі недоліки у вирішенні

сучасних складних типів низькошвидкісних HTTP DDoS-атак [91]. Наприклад, використання фіксованих порогів може бути недостатньо гнучким при роботі з низькошвидкісних HTTP DDoS-атаками, що призводить до зниження ефективності виявлення. Методи, запропоновані в [83, 84], недостатньо точні для атак з низькою щільністю. Аналогічно, методи, описані в [87, 88], не реагують швидко в динамічних мережевих середовищах. Крім того, оскільки методи атак продовжують розвиватися, ці методи потребують постійних оновлень та вдосконалень для адаптації до нових викликів мережевій безпеці.

В останні роки методи глибокого навчання поступово стали новою гарячою точкою для дослідників у галузі DDoS [92, 93, 94, 95, 96]. Крім того, машинне навчання – це метод, здатний автоматично навчати моделі з даних та робити прогнози. Поширені методи машинного навчання включають метод опорних векторів (SVM) [97], метод згорткових рекурентних одиниць (GRU) [98], згорткову нейронну мережу (CNN) [99] тощо. Вчений Чжоу та ін. [100] поєднали методи машинного навчання та аналітику великих даних для вирішення проблем моніторингу мережевого трафіку та виявлення DDoS, досягнувши чудових результатів. Вчений Елсьєр та ін. [101] використали ансамблевий класифікатор під назвою V-NKDE для точного виявлення та пом'якшення DDoS-атак в SDN. У застосуванні машинного навчання CNN набуває все більшої популярності в галузі виявлення DDoS завдяки своїм чудовим можливостям вилучення ознак [102, 103, 119]. Вчений Ченг та ін. [104] запропонували метод виявлення CNN на основі ознак сірої матриці мережевого потоку. Цей метод покращує точність сегментації ознак шляхом вилучення глобальних та локальних ознак за допомогою ядер згортки різних просторових масштабів.

Експерименти показують, що цей метод підвищує стійкість класифікатора, зменшує рівень хибних тривог та пропущених тривог, а

також ефективно виявляє DDoS-атаки в середовищі великих даних. Вчений Харіш [105] запропонував гібридну глибоку модель CNN-RF для виявлення низькошвидкісних HTTP DDoS-атак. Цей метод вирішує проблему точної ідентифікації низькошвидкісних HTTP DDoS-атак, і запропонована модель чудово працює в сценаріях виявлення в режимі реального часу, значно покращуючи рівень виявлення та зменшуючи рівень хибних тривог.

Підсумовуючи, існуючі механізми захисту від низькошвидкісних HTTP DDoS-атак повинні постійно вдосконалюватися та оптимізуватися у відповідь на дедалі складніші мережеві середовища та методи атак, щоб підвищити мережеву безпеку пристроїв на стороні користувача в мережах розподілу електроенергії. На основі вищезазначеного дослідження пропонується новий механізм захисту від DDoS-атак для забезпечення безпечної роботи пристроїв на стороні користувача в мережах розподілу електроенергії. Основний внесок цього дослідження полягає в наступному:

По-перше, у даній роботі проводиться аналіз безпеки низькошвидкісних HTTP DDoS-атак.

По-друге, враховуючи прогресивний характер обчислень, розроблено трирівневу архітектуру захисту від поверхневого до глибокого шару, що ефективно запобігає втраті ресурсів під час виявлення низькошвидкісних HTTP DDoS-атак.

По-третє, у цій статті використовується ентропія вчених Реньї для виявлення низькошвидкісних HTTP DDoS-атак. Цей крок удосконалено для низькошвидкісних HTTP DDoS-атак, і в поєднанні з класифікатором випадкового лісу він ефективно виявляє потенційну поведінку низькошвидкісних HTTP DDoS у трафіку, що проходить через комутатори.

У цій роботі пропонується новий механізм захисту від низькошвидкісних HTTP DDoS-атак, заснований на архітектурі SDN, який значно покращує точність та швидкість реагування виявлення

низькошвидкісних HTTP DDoS-атак завдяки багаторівневому виявленню та фільтрації. В аналізі результатів ентропії вченого Реньї, зі збільшенням інтенсивності низькошвидкісних HTTP DdoS-атак (від 1% до 20%) всі метрики (Acc, Pre, Rec, F1) демонструють стабільне покращення. Особливо під час низькошвидкісних HTTP DDoS-атак помірної інтенсивності метод ентропії вченого Реньї демонструє високу стійкість. Модель OneDCNN працює надзвичайно добре при інтенсивності одного інтервалу, демонструючи надзвичайно високу продуктивність виявлення з точки зору точності, прецизійності, повноти та F1-оцінки, що доводить її здатність до узагальнення та стабільність у матрицях трафіку. При інтенсивності низькошвидкісних HTTP DDoS 10% та 6% запропонований метод демонструє значні переваги в точності та стабільності виявлення, особливо порівняно з традиційними методами, що відображає вищу точність виявлення. Підсумовуючи, трирівнева архітектура захисту, розроблена в роботі, завдяки поступово зростаючому режиму обчислень ефективно уникає марнування обчислювальних ресурсів, особливо під час виявлення низькошвидкісних HTTP DDoS-атак, тим самим значно підвищуючи ефективність виявлення. Запропонований метод чудово справляється з DDoS-атаками різної інтенсивності, забезпечуючи надійну гарантію безпечної роботи пристроїв користувача розподільчої мережі.

Аналіз DDoS-захисних систем

В ході дослідження було порівняно шість відомих систем захисту від DDoS-атак, порівняння визначались за наступними особливостями:

- швидкодія (<10 сек.);
- вбудований модуль ШІ;
- пропускна здатність > 5 Тб/с;
- методи фільтрації L3/L4;
- методи фільтрації L7;
- автоматичне масштабування;

- хмарне розгортання;

- локальне розгортання;

- глибока інтеграція з іншими системами;

- доступність для малого бізнесу.

Дані були зібрані в таблицю 1.2, де позначення: «+» означає наявність характеристики, «-» її відсутність або обмежену підтримку.

Таблиця 1.2

Аналіз DDoS-захисних систем

Система	Швидкодія (<10 сек.)	Вбудований модуль ШІ	Пропускна здатність > 5 Тбіт/с	Методи фільтрації L3/L4	Методи фільтрації L7	Автоматичне масштабування	Хмарне розгортання	Локальне розгортання	Глибока інтеграція з іншими сервісами	Доступність для малого бізнесу
AntiDDoS	+	+	+	-	+	+	+	-	+	+
Національний центр резервування	+	-	+	+	+	-	-	+	+	-
Radware DefensePro	+	+	+	+	+	-	-	+	+	-
UA-Shield (українська розробка)	+ (залежить від конфігурації)	-	+ (спеціалізовані рішення)	+	-	-	-	+	-	-
Akamai Kona Site Defender	+	+	+	-	+	-	+	-	+	-
Cloudflare Basi Protection	+	-	+	+	-	частково	+	-	+	+

Дане порівняння показало, що Національний центр резервування є найкращим вибором для захисту від низькошвидкісних HTTP DDoS-атак з кількох причин:

- підтримка ключових характеристик для низькошвидкісних атак: Він забезпечує захист на рівнях L3/L4 та L7, включаючи повні POST-запити та боти, що є критичним для таких атак;

- локальне розгортання та інтеграція, що підходить для організацій, які потребують місцевого рішення з глибокою інтеграцією, наприклад, державних установ.

- обмеження, відсутність автоматичного масштабування та хмарного розгортання може бути недоліком у динамічних умовах, але для низькошвидкісних нападів менш критично.

А система AntiDDoS (наприклад, від Київстар) є сильним конкурентом через хмарне розгортання, автоматичному масштабуванню та доступності для малого бізнесу. Однак він не підтримує фільтрацію L3/L4, що може обмежити його ефективність у комплексних атаках.

Інші системи ефективні для базового захисту від атак на рівні мережі (L3/L4), але не забезпечують повноцінного захисту від низькошвидкісних L7-атак.

Національний центр резервування є найкращим вибором для протидії низькошвидкісним HTTP DDoS-атакам завдяки підтримці фільтрації L3/L4 і L7, захисту від вільних POST-запитів і ботів, а також наявності ШІ та локального розгортання. Для малого бізнесу AntiDDoS може бути кращим через доступність і хмарне розгортання, але він діє в комплексності захисту.

Висновки до розділу 1

1. На відміну від звичайних високошвидкісних атак, які, як правило, створюють інтенсивний мережевий трафік, низькошвидкісні HTTP DDoS-атаки представляють невелику кількість запитів, імітуючи законну поведінку користувача. Їх метою є, остаточно використати всю доступну

вихідну потужність сервера або заблокувати будь-яку життєво важливу службу. За таких параметрів звичайні системи з високою інтенсивністю трафіку на основі аномалій не дозволяють їх визначити, а отже, пропускають атаку через недопрацювання захисту даних систем.

2. Відомі на даний момент методології боротьби з низькошвидкісними HTTP DDoS-атаками здебільшого ігнорують той факт, що такі атаки мають низьку інтенсивність і вимагають колосальних витрат ресурсів. Для того щоб впоратися з великим мережевим потоком. Механізми виявлення, які не реагують або надто обтяжливі, призводять до зниження ефективності захисту. Особливо це можна помітити в зонах інтенсивного використання, таких як електронна комерція, банківські послуги або хмарні платформи. У першому розділі розглядаються основні класифікації DoS- і DDoS-атак, а також класифікація цілей-жертв, атакованих за допомогою цих методологій. Розглянуті механізми DDoS-атаки дають можливість зрозуміти, яким чином можуть працювати зловмисники. За допомогою цих даних можна побудувати правильний захист від низькошвидкісних DDoS-атак. Розглянуті контрзаходи дають зрозуміння, як будувався захист вченими, які розглянуті, і на основі їхньої діяльності побудувати власну систему захисту.

3. Оцінка відомих методів захисту веб-ресурсів від низькошвидкісних HTTP DDOS-атак. Була проведена за основними критеріями: швидкість, вбудований AI-модуль і пропускна здатність >5 Тбіт/с; разом із методами фільтрації L3/L4/L7, автоматичного масштабування та хмарного розгалуження тощо. Виявлено недосконаліть існуючих методів боротьби з низькошвидкісними HTTP DDOS-атаками.

РОЗДІЛ 2.

МЕТОД, МОДЕЛЬ ТА СИСТЕМА ПРОТИДІЇ НИЗЬКОШВИДКІСНИМ HTTP DDOS-АТАКАМ НА ВЕБ-РЕСУРСИ

2.1. Розробка моделі упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача

Опис моделей упередження низькошвидкісних HTTP DDoS атак.

Модель означає «систематичний опис об’єкта або явища, який має спільні важливі характеристики з об’єктом або явищем. Використовуючи моделі, ми можемо легше зрозуміти аналізований об'єкт, розглядаючи його в різних ситуаціях і параметрах [106].

При моделюванні комп’ютерної мережі слід враховувати два основних компоненти. Система має обробити системні дані та вхідний трафік.

Розробка основних компонентів запропонованої моделі.

Thomas M. Chen стверджує, що комунікаційну систему можна розглядати, зосереджуючись на різних рівнях: зв’язок, пакет, стільниковий або пакетний зв’язок. Він демонструє різні погляди на процес комп'ютерної комунікації. На рівні сеансу важливий лише загальний час підключення, а не дані про трафік. У той же час аналіз на рівні пакетів охоплює всі пакети, надіслані/отримані протягом певного часу. Проте вчений Pearson, M. та Cleary, J. виділяють більш детальні рівні моделювання трафіку [107, 108, 112, 114, 115, 132] (див. рис. 2.1.).

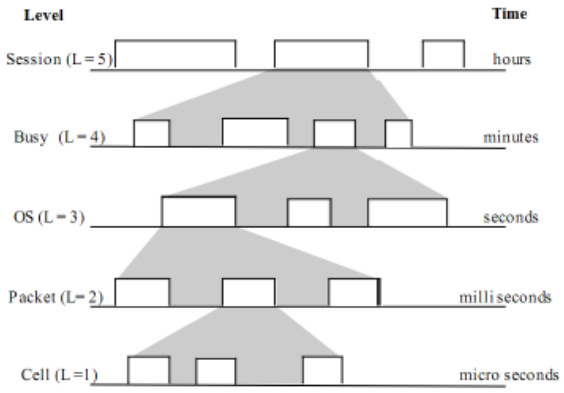


Рис. 2.1. Рівні моделювання руху

Найвищий рівень абстракції залишається рівнем сеансу, і кожен сеанс може складатися з багатьох пакетів, які в цій класифікації називаються періодами зайнятості. Порівнюючи із запропонованими рівнями Томаса М. Чена, M. Pearson пропонує брати до уваги рівень ОС (операційної системи), який представлятиме діяльність операційної системи. У кожному пакеті рівня ОС слід обробити кілька пакетів PCT/IP, які у випадку, коли робоча станція підключена до мережі ATM, створять пакет комірок ATM, не згаданих у класифікації T. M. Chen [109, 110, 113].

Залежно від рівня моделювання трафіку, необхідний інший рівень специфікації, а також відповідно до моделі трафіку.

Більш детальні моделі були запропоновані вчений Q. Huang. Цей автор в статті «Аналіз нової форми розподіленої атаки на відмову в обслуговуванні» описує дві моделі для різних типів DDoS-атак. Одна модель представляє TCP SYN-атаку, а інша – DDoS-атаку на виснаження пропускної здатності. Для моделі атаки TCP SYN була запропонована модель втрати Engset (G/G/N – як час прибуття, так і час обслуговування, як правило, розподілено, черга може обслуговувати N запитів і зберігати нескінченну кількість запитів користувачів). Ця модель дозволяє визначити ймовірність втрати пакетів, і її можна використовувати як вимірювання успіху DDoS-атаки.

Для моделі атаки на виснаження пропускної здатності вчений Q. Huang використову’ рідинну модель статистичного мультиплексування трафіку атак від n агентів, які чергуються між пакетним (увімкненим) станом і безмовним (вимкненим) станом. Тому запропоновану формулу можна застосувати як для постійної, так і для змінної швидкості трафіку атаки одного агента та представити приблизну кількість агентів, необхідну для вичерпання пропускної здатності жертви [138].

Вчений Q. Huang також запропонував та модифікував модель атаки TCP SYN для бездротових мереж. Ця модель розрізняє законні та атакуючі

запити, тому використовує узагальнену багатокласову модель змішаних втрат Erlang та Engset. Для законного трафіку надходження представлено як процес Пуассона, тоді як трафік атаки надходить відповідно до моделі кінцевого джерела. Ця модифікація вимагає, щоб кількість агентів атак була достатньо великою, однак забезпечує більш реалістичне представлення ситуації DDoS-атаки з вичерпанням ресурсів.

Згадані моделі DoS-атак із вичерпанням математичних ресурсів використовували загальний розподіл частоти надходження запитів. Вчений Q. Huang у моделі для бездротових мереж використано процес Пуассона для представлення законних запитів користувачів. Інші автори також пропонують використовувати експоненціальний розподіл частоти надходження для представлення трафіку атаки [129, 130, 139].

Вчені С. Хан та І. Траор пропонують представити час між прибуттями та час обслуговування, щоб також мати експоненціальний розподіл під час атаки. Запропонована модель зосереджена на виснаженні процесора, і тому використовує модель M/M/1/N, щоб показати, що лише один запит може обслуговуватися в один момент часу, тоді як N запитів можуть зберігатися в буфері. Використовуючи цю модель, автори представляють бажану ситуацію та за допомогою чисельних методів отримують показники швидкості зростання черги та часу відповіді. Ці показники можна використовувати як індикатор для виявлення атак, тому їх можна отримати шляхом чисельних розрахунків, але не моделювання, виконання якого вимагає більше часу [140].

Вчений А. Айсані пропонує модель атаки TCP SYN і розрізняє легітимний і атакуючий трафіки. Однак він також використовує експоненціальний розподіл (процес Пуассона) для представлення швидкості надходження як законного, так і атакуючого трафіку в цій моделі. Розділення легального трафіку та трафіку атаки дозволяє більш реалістично представити модель і представляє формули для ймовірності

втрати з’єднання та відсотка заповнення буфера напіввідкритими з’єднаннями як для звичайного, так і для атакуючого трафіку. Таким чином, ці показники можна використовувати для виявлення атак DoS, а також для моделювання та аналізу успіху атак TCP SYN [141].

Намагаючись відмовити в обслуговуванні протягом тривалого часу, оптимізація атаки стає більш важливою. Тому зловмисники DoS намагаються обчислити оптимальний трафік атаки та вибрати конкретний шаблон надсилання пакету атаки. Така DoS-атака називається низько-швидкісною, і для її моделювання потрібні додаткові характеристики атаки, що описують обраний шаблон. G. Macia-Fernandez та ін. пропонує модель, яка дозволяє зрозуміти динаміку такого роду атак. Тому вони не можуть використовувати простий процес надходження та враховувати пакетні характеристики вхідного трафіку. Відповідно час можна розрахувати за допомогою формул, представлених у цьому документі. Однак автори не були задоволені цією моделлю через нерозглянутий випадок ітераційних серверів із суперпозицією між функціями ймовірності появи або їх функціонування як паралельної системи. Тому вони розширили цю модель до нової, де ці проблеми вирішено та запропоновано нові формули для доступності сервера, ймовірності успіху клієнта та накладних витрат трафіку [123, 142, 143].

Однак іноді низька швидкість DoS-атаки може супроводжуватися випадковими збоями. Тому вчений N. Chaturvedi та ін. використовують чергування між активним і стабільним станами низьких спалахів DDoS-атак як стохастичний процес. Оскільки тривалість сплеску DDoS є випадковою, отже, задовольняє марковську властивість безпам’яті, вищезгаданий умовний розподіл ймовірностей представлений як експоненціальний [144].

Усі згадані математичні моделі атак DoS представляють атаку DoS на вищому рівні агрегації, але перехід між конкретними станами запиту.

Однак існують математичні моделі, які аналізують DoS-атаку в більш загальному вигляді за допомогою ланцюгів Маркова. Одним із прикладів є запропонована Y. Wang та інші модель DoS-атаки, де використовується двовимірний вбудований ланцюг Маркова. Він представляє атаку TCP SYN за допомогою двовимірного ланцюга Маркова. Двовимірний ланцюг Маркова використовується через два різних вхідних трафіки (атакувальний і звичайний) і дозволяє знайти стаціонарний розподіл ймовірностей, який використовується для отримання аналітичних результатів для кількох показників продуктивності безпеки. А також ймовірність втрати з'єднання, відсоток зайнятості буфера напіввідкритими з'єднаннями для обох звичайний і атакуючий трафіків [53, 71].

Модель упередження низькошвидкісних HTTP DDoS-атак з використанням ШІ.

Україна, будучи на передовій кібервійни з Росією, стала полігоном для тестування інноваційних методів протидії DDoS-атакам, зокрема низькошвидкісним HTTP-атакам, які характеризуються тривалим та "непомітним" впливом на веб-ресурси. Ці атаки спрямовані на виведення систем з ладу через поступове перевантаження серверів, що ускладнює їхнє виявлення традиційними засобами. У роботі аналізуються стратегії, технології та інституційні механізми, розроблені українськими установами та міжнародними партнерами для протидії цим загрозам.

З початком повномасштабної війни в 2022 році Україна стикнулася з безпрецедентною кількістю кібератак, зокрема DDoS. За даними Держспецзв'язку, з лютого 2022 року зафіксовано понад 2000 атак на державні та критичні інфраструктури, включаючи енергетику, фінанси та медіа. Низькошвидкісні HTTP DDoS-атаки, на відміну від класичних об'ємних, діють непомітно, імітуючи легальний трафік, що ускладнює їх ідентифікацію. Наприклад, у 2023 році кіберзлочинці атакували сайти

Міністерства аграрної політики та «Нафтогазу», використовуючи комбінацію фішингу та DDoS.

Держспецзв’язок впровадив систему захисту на базі рішень Radware та Akamai Technologies, яка включає очищення трафіку, аналіз шаблонів атак та автоматичне блокування підозрілих запитів. Ця система інтегрована в Державний центр кіберзахисту, що дозволяє масштабувати захист на 170 державних ресурсів.

Національний центр резервування пропонує DDoS Protection as a Service, де захист реалізується на трьох рівнях: хмарному, мережевому та гібридному. Використання IDS/IPS (систем виявлення вторгнень) дозволяє ідентифікувати низькошвидкісні атаки через сигнатурний та поведінковий аналіз.

Міжнародна співпраця

Проєкт USAID «Кібербезпека критичної інфраструктури» підтримав створення Центру очищення трафіку, який фільтрує до 70% шкідливого контенту. Технології машинного навчання, розгорнуті в партнерстві з RETN, автоматизують виявлення аномалій у трафіку, зокрема "повільних" HTTP-запитів.

Центр демократії та верховенства права (ЦЕДЕМ) провів аналіз кібератак за період 2022–2024 років, виявивши кореляцію між DDoS-атаками та дезінформаційними кампаніями. Дослідження підкреслює необхідність комбінації технічних (наприклад, водяні знаки для відстеження контенту) та інформаційних заходів.

Інститут дослідження кібервійни розробив рекомендації для РНБО, акцентуючись на покращенні координації між державним і приватним секторами. Їхній звіт за 2023 рік зазначає, що 40% атак на медіа були низькоінтенсивними, що вимагає адаптації існуючих систем моніторингу.

Технології протидії низькошвидкісним DDoS. RETN у своєму скрабінг-центрі в Києві використовує AI для аналізу трафіку в реальному

часі. Система розпізнає паттерни низькошвидкісних атак через аналіз тривалості сесій, частоту запитів та геолокацію джерел.

Сервіси Sandbox as a Service (Національний центр резервування) ізолюють підозрілий трафік для глибинного аналізу, що критично для виявлення "маскованих" HTTP-атак.

Багаторівневий захист. Хмарні рішення (наприклад, Akamai) забезпечують фільтрацію трафіку до його надходження на сервер, знижуючи навантаження на локальні мережі.

Гібридні системи поєднують локальні фаєрволи з хмарними сервісами, що дозволяє блокувати атаки на рівні додатків (L7), де часто діють низькошвидкісні DDoS.

Рекомендації для веб-ресурсів

Регулярний аудит CMS та плагінів для усунення вразливостей.

Використання протоколів HTTP/3 із вбудованим шифруванням для ускладнення аналізу трафіку зловмисниками.

Інтеграція з SOC (операційними центрами безпеки), як у RETN, для цілодобового моніторингу.

Україна розробила комплексну систему протидії DDoS-атакам, що включає державні, міжнародні та академічні ресурси. Для боротьби з низькошвидкісними HTTP-атаками ключовим є поєднання AI-аналітики, багаторівневого захисту та міжнародної координації. Досвід України демонструє, що ефективний кіберзахист вимагає не лише технічних інновацій, але й інституційної стійкості та громадської обізнаності.

Врахувавши досвід попередників та узагальнивши інформацію, яка описана вище, я вирішив створити власну модель раннього виявлення низькошвидкісних HTTP DDoS- атак.

Для створення системи реалізації серверів захисту я пропоную модель раннього виявлення, яка має наступні функції. На малюнку 2.2. показано процес виявлення, розбитий на два основних етапи:

• Етап 1 виконує попередню обробку та збирає даний мережевий трафік за допомогою методу часового вікна. Звичайна атака займає 2 секунди та збирає дані один раз; повна атака займає 5 секунд часового вікна, та також збирає дані один раз;

• Етап 2 виконує симуляцію навчання штучного інтелекту з виявленням аномалій у реальному часі та сповіщення про онлайн-дані (рис. 2.2.).

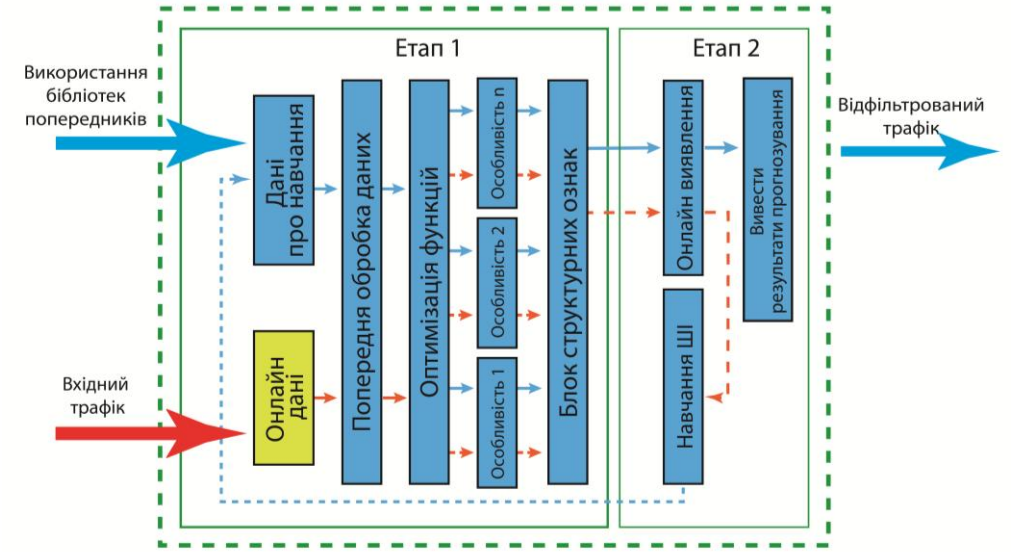


Рис. 2.2. Модель виявлення аномалій

Ця модель реалізовується наступним чином, за допомогою зготкової моделі ШІ, яка навчається виконується раннє виявлення низькошвидкісних HTTP DDoS-атак. Виконується це в два етапи:

етап 1 включає в себе наступні кроки:

- попередня обробка даних (порівняння вхідного трафіку з даними про навчання/використовуючи бібліотеки сигнантур даних інцидентів, які були раніше), бібліотеки даних беремо [145], та інші.

- до бібліотек даних додаємо особливості, в даному випадку ми обрали 3 особливості:

- наявність пустих пакетів;

- час тривалості запиту;

- регіон з якого здійснюється запит.

Розглянемо детальніше кожну особливість. Особливість №1 «Наявність пустих пакетів». Пусті пакети (наприклад, HTTP-запити без корисного навантаження або заголовків) рідко зустрічаються в легальному трафіку, оскільки користувачі зазвичай взаємодіють із сервісами через повноцінні запити (наприклад, завантаження сторінок, відправка форм). Однак для низькошвидкісних DDoS-атак пусті пакети є типовими:

- маніпуляція ресурсами сервера, атакуючі можуть надсилати тисячі неповних або порожніх запитів, змушуючи сервер витрачати ресурси на їх обробку та підтримку відкритих з'єднань;

- уникнення детекції, такі пакети не викликають різкого зростання трафіку, але їхня аномальна структура (наприклад, відсутність параметрів User-Agent або Referer) дозволяє відрізнити їх від легітимних запитів;

- тестування слабких місць, пусті запити часто використовуються для зондування сервера перед масштабною атакою;

Для виявлення пустих пакетів було використано наступні обчислення, які виконувались за допомогою формули 2.1.:

$$P\left(x_1\left(t\right)=k\right)=\frac{\left(\lambda\Delta t\right)^k e^{-\lambda\Delta t}}{k!}, k\in \mathrm{N} \tag{2.1}$$

Де:

P - наявність пустихпакетів;

$x_1(t)$ - кількість пустих пакетів;

Δt - часове вікно, можна моделювати як Пуассонівський процес з інтенсивністю λ;

e - основа натурального логарифму (\(e\прибл. 2,718\);

$k!$ - факторіал числа k;

k - є дискретною змінною ($k\in \mathrm{N}$, включаючи \(0\).

Особливість №2 «Час тривалості запиту»

Низькошвидкісні атаки орієнтовані на довготривалу експлуатацію з'єднань, що призводить до блокування доступу для інших користувачів. Аналіз часу тривалості запитів дозволяє виявити такі аномалії:

- Slowloris-атаки, зловмисники навмисно підтримують тисячі відкритих з’єднань, надсилаючи дані фрагментарно або затримуючи відповіді. Це призводить до того, що середній час обслуговування запитів сервером різко зростає;

- викривлення паттернів поведінки, легітимні користувачі рідко залишають з’єднання відкритими на тривалий час (наприклад, більше 60 секунд для звичайного HTTP-запиту). Атака ж може тривати годинами, що створює статистично значимі відхилення;

- аналіз таймаутів, сервери мають обмеження на час очікування даних. Якщо багато з’єднань перевищують цей ліміт, це може бути ознакою атаки;

Для виявлення тривалості запиту було використано наступні обчислення, які виконувались за допомогою формули 2.2.:

$$f\left(x_2\right)=\beta e^{-\beta x_2}, \quad x_2 \geq 0 \tag{2.2}$$

Де:

β - параметр швидкості;

x_2 - час обробки запиту;

Нормалізація часу тривалості запиту визначалась за наступною формулою 2.3.:

$$\tilde{x}_2=\frac{x_2-\mu}{\sigma} \tag{2.3}$$

де:

$\tilde{x}_2$ - нормалізована тривалість запиту;

μ - середнє значення;

σ - стандартне відхилення.

Особливість №3 «Кодування регіону»

Географічний аналіз джерел трафіку дозволяє виявити підозрілу активність, яка не відповідає звичній поведінці аудиторії сервісу:

- ботнети та проксі, низькошвидкісні атаки часто організовуються через ботнети, розподілені в конкретних регіонах (наприклад, країнах зі слабким рівнем кібербезпеки) [137]. Різкий сплеск запитів із таких регіонів є сигналом для подальшого розслідування;

- штучний інтелект (ШІ) та геофільтрація, легальні користувачі зазвичай зосереджені в певних регіонах. Наприклад, локальний сервіс для України раптово отримує тисячі запитів із Південно-Східної Азії — це явний індикатор атаки;

- обхід обмежень, зловмисники можуть використовувати VPN або TOR для приховування IP, але геолокація дозволяє виявити аномалії в розподілі трафіку (наприклад, 90% запитів від одного регіону при звичайному розподілі 5%).

Кодування регіону будемо знаходити за наступною формулою 2.4.:

$$x_{3,i} = \begin{cases} 1, якщо\ запит\ з\ регіону\ i, \\ 0, інакше. \end{cases} \quad (2.4)$$

де:

$x_{3,i}$ – *бінарний індикатор приналежності до регіону* i;

$i \in \{1, 2, \ldots, m\}$, *де* m – *кількість регіонів*

Для визначення зваженнь функцій втрат було використано наступну формулу 2.5.:

$$L = \frac{1}{N}\sum_{i=1}^{N} w_i \bullet \left(y_i - \hat{y}_i\right)^2, \text{ де } w_i = 1 + \alpha x_1 \quad (2.5)$$

де:

w_i - вага для i-го прикладу;

α - гіперпараметр, що регулює вплив пустих пакетів (\(\alpha\geq 0\);

$x_{1,i}$ - кількість пустих пакетів для i - го запиту.

Для визначення умовної ймовірності для регіонального впливу було використано наступну формулу 2.6:

$$P(y=1|x_3)=\frac{e^{W\cdot x_3}}{1+e^{W\cdot x_3}},\ де\ W\in\mathbb{R}^m \tag{2.6}$$

де:

$W=\left[w_1, w_2, \ldots, w_m\right]$ - вектор ваг, що відображають вплив кожного регіону;

x_3 - вектор регіону;

$y\in\{0,1\}$ - бінарна цільова змінна.

Об’єднана формула з урахуванням трьох особливостей

Нехай:

x_1 - кількість пустих пакетів у часовому вікні Δt;

x_2 - час тривалості запиту;

x_3 - категоріальна змінна регіону;

ϕ_1, ϕ_2, ϕ_3 - функції попередньої обробки для кожної особливості.

Попередня обробка даних, визначається за виразом 2.7:

$$X_{processed}=\left[\phi_1(x_1), \phi_2(x_2), \phi_3(x_3)\right] \tag{2.7}$$

де:

$\phi_1(x_1)=\frac{x_1}{\max(x_1)}$ - нормалізація кількості пустих пакетів;

$\phi_2(x_2)=\frac{x_2-\mu}{\sigma}$ - стандартизація часу тривалості, μ - середнє, σ - стандартне відхилення;

$\phi_3(x_3)$ - кодування регіону (\(\mathbf{x}_3\in\{0,1\}^m\).

Інтеграція в модель ШІ:

$H^{(0)}=X_{processed}$ - вхідний тензор розширений до форми, придатної для згортки

Згортковий шар представлено виразом 2.8:

$$H^{(l)} = \sigma(K^l * H^{l-1} + b^l) \tag{2.8}$$

де:

$K^{(l)}$ - ядро згортки;

$H^{(l)}$ - зміщення;

σ - функція активації (наприклад, Relu/резюме).

Виведення прогнозу:

\hat{y}=\text{softmax}\left(\mathbf{W}_{\text{out}}\cdot\mathbf{H}^{(L)}+\mathbf{b}_{\text{out}}\right)

де:

$H^{(L)}$ - вихід останнього шару ШІ;

(\mathbf{W}_{\text{out}}_\mathbf{b}_{\text{out}}} - ваги та зміщення класифікатора

Функція втрат з урахуванням особливостей будемо вираховувати за формулою 2.9.:

$$L = -\sum_{i=1}^{N}(y_i \log y_i + (1-y_i)\log(1-\hat{y}_i)) + \lambda(\alpha x_1 + \beta\|x_2\|^2 + \gamma\|x_3\|^2) \tag{2.9}$$

де:

λ - коефіцієнт регуляризації;

α, β, γ - ваги для кожного типу особливостей.

Етап 2

На етапі 2 виконується співставлення та виявлення низькошвидкісних HTTP DDoS-атак, дані які не відповідають особливостям даної моделі передаються для навчання моделі ШІ після чого передаються до блоку даних про навчання, та будуть використані при наступній попередній обробці даних наступного при новому вхідному трафіку.

Синергія особливостей для підвищення точності при навчанні ШІ для запобігання низькошвидкісним HTTP DDoS-атакам дає можливість значно покращити рівень кібербезпеки та захищеності в цілому.

Окремі ознаки можуть давати хибно-позитивні результати (наприклад, пусті пакети іноді генеруються через помилки в клієнтських додатках, а тривалі запити — через повільні мережі користувачів). Однак комбінація трьох параметрів значно підвищує точність:

- пусті пакети + тривалі з’єднання + трафік із незвичних регіонів = раннє виявлення HTTP DDoS-атак.

- машинне навчання допомагає виявити складні кореляції між цими ознаками, що неможливо зробити за допомогою простих правил.

Таким чином, ці три особливості формують базис для розпізнавання низькошвидкісних атак, які імітують легальний трафік, але мають критичні відмінності в структурі, часових параметрах та географії. Їх використання дозволяє запобігти витонченому "тихому" виведенню сервера з ладу, зберігаючи доступність сервісу для справжніх користувачів.

Алгоритм фільтрації трафіку

Коли контролер отримує невідомий пакет через протокол OpenFlow, пакет містить повну інформацію. Після отримання пакета контролер аналізує інкапсуляцію пакета та аналізує пакет шар за шаром. Таким чином, на основі вилученої інформації може бути створена таблиця потоку для пакета. Після чого вихідний пакет передається на плату комутатора через протокол OpenFlow, а плата комутатора містить інтерфейс для пересилання. На основі цього принципу плата комутатора обробляє надісланий пакет даних, витягує необхідну інформацію та передає її навченій моделі для розпізнавання та прогнозування. На рис. 2.3 показано алгоритм фільтрації трафіку.

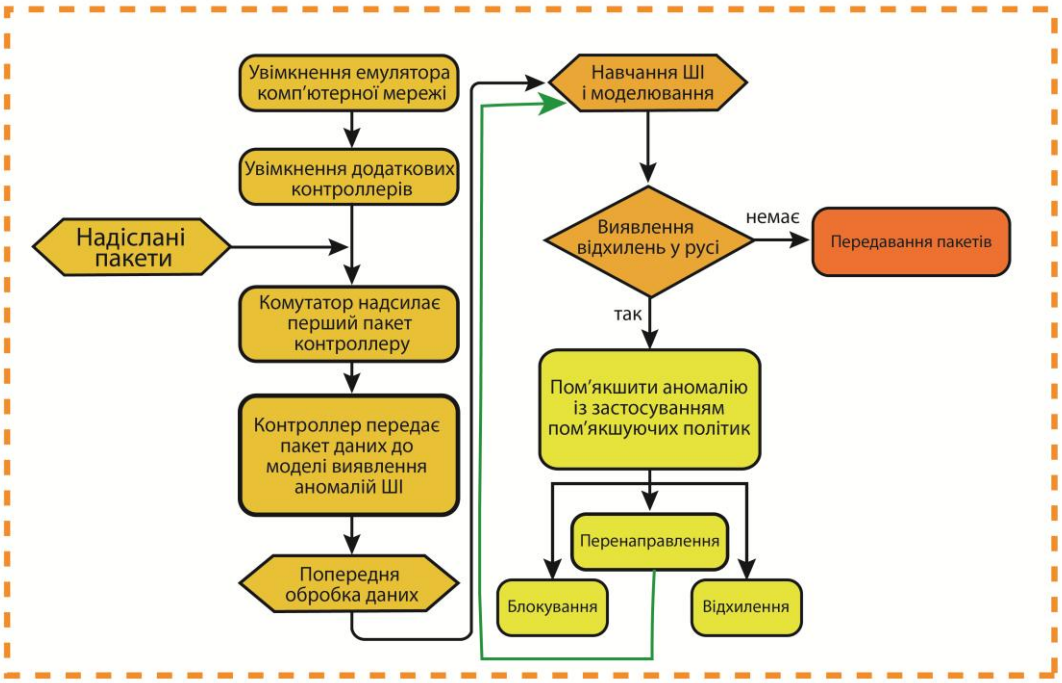


Рис. 2.3. Алгоритм фільтрації трафіку

Виконавши запуск симулятора комп'ютерної мережі та виконавши надсилання пробного пакету даних. В даному випадку комутатор використовувався для пересилання першого пакета даних до контролера. Контролер пересилає цей пакет даних до моделі виявлення аномалій штучного інтилекту. Після попередньої обробки використовуються дані про навчання штучного інтелекту та моделювання для виявлення відхилень у русі. Якщо трафік відповідає нормам, пакет даних просто звільняється. Якщо визначено зловмисний трафік, то відбувається пом'якшування блокуванням, перенаправленням і відхиленням. Інформація про відхилений трафік повертається в навчальні модулі штучного інтелекту та модулі моделювання для навчання штучного інтелекту.

За допомогою ретельного фільтрування трафіку за певними особливостями, які були визначені вдалося створити модель упередження низькошвидкісних HTTP DDoS-атак з використанням ШІ. А оскільки аномальний трафік який був відфільрований надсилається до блоку Навчання ШІ і моделювання, таким чином інформація про шкідливий

трафік буде опрацьована даним модулем та буде задіяна при новому колі фільтраці. Що забезпечить ефективний захист кінцевих користувачів.

Модуль виснаження пам’яті при DDoS-атаці.

Наступним кроком було аналізування модуля виснаження пам’яті при DDoS-атаці. У низькошвидкісній DDoS-атаці з вичерпанням пам'яті жертва має обслуговувати запити від законних користувачів, а також атакуючих ботів, як і в DDoS-атаці з вичерпанням пропускної здатності. Тому в цій моделі для позначення вхідного трафіку можна використовувати той самий процес Пуассона. Але в цьому випадку аналіз трафіку на рівні пакетів більш доречний.

Зазвичай деякі дані зберігаються в буфері пам'яті лише на етапі встановлення з'єднання з протоколом TCP. Отже, аналіз трафіку на рівні сеансу є більш доцільним для виявлення DDoS-атаки з вичерпанням пам’яті. Зважаючи на це, середній розмір пакета чи сенс не має значення.

Загальна швидкість надходження сеансу бота $\lambda_{СБ}$ та легального сеансу користувача $\lambda_{СК}$ – це те, що можна вважати нормою для опису вхідного трафіку $\lambda_{ВТ}$. Так само, як і в моделях DDoS-атаки знижується підвищена частота смугового пропускання, загальна частота надходжень $\lambda_{ВТ}$ базується на тому, що велика кількість систем фільтрує хибно-позитивні параметри $P_{ХП}$, що є ймовірними помилковими спрацьовуваннями і помилково негативними результатами $P_{ХН}$, на додаток до середньої частоти сеансів ботів і легальних користувачів $\lambda_{ЗК}$, а також кількість ботів $\lambda_{КБ}$ використаних при атаці формули 2.10.:

$$\begin{gathered}
\lambda_{СБ} = \sum_{i=1}^{n} \lambda_{СК_i}; \\
\lambda'_{СБ} = \lambda_{СБ} \cdot P_{ХН}; \\
\lambda'_{КБ} = \lambda_{КБ} \cdot (1 - P_{ХП}); \\
\lambda_{ВТ} = \lambda'_{КБ} + \lambda'_{СБ}.
\end{gathered} \tag{2.10}$$

У разі DDoS-атаки з вичерпанням пам'яті вхідні запити зберігаються хостом-жертвою, доки вони в все ж таки не будуть виконані. Але буфер пам'яті обмежений, та може зберегти лише до N сеансів за один раз. І збережені сеанси не враховуються за принципом FIFO (першим увійшов, першим вийшов). Вони опрацьвуються, поки залишаються в черзі. Отже, ми пропонуємо скористатися послугою M/M/N/N.

У цій моделі є N служби, які показують, скільки даних сеансу може зберігатися в буфері пам'яті. Коли черга переповнена, то нові сенси будуть обслуговуватись лишень за наявності вільного місця в буфері пам'яті. Якщо вся пам'ять зайнята, нові запити відкидаються без їх обслуговування, незалежно від того, чи це запит від законного користувача чи зараженої машини. (рис. 2.4.).

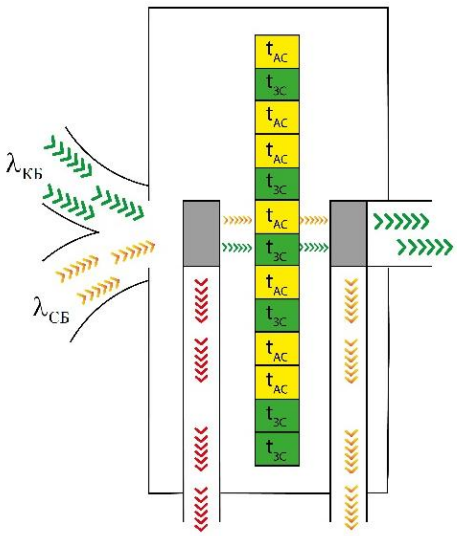


Рис. 2.4. Приклад модуля виснаженням пам’яті при DDoS-атаці

Для спрощення моделі та стійкості розрізнення атак та законних сеансів у реальному часі пропоную використовувати загальний середній час обслуговування t_O (2.11), який описує середній час зберігання даних сеансу в буфері пам’яті (не має значення, чи це атака чи дані законного сеансу користувача):

$$t_{\text{О}} = \frac{\lambda'_{\text{КБ}}}{\lambda_{\text{ВТ}}} \cdot t_{\text{ЗС}} + \frac{\lambda'_{\text{СБ}}}{\lambda_{\text{ВТ}}} \cdot t_{\text{АС}} = \frac{\lambda'_{\text{КБ}} \cdot t_{\text{ЗС}} + \lambda'_{\text{СБ}} \cdot t_{\text{АС}}}{\lambda_{\text{ВТ}}}. \quad (2.11)$$

Імовірність аварійного завершення запиту $P_{\text{ПЗ}}$ через брак пам’яті можна використовувати за загальним середнім часом $t_{\text{О}}$ обслуговування сеансу, загальною середньою швидкістю надходження сеансу $\lambda_{\text{ВТ}}$ та розміром буфера пам’яті N:

$$P_{\text{ПЗ}} = \frac{\frac{p^N}{N!}}{\sum_{j=0}^{N} \frac{p^j}{j!}}, \text{ де } p = \lambda_{\text{ВТ}} \cdot t_{\text{О}}. \quad (2.12)$$

Імовірність успіху DDoS-атаки через вичерпання пам’яті $P_{\text{ВП}}$ – це частина законних сеансів користувача, які не були обслужені (під час фільтрації або в буфері не вистачило пам’яті для їх зберігання).

$$P_{\text{ВП}} = P_{\text{ХП}} + P_{\text{ПЗ}} \cdot \left(1 - P_{\text{ХП}}\right). \quad (2.13)$$

Було виконано впровадження для перевірки ефективності фільтрації пакетів DDoS-атаки. Експериментальна установка проводилася у вигляді сервера, оснащеного Ubuntu 20.04, процесором Intel Core i7-1165G7 з частотою 2,80 ГГц і 16 ГБ оперативної пам'яті. Для моделювання топології мережі була використана платформа Mininet 2.3.0, яка допомагає створити віртуальну мережу, що містить хости, комутатори, контролери та запити. В якості комутатора було обрано Cisco та зроблено відповідні налаштування [20]. Для моделювання динаміки DDoS-атаки використовувалася утиліта hping3, яка відома тим, що надсилає спеціалізовані пакети TCP/IP. Крім того, надійний інструмент обробки пакетів Iperf використовувався для створення пропускної здатності та затримки, необхідних для запуску атаки.

Сценарій перед DDoS-атакою.

Розглянувши графік на малюнку, ми бачимо, що трафік коливається з часом, коливаючись від 9,3 Мбіт/с до 10,5 Мбіт/с. Це коливання триває до 12-ї одиниці часу, після чого трафік стабілізується на рівні 9,6 Мбіт/с. Подальші спостереження показують, що трафік має тенденцію до зниження, і до 15-го моменту часу виміряне значення падає до 9,38 Мбіт/с. Після цього пропускна здатність змінюється більш істотно, що збігається з моментом DDoS-атаки (рис. 2.5).

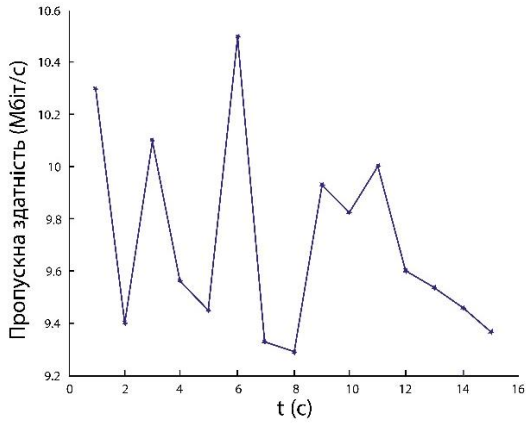


Рис. 2.5. Пропускна здатність перед сценарієм DDoS-атак

Сценарій після DDoS-атаки

Вивчаючи 2.5 графік на малюнку вище, видно, що спочатку перший сплеск, при цьому потік досягає пікового значення 630 Мбіт/с до моменту 1. Далі слід помітити зниження з коливаннями між 8 і 12 Мбіт/с. Це ознаки зниження пропускної здатності після DDoS-атаки (рис. 2.6.).

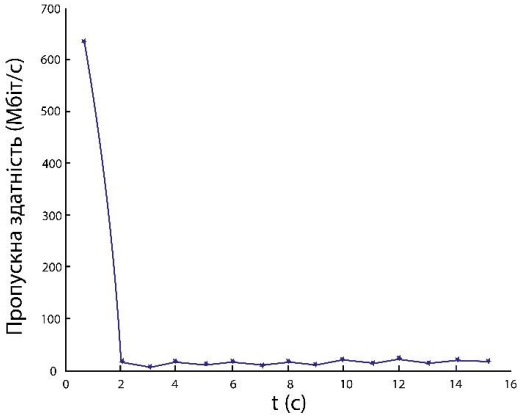


Рис. 2.6. Пропускна здатність після сценарію DDoS-атаки

У створенні потужної системи захисту сервера потрібно інтегрувати раннє виявлення з алгоритмами фільтрації, що створює міцну основу. Наприклад, моделі, які включають оновлення алгоритмів машинного навчання, можуть не відставати від змін у моделях атак. У той же час багаторівневий підхід, який об'єднує статистичний аналіз, класифікацію такої поведінки фільтрацією, зменшує кількість помилкових спрацьовувань, а також зменшує навантаження на систему.

2.2. Метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, заснована на аналізі кластера пакетів

Опис класифікацій атак DoS і DDoS для покращення підходу переднього виявлення. Існують різноманітні системи DoS- і DDoS-атак, які відрізняються за представленими аспектами DoS-атаки, рівнем пояснення та ступенем застосовності.

Запропоновано нову класифікацію протидії DoS-атакам, яка поєднує різні ідеї. Це показано на рис. 2.7. Три критерії для класифікації контрзаходів проти атак DoS: фаза протидії, місце розгортання контрзаходу та взаємодія контрзаходів з іншими рівнями системи.

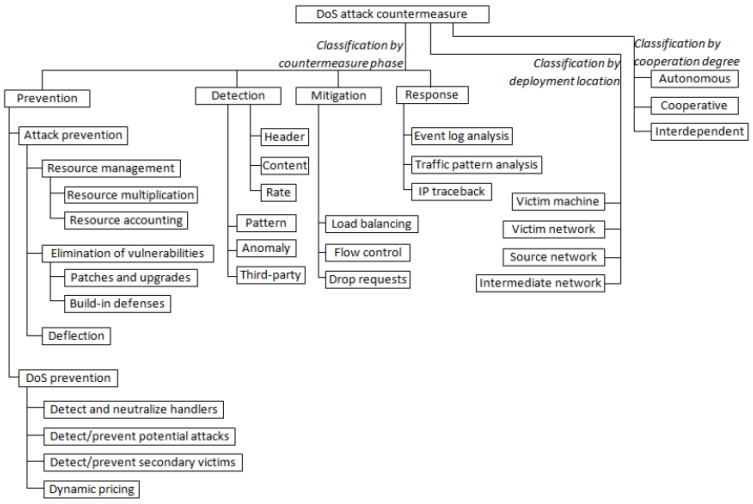


Рис. 2.7. Нова класифікація протидії атакам DoS та DDoS

Більше критеріїв, які використовуються для класифікації фази виявлення, стосуються стратегій, які використовуються для виявлення атаки. Класифікація механізмів захисту від DDoS на реактивному рівні розглядається завдяки роботам вченого J. Mirkovic і розподіляється на три групи:

• Виявлення шаблонів. Будь-яка стратегія, яка порівнює всі комунікації з записами в базі даних сигнатур атаки, називається виявленням шаблонів.

• Виявлення аномалій. На відміну від звичайного та вхідного трафіку, схема виявлення аномалій попереджає, якщо трафік значно відрізняється від нормального.

• Виявлення сторонніх розробників. Налаштування, які реалізують виявлення сторонніх розробників і не виконують механізм виявлення всередині себе, а залежать від зовнішніх систем.

• Пом'якшення. Фаза пом'якшення намагається зменшити або зупинити атаку. Вчений М. Шпехт поділяє цю фазу на три частини:

• Балансування навантаження. Балансування навантаження означає збільшення пропускної здатності для важливих посилань або серверів копіювання, яке зазвичай виконує постачальник мережі.

• Контроль потоку. Максимально мінімальне справедливе регулювання орієнтованого на сервер маршрутизатора налаштовує маршрутизатори, які звертаються до сервера, за допомогою логіки для обмеження вхідного трафіку до рівня, безпечного для обробки сервером.

• Відкинуті запити. Деякі запити можуть бути скинуті, щоб пом’якшити атаку випадковим чином або навмисно.

• Криміналістика. Усі атаки необхідно належним чином аналізувати, щоб запобігти подібним ситуаціям. Вчені Дулігеріс і Мітрокотс описують це як відповідь на вторгнення та надають внутрішню класифікацію наступним чином, тому виокремлюємо наступні ознаки:

• Аналіз трафіку. Під час DoS-атак шаблони трафіку можна зберігати та пізніше аналізувати. Це забезпечує оновлення інформації для виявлення наступних атак або навіть пом'якшення.

• Аналіз журналу подій: аналізуйте журнали подій, зафіксовані під час атаки. Це допоможе точніше визначити тип атаки та бути готовим до таких атак у майбутньому.

• Відстеження IP, важливо відстежувати трафік атаки, щоб ідентифікувати та, можливо, усунути зловмисника. Це можна зробити різними способами.

Іншим фактором, який використовується для класифікації протидії DoS, є місце розташування контрзаходу. Є три можливі місця, визначені вченими К. Дулігерісом, А. Фадлаллахом і Дж. Мірковичем. Саме тому пропонуємо чотири можливі місця [40, 41, 42]:

• Машина жертви. Деякі засоби протидії DoS призначені для використання на одній машині для захисту цієї машини від атак або принаймні для пом’якшення атак.

• Мережа жертв. Якщо контрзахід полягає в тому, щоб врятувати всі комп’ютери в мережі від ефекту DoS або навіть від самоатаки, його слід розгорнути в мережі жертви.

• Вихідна мережа. Засіб протидії DoS, застосований у мережі зловмисника, який блокує весь вихідний трафік атаки, називається захистом вихідної мережі.

• Проміжна мережа. Повинна захищати велику кількість хостів і повинена бути розгорнута десь в Інтернеті, де вона відстежує весь підозрілий трафік.

Іншою темою, яка використовується для класифікації протидії DoS, є ступінь співпраці, як це обговорюється в роботах А. Фадлалла та Дж. Мірковича. Це дозволить нам оцінити тип зловмисника та виділити три можливі випадки [66, 118]:

• Автономні механізми працюють незалежно, коли вони розгорнуті в точці, будь то хост або мережа, де вони потрібні.

• Кооперативні механізми зазвичай співпрацюють з іншими системами, але можуть також функціонувати незалежно.

• Взаємозалежні механізми не можуть функціонувати незалежно в одній точці, де вони розгорнуті. Це має бути в кількох точках.

Усі виділені властивості та категорії засобів протидії DoS-атакам утворюють певну класифікацію засобів протидії DoS-атакам (див. рис. 3.1). Інформацію про атаку необхідно вказувати у всіх трьох категоріях, намагаючись повністю описати протидію DoS-атаці. Завдяки розподіленому та комбінованому захисту можна виділити один засіб протидії навіть при розгляді кількох категорій.

На основі даної інформації розроблено метод раннього виявлення та пом’якшення низькошвидкісних DDoS-атак.

Низькошвидкісні DDoS-атаки на рівні L7 є одними з найскладніших для виявлення, оскільки вони можуть імітувати законний трафік. Більшість сучасних систем захисту не встигають адаптуватися до динаміки таких атак, що призводить до втрати доступності критичних ресурсів. У цьому документі пропонується метод, заснований на аналізі груп пакетів (PGA), який об’єднує часові, кількісні та контекстні параметри для раннього виявлення аномалій.

Метою цього методу є:

- розробити адаптивні алгоритми фільтрації на основі групового аналізу пакетів;

- зменшити хибнопозитивні результати.

Вивчивши праці вчених, я зрозумів, що обмежуватися традиційними техніками недоцільно. Аналіз сигнатур виявився неефективним для атак зі зміною шаблону. Статистичні пороги не враховують контекстний зв’язок між пакетами.

Зосередимо увагу на перевагах групового аналізу пакетів. Виявленні групи пакетів дозволяють аналізувати рядок запитів, які відображають законну поведінку. Контекстний аналіз враховує зв'язок між джерелами, інтервалами та типами запитів.

Математична модель методу, визначення груп пакетів. Група G формується з пакетів, які надходять у часовому вікні ΔT вирази: 2.14 та 2.15:

$$G = \{P_1, P_2, ..., P_n\} \tag{2.14}$$

де: P_i - і-тий пакет.

Функція ризику атаки

$$R(G) = \alpha \cdot \frac{N}{\Delta T} + \beta \cdot \left(1 - \frac{U_{IP}}{N}\right) + \gamma \cdot \sum_{i=1}^{N-1} \frac{1}{\Delta t_i} \tag{2.15}$$

де:

α, β, γ - вагові коефіцієнти (калібруються за допомогою оптимізації на основі історичних даних);

U_{IP} - кількість унікальних IP-адрес у групі;

$\Delta t_i = t_{i+1} - t_i$ - інтервал між пакетами.

Калібрування коефіцієнтів:

$\alpha = 0.5, \quad \beta = 0.3, \quad \gamma = 0.2$ (на основі емпіричних даних)

Порогове значення ризику знаходимо за допомогою виразу 2.16.

$$R_{threshold} = \mu + k \cdot \sigma \tag{2.16}$$

де:

$\mu = \frac{1}{M} \sum_{j=1}^{M} R(G_j)$ - середнє значення ризику для легальних груп

$\sigma = \sqrt{\frac{1}{M}\sum_{j=1}^{M}(R(G_j - \mu)^2}$ - стандартне відхилення

$k = 3$ - (коефіцієнт, що забезпечує 99.7% впевненості при нормальному розподілі)

Алгоритм кластеризації DBSCAN/

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) обрано через його здатність виявляти ділянки довільної форми та ігнорувати шум.

Математичне представлення:

- відстань між пакетами вираз 2.17.:

$$d(P_i, P_J) = w_1 \cdot \left| t_i - t_j \right| + w_2 \cdot IP\_dist(IP_i, IP_j) \qquad (2.17)$$

де:

$w_1 = 0.7$, $w_2 = 0.3$ - ваги часової та IP відстані

Параметри DBSCAN:

$e = 0.5$ (максимальна відстань між сусідніми точками)

$\min Pts = 5$ (мінімальна кількість точок для формування кластера)

Порівняння з K-means

K-means, вимагає заздалегідь визначеної кількості кластерів, чутливий до викидів.

DBSCAN, автоматично визначає ділянки, здатний протидіяти шуму.

Експериментальні результати, тестування на емуляторі

Умови:

- 10 000 легальних користувачів, 500 ботів.
- трафік включає HTTP GET/ POST-запити.

За допомогою даного експеременту зібрані дані представлені в таблиці 2.1.

Таблиця 2.1.

Результати тестів за допомогою емулятора

Параметр	Традиційний метод	Удосконалений метод
Час виявлення (сек)	12	7
Хибнопозитивні (%)	8	3
Витрати ЦП (%)	45	30
Ефективність блокування (%)	88	96

Щоб перевірити здатність нового методу працювати в зашифрованому трафіку, проводиться серія експериментів з використанням HTTPS. Результати перевіряються за допомогою того самого типу тестів для HTTPS, а також за допомогою стандартних методів захисту. Експериментальні дані наведені в таблиці 2.2.

Таблиця 2.2.

Порівняння ефективності для HTTP та HTTPS трафіку

Параметр	Удосконалений метод (HTTP)	Удосконалений метод (HTTPS)	Традиційний метод (HTTPS)
Ефективність блокування (%)	96	92	85
Хибнопозитивні (%)	3	5	10
Час виявлення (сек)	7	9	12
Витрати ЦП (%)	30	35	45

Ефективність блокування:

- для HTTPS трафіку ефективність знизилася на 4% (з 96% до 92%) через обмежений аналіз вмісту пакетів. Однак цей показник все ще на 7% вищий, ніж у традиційних методів.

Кількість помилкових спрацьовувань зросте з 3% до 5%, оскільки важко відрізнити атакуючий трафік від легального; однак аналіз вмісту запиту не проводиться.

Час виявлення:

- ще 2 секунди для HTTPS через необхідність аналізувати метадані (час, розмір пакета), а не безпосередньо перевіряти дані.

Споживання ЦП:

- збільшення навантаження на 5% відбувається через складність обробки зашифрованих даних.

Використовуючи ці експерименти, можна сказати, що метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак за допомогою аналізу обробки груп пакетів працює. Можна відзначити такі особливості:

- адаптивність - динамічне оновлення $R_{threshold}$ дозволяє системі "вчитися" на нових типах атак;

- енергоефективність - використання DBSCAN зменшило навантаження на ЦП на 15% (експериментально підтверджено);

- стійкість до обходу: - аналіз груп унеможливлює маніпуляції з окремими пакетами.

Також на рахунок обмежень наведемо наступні аспекти:

- залежність від якості кластеризації: Помилки в DBSCAN можуть призвести до пропуску атак;

- чутливість до параметрів, неправильне калібрування α, β, γ знижує ефективність.

Ефективне використання обчислювальних ресурсів походить від хорошого методу раннього виявлення та захисту від низькошвидкісних атак HTTP DDoS. Оскільки часові рамки довгі, а піки навантаження чітко

визначені, важко виявити та захистити від низькошвидкісних HTTP DDoS-атак традиційним способом.

Основні принципи методу базуються на аналізі групової обробки пакетів за певних умов фільтрації для виявлення підозрілого трафіку та запобігання його впливу на систему. Ось основні елементи методу:

1. Обмеження кількості запитів з однієї IP/підмережі:

- встановити обмеження на кількість запитів, які можна зробити за певний період часу (наприклад, хвилину або годину) з однієї IP-адреси або підмережі.

- збільшити ліміт для джерел, яким можна довіряти (наприклад, внутрішні служби або клієнти).

- автоматично блокувати IP-адреси тих, хто перевищує встановлений ліміт.

2. Для блокування трафіку з некористувальницьких регіонів:

- визначити регіони, звідки надходить трафік, на основі даних геолокації.

- закритий доступ з регіонів відсутніх зареєстрованих клієнтів або фізично відсутніх користувачів.

- налаштувати «білий список» регіонів, щоб пропускати трафік лише з надійних джерел.

3. Аналіз тривалості запиту:

- виміряти час обробки кожного запиту.

- ідентифікувати запити, які мають велику тривалість, що може свідчити про повільну атаку.

- встановити поріг тривалості, а потім заблокувати запити, які перевищують цей поріг.

Наведені нижче формули (2.18.) були використані для виявлення аномалій пакетів і для подальшого розрахунку:

$$P_{n_s}(t) \le P_{n_{an}}(t), \text{ де } P_{n_{an}} \ge AP_{n_s} \quad (2.18)$$

1 мб/с 10 – 12%

$$t_{зап_{an}} \gg t_{зап_s}$$

де: P_{n_s} - кількість пакетів за нормальних умов; $P_{n_{an}}$ - кількість пакетів аномального потоку; A - коефіцієнт (залежить від особливостей функціонування мережі/від навантаження та призначення); $t_{зап_{an}}; t_{зап_s}$ - час запиту при аномальному з'єднанні; час запиту за нормальних умов.

Ми моделюємо нашу мережу комп'ютерів і налаштовуємо сервер для проведення експерименту.

Нижче наведено конфігурацію HTTP-сервера, який буде використовуватися в дослідженні:

- процесор: Intel Core i3-2120 CPU, 3.30 GHz, 3M Cache
- частота процесора: 3,30 ГГц
- оперативна пам'ять: 8 Гб
- мережева карта: 3Com Typhoon (3CR990-TX-97) на MMIO 0xecf80000, 00:01:03:e6:65:e9
- ОС: CentOS Linux версія 6.0; Linux версія 2.6.32-71.29.1.el6.i686 gcc версія 4.4.4 20100726 (Red Hat 4.4.4-13)

Розглянемо захист GNU/Linux від низькошвидкісного HTTP DDoS.

Підвищення безпеки системи, як правило, є відносно складним процесом. Зазвичай це включає налаштування всіх служб для роботи в найбільш відповідний спосіб, налаштування системи для запобігання локальним вторгненням.

Захист запущених процесів не пов'язаний із захистом системи та невідомими вразливими місцями системи. Система GNU/Linux повинна

запускати лише ті компоненти, без яких вона не може виконувати свої функції. Всі інші компоненти не повинні бути задіяні в конфігурації.

Враховуючи доступні оновлення, які допомагають системному адміністратору запровадити безпеку, ми виберемо grsecurity.

Використовуючи конфігурацію GNU/Linux з оновленням grsecurity, яка може допомогти зупинити атаки переповнення буфера, а також створити списки контролю доступу, після встановлення рівня безпеки відкривається діалогове вікно для вибору активних функцій. Усі служби потребують реєстрації всіх подій. Розглянемо параметри конфігурації стеку TCP/IP.

Конфігурація Apache має Protection In, яку застосуємо проти низькошвидкісного HTTP DDoS. Розглянемо налаштування Apache, призначені для уникнення проблем, які виникають через DDoS-атаки.

TimeOut – нехай має найменше можливе значення (на HTTP-сервері під час DDoS-атаки).

Директива KeepAliveTimeout – нехай вона також буде зменшена та/або повністю відключена.

Значення різних директив синхронізації можна виразити таким чином:

LimitRequestBody, LimitRequestFields, LimitRequestFieldSize, LimitRequestLine, LimitXMLRequestBody – слід правильно встановити, для обмеження споживання ресурсів, пов’язаних із запитами користувачів.

Це вимога, коли використовується директива AcceptFilter. За замовчуванням він поставляється з конфігурацією Apache httpd, хоча іноді для роботи його може знадобитися перекомпілювати з новими параметрами ядра ОС.

Директива MaxClients встановлює максимальну кількість клієнтів, які можуть бути підключені одночасно. Встановлення нижчого значення тут зменшить навантаження на сервер HTTP.

Використовуючи інший модуль mpm, щоб мати можливість обробляти більше з’єднань одночасно, а не просто обмежувати вплив повільної HTTP DDoS-атаки. Системи GNU/Linux постачаються з mpm - prefork за замовчуванням, який використовує найбільше системних ресурсів і тому його продуктивність є найнижчою.

Інші модулі Apache накладають обмеження на деякі моделі поведінки клієнтів і, отже, знижують швидкість повільної HTTP DDoS-атаки. Блокування атакуючих зомбі-машин повинно здійснюватися автоматично.

Огляд базується на модулі Apache, який організовує захист від DDoS-атак - mod_dosevasive. Приклад налаштування серверу Apache представлено у додатку А.

Для наступного експеременту застосуємо скрипт, який використовують для помякшення DDoS-атак. В даному коді реалізовано систему сповіщень, для моніторингу активних DDoS-атак, що надасть можливість захиститись від навалів ботів. Даний код написано на мові Shell, а також в код додано аналізатор підписів, щоб розпізнавати ботів. Приклад встановлення та налаштувань DDoS Deflate показано в додатку В.

На (рисунку 2.8.) представлено блок-схему алгоритму, реалізованого в модулі netfilter для забезпечення того факту, що мережа захищена від DDoS-атак шляхом моніторингу та обмеження вхідного трафіку. Це реалізовано за допомогою декількох ключових етапів алгоритму, розглянемо їх детальніше.

Початок: Алгоритм починається з налаштування всіх необхідних параметрів і змінних для подальшої роботи.

Перевірка порту (dport 80, 443): Першим кроком є застосування фільтра та аналізу пакетів TCP для цільових портів 80 (HTTP) і 443 (HTTPS). Ця перевірка важлива, оскільки ці порти найчастіше є цільовими.

Контроль запитів SYN (обмеження синхронізації 1/с): підрахунок вхідних запитів SYN гарантує, що 1 запит не перетинатиметься протягом другого періоду, таким чином запобігаючи перевантаженню сервера через атаку SYN Flood.

Перевірка ліміту IP-адрес (iplimit вище 10): права на кількість підключень з однієї IP-адреси не повинні перевищувати 10, що є ключовим кроком для виявлення ймовірних зловмисників.

Новіший ліміт підключення (новий ліміт 300/с, пакет 400): більше перевірок на початку нових посилань. Кількість нових посилань не повинна перевищувати 300 в секунду, з шансом спалаху до 400. Це дозволяє зберегти звичайний рівень відвідувань і припинити швидкі стрибки.

Синхронізація підрахунку IP-адрес (iplimit вище 10): Перевірте підрахунок IP-адрес, щоб переконатися, що зловмисник не перевищить дозволену кількість підключень.

Перевірка мережевої маски (маска 24): установіть мережеву маску (24), щоб відповідати та забороняти клієнтам із відомих мереж, що може знизити ризик широкомасштабних атак.

Дії пакетів (DROP або ACCEPT): Відповідно до результатів усіх попередніх перевірок, пакети мають бути прийняті (ACCEPT) або відкинуті (DROP).

Припинення процесу (зупинка): важливо записати результати обробки під час завершення алгоритму.

Розробка алгоритму пропонує організовану та ефективну структуру для роботи з TCP-пакетами та поступової перевірки параметрів з’єднання. Таким чином реалізовано захист серверу він низькошвидкісних та іншого роду DDoS-атак, підтримуючи мережу працездатною та стабільною. Для покращення та ефективного захисту потрібно постійно досліджувати динаміку мережевого трафіку. Виконання даного моніторингу

унеможливить ризики та паралізування критичних систем від нових методологій атак.

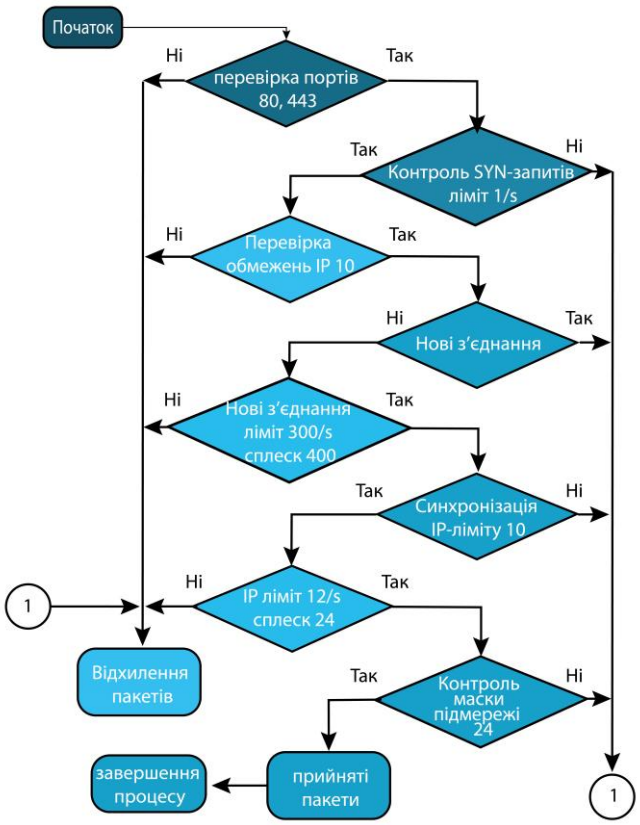


Рис 2.8. Блок-схема алгоритму

Значення ресурсів, які займає віртуальна машина, наведено на рис. 2.9.

```
[root@server1 cache]# vzctl exec 2 cat /proc/user_beancounters
Version: 2.5
uid  resource           held    maxheld    barrier      limit    failcnt
101:kmemsize         1508202    1661695   11055923   11377049          0
  lockedpages              0          0        256        256          0
  privvmpages           5430       7102      65536      69632          0
  shmpages               381        381      21504      21504          0
  dummy                    0          0          0          0          0
  numproc                 19         21        240        240          0
  physpages             2489       2775          0 2147483647          0
  vmguarpages              0          0      33792 2147483647          0
  oomguarpages          2489       2775      26112 2147483647          0
  numtcpsock               5          5        360        360          0
  numflock                 3          4        188        206          0
  numpty                   0          1         16         16          0
  numsiginfo               0          2        256        256          0
  tcpsndbuf            44720          0    1720320    2703360          0
  tcprcvbuf            81920          0    1720320    2703360          0
  othersockbuf         13144      14356    1126080    2097152          0
  dgramrcvbuf              0       8380     262144     262144          0
  numothersock            11         13        120        120          0
  dcachesize               0          0    3409920    3624960          0
  numfile                503        531       9312       9312          0
  dummy                    0          0          0          0          0
  dummy                    0          0          0          0          0
  dummy                    0          0          0          0          0
  numiptent               10         10        128        128          0
[root@server1 cache]#
```

Рис. 2.9. Значення ресурсів, які займає віртуальна машина

Стовпець failcnt показує тільки нулі, інакше це означатиме, що ресурсів, які використовуються сервером недостатньо на даний момент часу. Даний ресурс збільшується у відповідному /. conf, розміщений у каталозі /etc/vz/conf, потім перезапустіть систему за допомогою команди: vzctl перезапуск 101.

2.3. Система протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси.

Створення системи захисту серверів. Зазвичай існує достатня кількість моделей атак DoS і DDoS, однак вони зосереджені на одному конкретному типі атаки або навіть на конкретній атаці чи представленні ситуації. Для практичних цілей можуть знадобитися більш загальні моделі, які б враховували якомога більше різних загроз атак, а також шляхів захисту.

У цьому розділі ми представляємо моделі атак DDoS для трьох основних типів атак (вичерпання смуги пропускання, виснаження пам'яті та виснаження роботи ЦП), а також складену модель атак DDoS, яка представлятиме ймовірність вижити після змодельованої атаки DDoS незалежно від того, який ресурс було вичерпано.

Модель DDoS-атаки із зменшенням пропускної здатності.

Аналізуючи DDoS-атаку із зменшенням пропускної здатності, вхідний трафік, який досягає системи-жертви, розглядається як складений з двох компонентів: звичайного трафіку та трафіку атаки.

Як згадувалося в розділі 1, багато досліджень показали, що на рівні пакету та часових масштабах, менших за 1 с, трафік у великій зоні поводиться як мультифрактальний [116]. Однак це стосується виключно звичайного руху. Трафік атаки зазвичай не настільки залежить від сплеску трафіку та автокореляції пакетів через свою природу – він намагається

виснажити ресурси жертви першими відправленими пакетами та не продовжувати спілкуватися з жертвою як звичайний користувач. Подібна поведінка дуже поширена для DDoS-атак із зменшенням пропускної здатності та пам’яті. Беручи до уваги той факт, що під час DDoS-атаки трафік атаки може бути більшим за розміром, ніж звичайний, загальний вхідний трафік жертви є мультифрактальним, коли трафік атаки близький до нуля, але коли трафік атаки перевищує звичайний, загальний трафік можна представити як процес Пуассона навіть на рівні пакету.

У концептуальній моделі DDoS-атаки із зменшенням пропускної здатності ми пропонуємо не аналізувати всю мережеву структуру від організатора атаки, агентів атаки, глобальних маршрутизаторів і жертви через потенційно занадто великий обсяг змодельованих даних. Для моделювання DDoS-атак із виснаженням пропускної здатності ми враховуємо поведінку жертви атаки та найближчого до неї маршрутизатора. Однак властивості маршрутизатора не описані детально, і ми припускаємо, що він здатний маршрутизувати всі вхідні пакети, не впливаючи на схему вхідного трафіку. При цьому канал між маршрутизатором і жертвою має обмежену пропускну здатність, оскільки він здатний передавати пакети лише з обмеженою швидкістю T.

Через обмеження зв’язку з жертвою маршрутизатор у запропонованій моделі може діяти трьома способами: відправляти пакет на інший вузол, відмінний від жертви, якщо він був призначений для неї; відправляти пакет жертві, якщо він їй присвячений і посилання здатне обслуговувати додаткові дані; скинути пакунок через надто зайняту лінію до одержувача пакунку (див. рис. 2.10.).

Відкидання пакетів є результатом нездатності маршрутизатора зберігати запити, що очікують (жертва несе відповідальність за це, і це буде розглянуто в розділі 3 як особливість DDoS-атаки з виснаженням пам’яті) і недостатнього зв’язку з жертвою можливостей маршрутизатора

обслуговувати весь вхідний трафік. Щоб підвищити стійкість до DDoS-атаки зі зменшенням пропускної здатності, слід збільшити пропускну здатність каналу. Тому можна відкрити додаткові канали для збільшення ресурсів пропускної здатності.

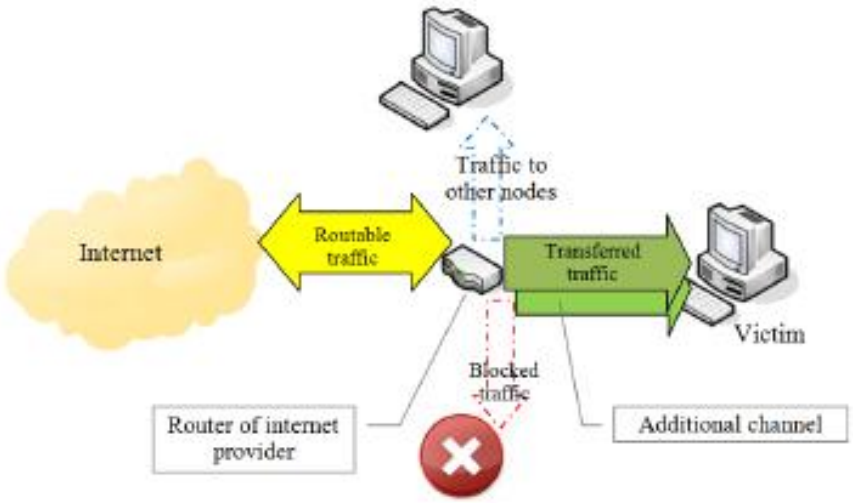


Рис. 2.10. Модель виснаження пропускної здатності при DDoS-атаці

Модуль виснаженням пам’яті при DDoS-атаці.

Усі вхідні запити та внутрішні служби системи мають виконуватися центральним процесором (CPU). Однак ресурси ЦП обмежені, і він здатний виконувати команди з обмеженою швидкістю одну за раз.

Множення частоти процесора f і кількості необхідних циклів для виконання завдання c показує, скільки часу потрібно для завершення одного завдання. Однак робота може почекати це буде страчений, бо один робота вже є під виконанням або навіть більше завдань стоять у черзі перед ним.

Алгоритми планування операційної системи керують запитом завдань, що очікують. У FCFS (First Come Firs Serve) алгоритм планування нових завдань буде розміщено в кінці черги і буде чекати, поки всі попередні завдання будуть виконані (див. рис. 2.11).

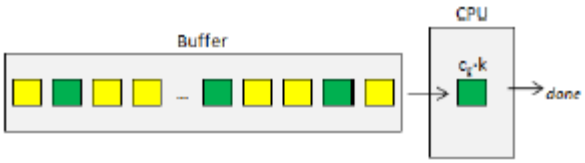


Рис. 2.11. Принцип алгоритму планування FCFS

Відома Кругова система планування алгоритм місць новий запит ставить на кінець з в чергу. Однак, все робочих місць є виконано в квантові і після виконання одного кванта завдання повертається в кінець черги, якщо воно ще не завершено, або виходить із системи, якщо його виконання завершено (див. рис. 2.12.). Цей алгоритм планування має власну область застосування, однак продуктивність порівняно з FCFS є досить схожою, коли квант часу великий і може бути повільніше, коли квант часу занадто малий.

Рис. 2.12. Принцип циклічного алгоритму планування

Обидва ці алгоритми планування не використовують пріоритети для завдань. Сучасні операційні системи використовують більш складні алгоритми планування, враховуючи пріоритетність завдання, розмір завдання тощо [131]. Однак DDoS-атаки виснаження процесора можуть впливати на ці параметри, тому для моделі DDoS-атаки виснаження процесора ми не звертаємо увагу на конкретний алгоритм планування. і припустимо, що використовується алгоритм FCFS.

Це припущення дозволяє нам використовувати систему масового обслуговування M/M/1 для моделі DDoS-атаки з виснаженням роботи ЦП. У номері є один канал і одна нескінченна лінія очікування, що представляє можливість зберігати стільки запитів на роботу, скільки потрібно (існує

обмеження в системній пам'яті, однак на практиці цього важко досягти).

Весь вхідний трафік обробляється центральним процесором, однак різні пакети може вимагати різного обсягу роботи ЦП. Тому в цій моделі ми використовуємо середню швидкість надходження пакетів легального користувача та бота λ_{nc}, λ_{bc} а також середня кількість циклів обробки пакетів, надісланих законним користувачем і роботом c_n, c_b.

Знаючи кількість ботів, які беруть участь у DDoS-атаці n, середня швидкість надходження пакетів атаки λ_{ac} можна розрахувати:

$$\lambda_{ac} = \sum_{i-1}^{n} \lambda_{bci} \tag{2.19}$$

Однак, щоб знати загальну швидкість надходження пакетів λ gc і середнє число циклів для загальної обробки пакетів c g вимагає додаткових системних характеристик, таких як середня швидкість надходження службових завдань λ s в системі та середнє число циклів, необхідних для його обробки c s зробити модель більш реалістичною. Ці характеристики дозволяють враховувати як обробку пакетів, так і запущені процеси системи. Однак, якщо це не потрібно, ці параметри можуть бути пропущено в 23 і 24 формули до розрахувати загальну роботу прибуття швидкість λ gc і середнє число циклів для загальної обробки завдання c g .

$$\lambda_{gc} = \lambda_{nc} + \lambda_{ac} + \lambda_s \tag{2.20}$$

$$c_g = \frac{\lambda_{nc} \cdot c_n + \lambda_{ac} \cdot c_a + \lambda_s \cdot c_s}{\lambda_{gc}} \tag{2.21}$$

Загальна середня швидкість надходження завдань являє собою швидкість надходження завдань до ЦП. Тоді як середня швидкість обслуговування ЦП $\mu_{куб}$ можна знайти за допомогою середньої кількості циклів для загальної обробки завдання c_g і частота процесора f:

$$\mu_{cc} = c_g \cdot f \tag{2.22}$$

Жертва може помітити роботу ЦП, виснаження DDoS напад за збільшення завантаження ЦП. Однак для користувачів послуг має значення лише якість обслуговування. Тому пропонуємо судити про виснаження роботи процесора DDoS-атаки ймовірність за середнім часом, який робота проводить у системі L, і її порівняння з обмеженням часу t w який користувач готовий чекати на виконання завдання.

Розрахунок середнього часу, який робота проводить у системі, можна зробити лише в стаціонарному стані (коли швидкість надходження менше, ніж швидкість обслуговування) (Anderson et al. 2002), інакше довжина черги також збільшиться до нескінченності. як час обслуговування вираз 2.23.:

$$L = \frac{1}{\mu_{cc} \cdot S - \lambda_{gc}}, \; коли \; \frac{\lambda_{gc}}{\mu_{cc} \cdot S} < 1 \tag{2.23}$$

Там *S* представляє кількість процесорів у системі. Усі вони мають власну чергу очікування, яка має приблизно однакову довжину, а тому *1/c* із середньої загальної швидкості надходження на роботу має обслуговуватися одним центральним процесором.

Для нестабільних випадків системи M/M/1 виснаження роботи процесора ймовірність успіху DDoS-атаки P_C дорівнює 1. Інакше ймовірність успіху атаки залежить від середнього часу, який робота проводить у системі: якщо воно менше t_w – ймовірність успіху дорівнює L/t_w; якщо більше або дорівнює t_w – ймовірність успіху дорівнює 1:

$$P_C = \begin{cases} 1, \; \dfrac{\lambda_{gc}}{\mu_{cc} \cdot S} \geq 1 \;\; або \;\; L \geq t_w \\ \dfrac{L}{t_w}, \; \dfrac{\lambda_{gc}}{\mu_{cc} \cdot S} < 1 \; і \; L < t_w \end{cases} \tag{2.24}$$

Ця модель не враховує час, необхідний для планування завдань для кількох процесорів, якщо використовується більше ніж один.

Модель DDoS Атаки.

Розроблені моделі пропонуються для конкретного типу DDoS-атаки – виснаження пропускної здатності, виснаження пам’яті або виснаження роботи ЦП. Зазвичай під час одного виду DDoS-атаки використовуються всі три типи ресурсів, але деякі з них в а менше сума. тому для більше справжній ситуації представництво Імовірність успіху DDoS-атаки слід оцінювати як ймовірність того, що хоча б один різних типів DDoS-атак буде успішним вираз 2.25.:

$$P = 1 - \overline{P_B} \cdot \overline{P_M} \cdot \overline{P_C} \qquad (2.25)$$

Однак ці моделі не є незалежними одна від одної (див. рис. 2.13.) і потребують певних модифікацій, щоб об’єднати їх разом у єдину складну систему.

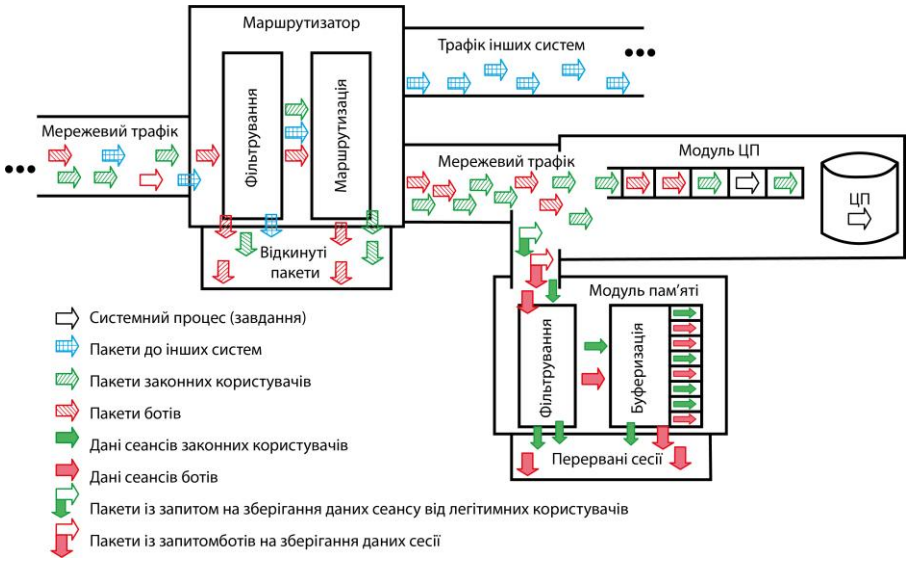


Рис. 2.13. Принципова схема складної DDoS-атаки

Вхідний трафік для моделі виснаження пам’яті та процесора має співвідноситися з вихідним трафіком моделі виснаження пропускної здатності. З іншого боку системи виснаження пам'яті та процесора повинні працювати паралельно. Однак у реальному житті ці дві підсистеми

взаємодіють, щоб спростити модель і оскільки деякі запити в ЦП вимагають місця в буфері пам’яті, а інші – ні, ми розділяємо ці дві підсистеми як такі, що використовують подібні вхідні дані, але не взаємодіють одна з одною.

У даному дослідженні використовується алгоритм фільтрування трафіку.

На рис. 2.14. представлено Систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси.

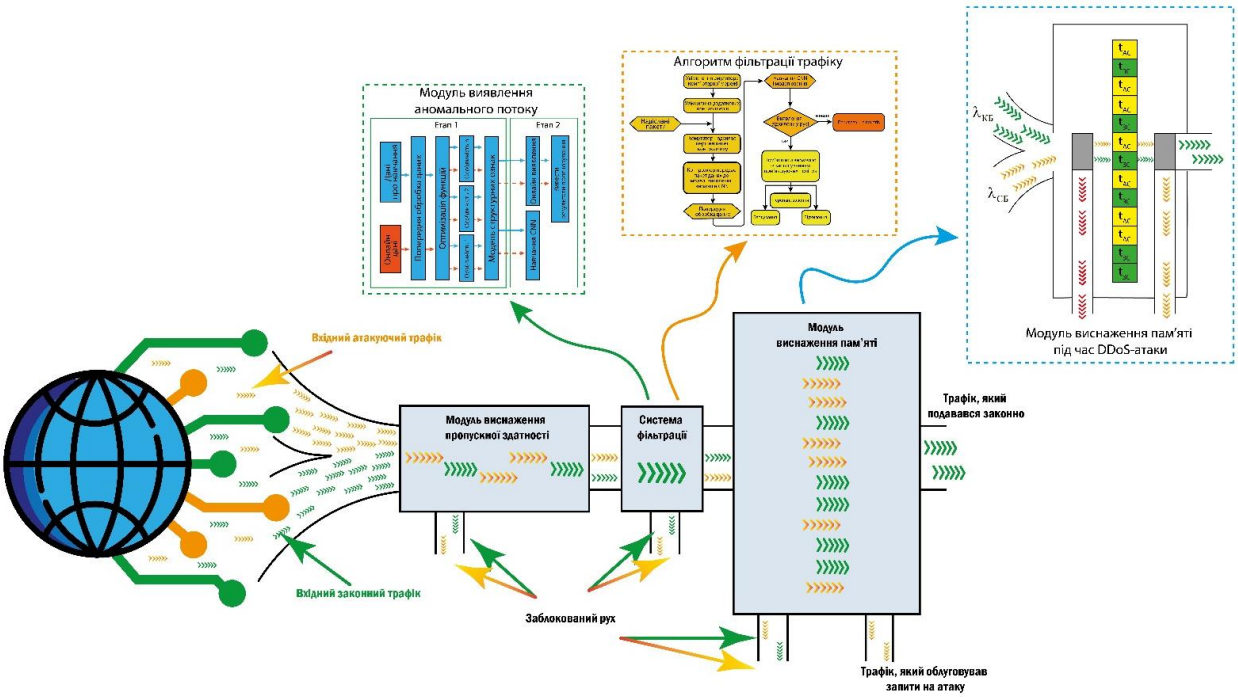


Рис. 2.14. Систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси

Аналіз шкідливого пакетів впливає на швидкодію та роботоспроможність сервера. У майбутньому це буде використано для створення систем, які добре відповідають сучасним загрозам, мають високий рівень надійності та базуються на алгоритмах фільтрації трафіку та виявленні аномалій. Дослідницькі перспективи включають:

- оновити правила сортування, щоб мати можливість пристосуватися до нових видів онлайн-інцидентів і атак;

• створення нових алгоритмів, які використовуватимуться в роботі з хмарними сервісами;

• об'єднання з системами захисту для забезпечення кращої безпеки в Інтернеті.

Висновки до розділу 2

Аналізуючи сучасних виклики кібербезпеки, зокрема складності детектування низькошвидкісних HTTP DDoS-атак через їхню здатність маскування під легітимний трафік та уникати традиційних засобів захисту, було розроблено комплексну систему протидії. Ця система ґрунтується на наступних ключових наукових та практичних досягненнях:

1. Модель детектування аномалій трафіку, що враховує різнопланову природу низькошвидкісних HTTP DDoS-атак. Модель інтегрує аналіз часових інтервалів запитів, глибинне інспектування HTTP-заголовків, оцінку географічної дисперсії джерел та виявлення відхилень у шаблонах поведінки користувачів. Використання адаптивних порогових значень та машинного навчання для аналізу часових рядів забезпечує високу точність розрізнення шкідливої активності від легальних сплесків навантаження, мінімізуючи кількість хибно-позитивних спрацьовувань.

2. Метод попереднього виявлення кіберінцидентів, що базується на поєднанні сигнатурного аналізу з аномальною детекцією в реальних умовах. Даний спосіб включає моніторинг мікрошаблонів запитів (наприклад, частоти звернень до специфічних ресурсів, тривалості сесій, аномалій TCP handshake) та кореляцію подій у розподілених сегментах мережі. Поєднання кількісних факторів (наприклад, ентропія IP-адрес, коефіцієнт відмов) з якісним аналізом намірів дозволяє формувати цілісну картину загрози, навіть за умови використання зловмисниками приховування та зміни джерела коду.

3. Система динамічного прогнозування та виявлення атак, яка використовує топологічний аналіз мережевих потоків і побудову графів взаємозв'язків між підозрюваними джерелами. Система автоматично ідентифікує потенційні траєкторії поширення атаки в межах інфраструктури, враховує динаміку зміни шаблонів трафіку та інтегрує дані про вразливості веб-ресурсів. Це забезпечує не лише своєчасне блокування шкідливих сесій на рівні мережевих елементів або WAF, але й дозволяє прогнозувати й запобігати ускладнення атаки шляхом упередження, оптимізації правил модуля штучного інтелекту, резервування ресурсів та перенаправлення трафіку.

4. Ефект запропонованої системи полягає у формуванні надійного кіберзахисного простору. Розроблені модель, метод та система створюють єдиний контур захисту, спроможний ефективно протистояти складним низькошвидкісним HTTP DDoS-атакам. Це суттєво підвищує доступність і стійкість веб-ресурсів, зменшує ризики фінансових втрат і репутаційної шкоди, а також забезпечує можливість оперативної адаптації заходів безпеки до еволюції тактик зловмисників та змін у конфігурації захищеної інфраструктури. Система є основою для інтелектуальних систем кібербезпеки нового покоління, орієнтованих на упередження та запобігання кіберінцидентам.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНОЇ СИСТЕМИ ПРОТИДІЇ НИЗЬКОШВИДКІСНИМ HTTP DDOS-АТАКАМ

3.1. Експериментальне дослідження методу упередження низькошвидкісних HTTP DDoS-атак

Для апробації розробленого методу упередження низькошвидкісним HTTP DDoS-атакам було змодельовано середовище з 15 штурмових машин та серверу. Різні ситуації DoS-атак є змодельовані з використанням запропонованих моделей виснаження пропускної здатності, виснаження пам’яті та виснаження роботи ЦП, щоб порівняти їх з альтернативними моделями атак. Крім того, моделюється та аналізується комбінована DDoS-атака.

Порівняння характеристик низькошвидкісних HTTP DDoS-атак та їх класифікація контрзаходів.

Критерії аналізу класифікацій DDoS-атаки можуть відрізнятися залежно від сфери її використання. Для цієї роботи було проведено певні дослідження, щоб з’ясувати характеристики зручності використання для запропонованих критеріїв та класифікацій, проаналізованих у Розділі 1.

- Аналіз класифікацій із DDoS-атак.

Щоб описати класифікації DDoS-атак кількісно, було вирішено проаналізувати, як багато категорій представлено в класифікаціях (загальні та ті, що не поділені на дрібніші) та скільки класифікаційних критеріїв (розмірів) використовується в класифікації.

Для цього аналізу, використано сім DDoS класифікацій наступних авторів:

- Асошех (Асоше і Ранезані).
- Дулігеріс (Дулігеріс і Митрокоць).
- Фадлаллах (Фадлаллах і Serhrouchmi).

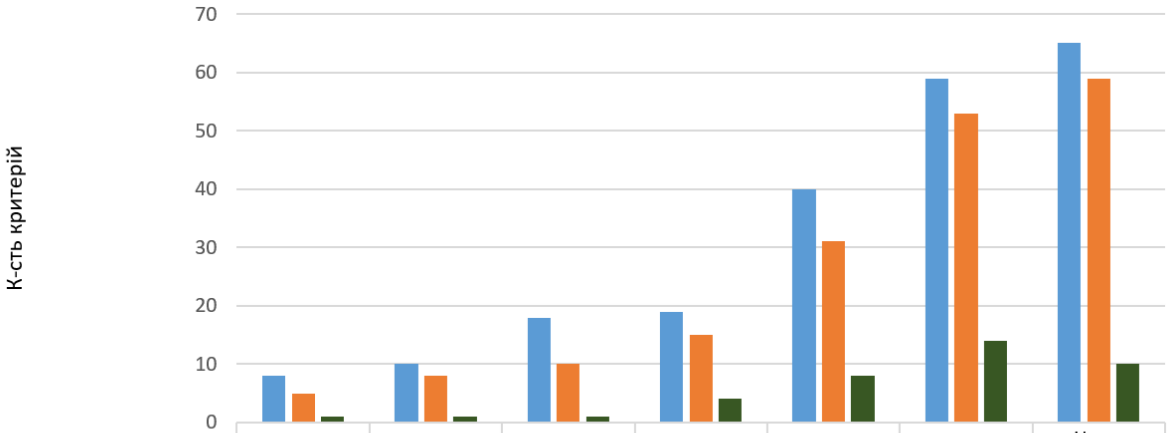
- Каріг (Кариг і Лі).

- Міркович (Миркович і Райхер).

- Specht (Шпехт і Лі).

- та запропонована нами класифікація.

Аналіз класифікацій DoS і DDoS показав, що всі ці класифікації мають різні рівені хвилинності, які змінюється від 1 розмірності, 5 неподільних і 8 унікальних категорій на класифікацію до 14 вимірів (різного рівня), 52 неподільних і 59 унікальних категорій на класифікацію (рис. 3.1). У той же час запропонована класифікація DoS-атак є кращою, враховуючи ці критерії серед проаналізованих таксономій (10 вимірів, 59 неподільних і 65 унікальних категорій).



	Фадлаллах	Кагір	Шпехт	Дулігеріс	Асошех	Мірковіч	Наша класифікація
Унікальні категорії	8	10	18	19	40	59	65
Неподільні ккатегорії	5	8	10	15	31	53	59
Кількість критерій	1	1	1	4	8	14	10

Рис. 3.1. Класифікація статистичних даних проаналізованих DoS та DDoS-атак

Щоб оцінити рівень критерій, ми розглядаємо частку унікальних категорій з врахуванням неподільних категорії, які можна розділити на їх кількість. Це співвідношення має відображати середню кількість варіантів для категорії. Рівень критеріїв показав, що запропоновані класифікації DoS за вченим Дж. Міркович та наша класифікація мають найбільшу кількість

унікальних значень для DoS-атак. Класифікація за вченим Дж. Мірковіч налічує 8.83хв. унікальних значень для DoS-атак. В той час наша класифікація 7.35хв. та запропонована модель стоїть на першому місці. Запропонована модель є найкращою серед обраних, та має 6 варіантів критеріїв, так як усі інші таксономії мають менше 4 варіантів на категорію, винятком являється лише класифікація Дж. Мірковіч. (рис. 3.2).

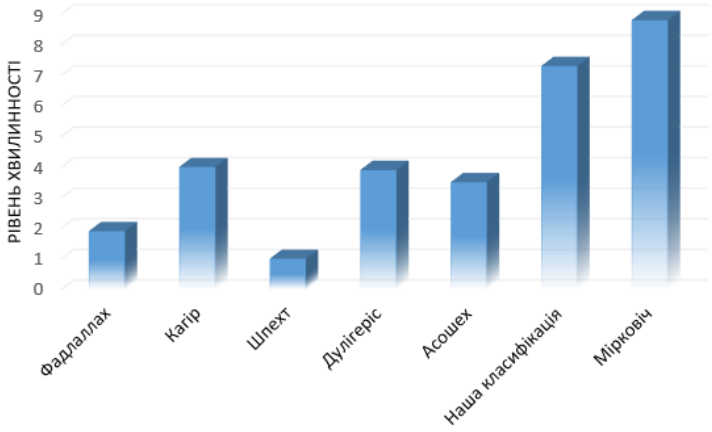


Рис. 3.2. Класифікація категорій хвилинності проаналізованих DoS та DDoS-атак

Статистичні дані показують, що класифікація, запропонована Дж. Мірковичем [3, 4]., є найбільш детальною (найповнішою за різними характеристиками атак та їх можливим вибором значення). Тим не менш, запропоновані дві класифікаціїї DoS та DDoS-атак мають найбільшу кількість варіантів. Трішки поступається кількісними критеріями наша класифікація.

Для представлення характеристик застосування класифікацій були проведені практичні експерименти. Виконано різні DoS-атаки (атака з підстановкою SQL, атака Nuke та червяк), під час моделяції атак були відключені певні налаштування захисту. В спеціально створеній мережі дослідники класифікували їх відповідно до проаналізованих класифікацій. Було 30 респондентів (Студенти бакалаврату кафедри Технічних систем

кіберзахисту), які брали участь у дослідженні, і всі вони класифікували ці три DDoS-атаки в усіх проаналізованих класифікаціях. Вони діяли як жертви та знімали дані зі спостереження машин жертви (машини нападу їм були невідомі).

Одну з таких атак не можна назвати DDoS-атакою, оскільки це сталося через дії одного із черв'яків, коли деякі з цих таксономій були призначені для класифікації DDoS. Однак цей випадок дозволяє нам стверджувати, чи може така атака класифікуватися як DDoS чи ні.

Результати дослідження показали, що класифікація SQL підстановки та атаки черв'яка займає найбільшу кількість категорій у запропонованій класифікації. Це найбільший показник напад Nuke категорії, які були позначені у класифікації Дж. Мірковіча (рис. 3.3 a). Однак, оцінюючи частку позначених та існуючих категорій у проаналізованих класифікаціях, найбільший відсоток позначених категорій був у запропонованій класифікації DoS-атак для всіх трьох випадків атаки (рис. 3.3 b).

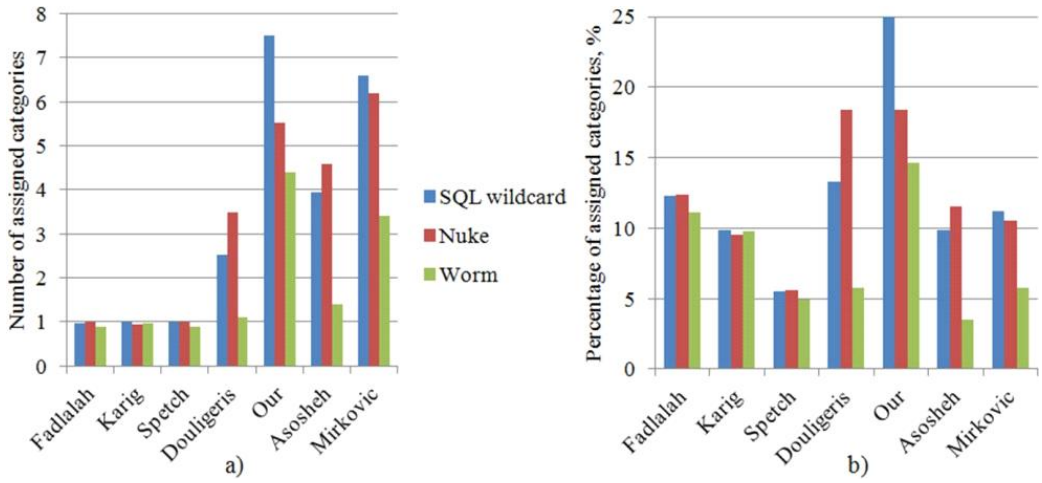


Рис. 3.3. Номер (а) і відсоток (б) з призначений категорії в певної класифікації атак DoS та DDoS

Щоб розрізнити конкретні властивості використання класифікацій, із цього експерименту були розраховані додаткові характеристики:

- які з визначених категорій мали меншу класифікацію;

- яка кількість категорій була залучена при визначенні атаки. (табл. 3.1.).

Таблиця 3.1.

Статистика для різних типів та класифікацій DoS та DDoS-атак

Атака	Характеристика	Класифікація DoS та DDoS-атаки автори						
		Кагір	Фадлаллах	Спетч	Асошех	Наша класифікація	Дулігеріс	Міркович
SQL символ підстановки	Позначені категорії (%)	12.5	100,0	5.6	13.2	25,0	10,0	11.0
	не розширено категорії (%)	50,0	0,0	100,0	0,0	0,0	25,0	0,0
	Позначені розміри (%)	100,0	100,0	100,0	62.5	85.7	50,0	46.4
Nuke	Позначені категорії (%)	12.5	10,0	5.6	18.4	18.3	11.3	10.2
	не розширено категорії (%)	50,0	0,0	0,0	0,0	9.1	0,0	0,0
	Позначені розміри (%)	100,0	100,0	100,0	75,0	78.6	50,0	42.9
Черв'як	Позначені категорії (%)	12.5	10,0	0,0	5.3	15,0	3.8	5.9
	не розширено категорії (%)	50,0	0,0	0,0	0,0	0,0	0,0	0,0
	Позначені розміри (%)	100,0	100,0	0,0	25,0	64.3	18.8	25

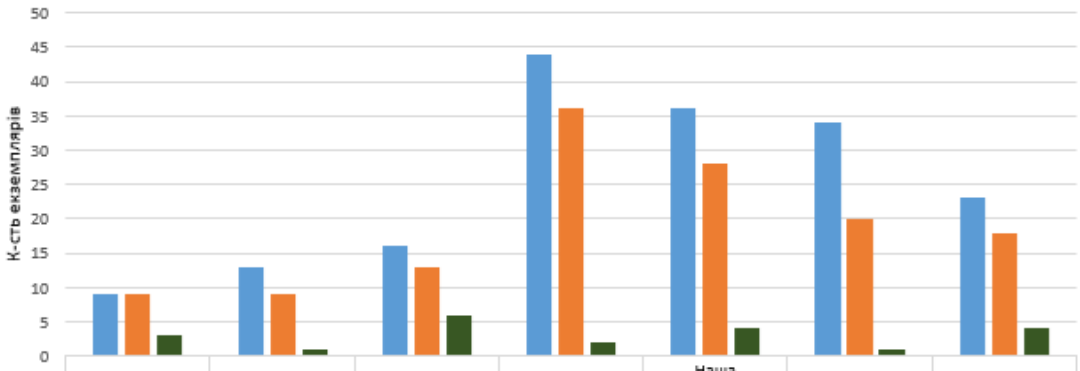
Класифікуючи DoS-атаки, відсоток відзначених розмірів зменшується кількість вимірів збільшується. Таке дослідження виконується, щоб визначити всі властивості атаки жертвою, якщо класифікація включає лише відомі властивості зловмисника. Однак це може бути хибним твердженням, якщо історичні дані про загрози, є добре відомими даними про атаки були засекречені.

Аналіз класифікацій протидії DoS -атакам

За аналогією, як і в аналізі класифікацій DoS та DDoS-атак, були проаналізовані таксономії протидії різним атакам DDoS. Для статистичного аналізу було обрано запропонований засіб протидії кібератак та шість класифікацій DoS або DDoS-атак, проаналізованих у розділі 1:

- А. Асоше.
- С. Дулігеріс.
- А. Фадлаллах.
- Д. Кагір.
- Дж. Міркович.
- С. Шпехт.
- запропонована наша класифікація.

Це дослідження з залученням запропонований протидій та упередженнь D DoS-атакам приймає друге місце серед інших класифікацій за будь-яким із аналізованих критеріїв. Дані представлені на Рис. 3.4.



	Фадлаллах	Кагір	Шпехт	Дулігеріс	Наша класифікація	Асошех	Мірковіч
Унікальні категорії	9	13	16	44	36	34	23
Неподільні ккатегорії	9	9	13	36	28	20	18
Кількість критерій	3	1	6	2	4	1	4

Рис. 3.4. Статистичні дані проаналізованих класифікацій упередження DDoS-атак

Класифікація контрзаходів DDoS-атак, представлена К. Дулігеріс має найбільшу кількість унікальних і неподільних категорій (37 і 45), а також найбільший вибір значення для однієї категорії (Рис. 3.5.). Однак дана класифікація має лишень дві категорії.

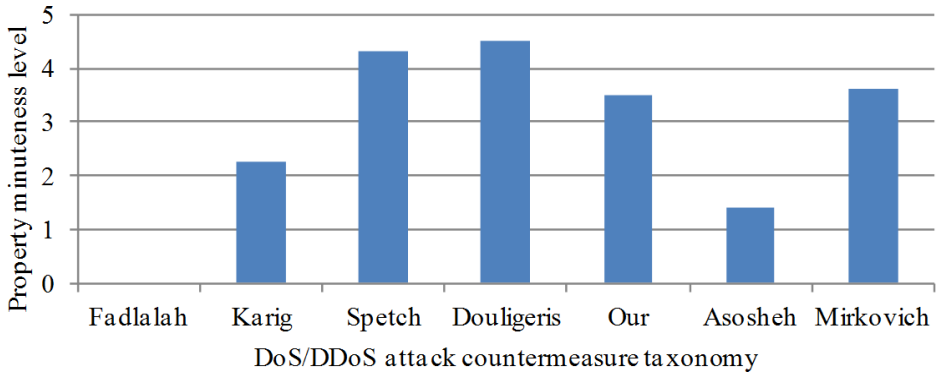


Рис. 3.5. Класифікація категорій хвилинності проаналізованих контрзаходів DDoS-атак

У той час як рівень класифікаційної категорії DDoS-атаки варіювався від 1 до 9, протидія DDoS-атаці не досягає більше 4,5 хвилин. Більше половини проаналізованих класифікацій також відрізняються від 3,5 хв. до 4,5 хв..

3.2. Експериментальні дослідження використання контрзаходів DDoS-атак.

У даному дослідженні для класифікації DDoS-атак було взято 3 атаки. Респондентів попросили запропонувати кіберзахист, який можна застосувати проти наданих DDoS-атак. Вони повинні були позначити всі відповідні контрзаходи у всіх наших проаналізованих класифікаціях контрзаходів.

Аналізуючи пропозиції протидії DDoS-атакам для конкретної DoS-атаки, виявилося, що найбільша кількість запропонованих контрзаходів була в запропонованій класифікації. Тим не менш, оцінюючи відсоток між кількістю можливих категорій і запропонованих категорій контрзаходів,

найбільша відсоток з класифікацій категорії був у класифікації запропонованій за класифікацією протидії DDoS-атакам вченими A. Fadlallah та J. Mirkovic представлена на рисунку 3.6.

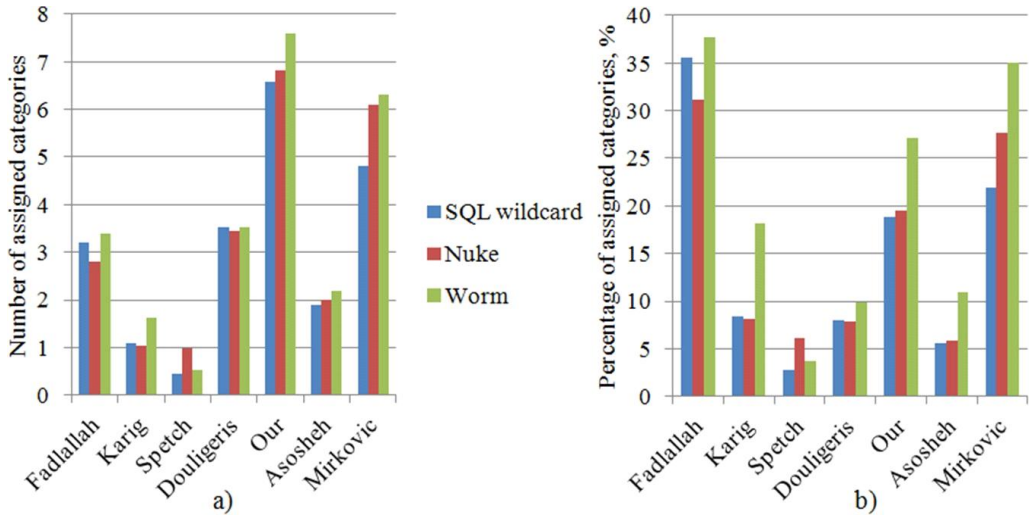


Рис. 3.6. Номер (а) і відсоток (б) який призначений в певній класифікації протидії DDoS-атакам для різних типів атак DoS

При дослідженнях з DoS та DDoS-атак на рахунок контрзаходів, таксономії поділяють (див. табл. 3.2.)

Таблиця 3.2.

Запропонована класифікація DoS та DDoS-атак з урахуванням контраходів.

Атака	Характеристика	DDoS-атака, контрзахід, класифікація, автор						
		Кагір	Фадлаллах	Спетч	Асошех	Наша класифікація	Дулігеріс	Міркович
SQL символ підстановки	Позначені категорії (%)	33.3	7.7	3.1	5.9	18.1	7.9	21.7
	Нерозширені категорії (%)	0,0	0,0	0,0	0,0	0,0	0,0	0,0
	Позначені розміри (%)	100,0	100,0	8.3	100,0	100,0	100,0	100,0
Nuke	Позначені категорії (%)	33.3	7.7	6.3	5.9	19.4	7.9	26.1
	Нерозширені категорії (%)	0,0	0,0	50,0	0,0	0,0	0,0	0,0
	Позначені розміри (%)	100,0	100,0	16.7	100,0	100,0	100,0	100,0

Черв'як	Позначені категорії (%)	38.9	11.5	3.1	5.9	20.8	7.9	26.1
	Нерозширені категорії (%)	0,0	0,0	0,0	0,0	0,0	0,0	0,0
	Позначені розміри (%)	100,0	100,0	8.3	100,0	100,0	100,0	100,0

Аналіз запропонованих DDoS-атак, структура протидії у даній класифікації показала бажання респондентів вибрати найбільш детальне рішення (вузли, які більше не можна розширити) і відзначити всі можливі рішення як можливі (у всіх вимірах). Ця тенденція була запозичена у вчених, які класифікували DDoS-загрози Specht and Lee.

3.3. Перевірка адекватності роботи моделі упередження DDoS-атак.

Немає моделей чи методів оцінки ймовірності успіху DoS-атаки. Тому важко підтвердити запропоновані моделі, існуючі моделі дають різні типи результатів, тоді як реальні експерименти спираються на суб’єктивну думку експерта.

Для порівняння нашої моделі з іншими моделями ми вибираємо характеристики, що представляють використання певного виду ресурсу та загрозу йому як рівність успіху атаки.

Експериментальна ситуація та перевірка навколишнього середовища.

Для перевірки моделей OPNET IT Guru використовувався інструмент моделювання academic edition (Kaparti). Це корисний інженерний і дослідницький інструмент для оптимізації проектування та аналізу продуктивності систем зв’язку та протоколи. Це програмне забезпечення підтримує різні архітектури зв’язку, такі як PSTN, ISDN, кабельні мережі, технології xDSL, оптоволоконні мережі, а також бездротові мережі, такі як Wi-Fi, GPRS, UMTS. В середовищщі можна швидко побудувати мережу з наступних складових: комп'ютер, робочі

станції та сервери, маршрутизатори, комутатори, мости, зірки, точки доступу, посилання, брандмауери, шлюзи, сервери та інші складові елементи.

Карту ситуації було створено для представлення сервера жертви, розташованого в Іспанії, законних джерел трафіку на півночі та півдні Європи та джерел трафіку атаки в Росії (рис. 3.7). Всі вузли ситуації пов'язані з at принаймні лінії 100BaseT, тоді як сервер жертви підключено через з’єднання 10BaseT.

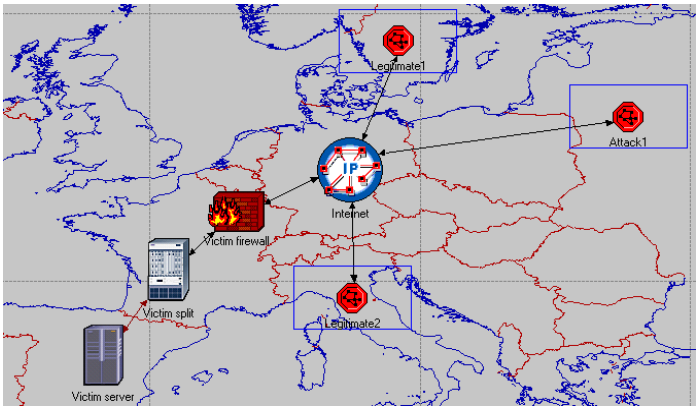


Рис. 3.7. Змодельована ситуаційна карта в інструменті OPNET IT

Сервер-жертви підтримує різні типи послуг: базу даних, електронну пошту, передачу файлів і веб-перегляд, а користувачів системи можна розділити на п’ять категорії:

- інженер – використовує Інтернет перегляд, електронну поштою і файл передачі.

- дослідник – використовує Інтернет перегляд, та електронну пошту.

- клієнтів електронна комерція – використовує Інтернет перегляд.

- менеджер з продажу – використовує доступ до баз даних, електронну пошту, веб-перегляд.

- бот агент – використовує доступ важких баз даних, Інтернет перегляд і передачу файлів.

Є три основні конфігурації моделі для представлення різних

можливих ситуацій. У всіх з них містяться підмережі законного користувача (Legitimate1 і Legitimate2). три локальні мережі. Кожна з LAN містить 20 користувачів з них: 5 інженерів, 5 дослідники, 5 клієнтів електронної комерції та 5 менеджерів з продажу. Одина із трьох моделей не має атакуючої підмережі, тоді як у двох інших є атакуюча підмережа з п’ятьма локальними мережами. В одному з випадків є 10 вузлів у кожній атакуючій локальній мережі (використовується інтенсивна передача файлів і служби веб-перегляду), а в іншому – 25 вузлів у кожній атакуючій локальній мережі (з використанням потужних баз даних, передачі файлів і служб веб-перегляду).

Ці три модельні ситуації відрізняються використовуваними сервісними параметрами, які представлені в таблиці 3.3.

Таблиця 3.3.

Параметри з три експериментальний модель ситуації

Ситуація назва особливість	Без нападу	Атака 1	Атака 2
Номер законної локальної мережі	6	6	6
Номер з законними бази даних користувачів в одній локальній мережі	5	5	5
Номер з законною електронною поштою користувачів в одиній LAN	15	15	15
Номер з законною передачею файлів користувачів в одній локальній мережі	5	5	5
Номер з законним Інтернет переглядом користувачів в одній локальній мережі	20	20	20
Напад в локальній мережі	0	5	5
Вузли однієї атака локальної мережі	0	10	50
Жертва ЦП частота, (ГГц)	10.33	10.33	10.33
Законні бази даних обслуговування (розмір середнього пакету, біт)	250.7	251.1	272,6
Законні бази даних обслуговування (середній прибуття, швидкість, пакети)	0,010	0,006	0,003
Законні бази даних обслуговування (середній цикл, номер запиту)	910,5	910,5	910,5

Атака служби бази даних (середній розмір пакету, біт)	Не використовується	$1{,}634 \cdot 10^{4}$	$1{,}603 \cdot 10^{4}$
Атака служби бази даних (середнє прибуття, швидкість, пакети)	Не використовується	0,002	0,006
Атака бази даних обслуговування (середній цикл, номер запиту)	$9{,}655 \cdot 10^{5}$	$9{,}655 \cdot 10^{5}$	$9{,}655 \cdot 10^{5}$
Сервіс законної електронної пошти (розмір середнього пакету, біт)	372,0	363.2	383,8
Сервіс законної електронної пошти (середнє прибуття, швидкість, пакети)	0,002	0,002	0,001
Сервіс законної електронної пошти (середній цикл, номер запиту)	$2{,}012 \cdot 10^{5}$	$2{,}012 \cdot 10^{5}$	$2{,}012 \cdot 10^{5}$
Законна служба передачі файлів (розмір середнього пакету, біт)	827,8	715.3	902.4
Законна служба передачі файлів (середнє прибуття, швидкість, пакети)	0,0007	0,0005	0,0001
Законна служба передачі файлів (середній цикл, номер запиту)	$2{,}203 \cdot 10^{6}$	$2{,}203 \cdot 10^{6}$	$2{,}203 \cdot 10^{6}$
Атака файл послуга трансферу (розмір середнього пакету, біт)	Не використовується	$2{,}539 \cdot 10^{4}$	$3{,}270 \cdot 10^{4}$
Атака файл передача обслуговування (середнє прибуття, швидкість, пакети)	Не використовується	0,010	0,003
Атака файл передача обслуговування (середній цикл, номер запиту)	$1{,}868 \cdot 10^{7}$	$1{,}868 \cdot 10^{7}$	$1{,}868 \cdot 10^{7}$
Законна служба веб-перегляду (розмір середнього пакету, біт)	350,0	350,0	350,0
Законна служба веб-перегляду (середнє прибуття, швидкість, пакети)	0,010	0,010	0,004
Законна служба веб-перегляду (середній цикл, номер запиту)	$1{,}701 \cdot 10^{5}$	$1{,}701 \cdot 10^{5}$	$1{,}701 \cdot 10^{5}$
Атака Інтернет перегляд обслуговування (розмір середнього пакету, біт)	Не використовується	350,0	350,0
Атака Інтернет перегляд обслуговування (середнє прибуття, швидкість, пакети)	Не використовується	0,229	0,085
Атака Інтернет перегляд обслуговування (середній цикл, номер запиту)	$1{,}954 \cdot 10^{4}$	$1{,}954 \cdot 10^{4}$	$1{,}954 \cdot 10^{4}$

Ці параметри представляють ситуації, коли жертва не зазнає DDoS-атаки (без атаки) та під час DDoS-атак різного розміру (Атака 1 і Атака 2).

Пропускна здатність виснаження. Цей критерій може бути основним для кіберзлочинців щоб досягти високого рівня виснаження при DDoS-атаці. Саме цей критерій визначає відсоток пропускної здатності, який використовується зловмисниками. Тому можна припустити, що ймовірність атаки нижче 0% використання пропускної здатності рівні до 0% (таким чином вистачатиме пропускної здатность системи для нових запитів користувачів). У випарку збільшення заповненості пропускної здатності або рівності 100% використання ресурсів пропускної здатності, такий відсоток заповненості не даватиме можливості запитів нових користувачів (отдже, успішність атаки буде 100%).

Проаналізована модель використовує різні швидкості надходження пакетів і розміри для різних послуг, тому середня нормальна швидкість надходження пакетів λ_{np} (пакети/с) і середній нормальний розмір пакета v_n (біт) можна отримати за формулами 2.19 і 2.20, а також середню швидкість надходження пакетів атаки λ_{ap} (пакети/с) і середній розмір пакета атаки v_a (біт).

У цих експериментах ми не використовуємо жодної фільтрації, тому атака є законною трафік не буде зменшення через втрату пакети і може бути використовується у формулах 3.6 і 3.7 знайти загальну середню швидкість надходження пакетів λ_{gp} і загальний середній розмір пакета v_g.

У ситуації «без атаки» середня нормальна швидкість надходження пакетів λ_{np} дорівнює 1,724 пакет/с, середній нормальний розмір пакета v_n дорівнює 2727 біт, середня атака пакет прибуття швидкість λ_{an} становить 0 пакетів/с, середній напад розмір пакета v_a становить 0 біт, загальна середня швидкість надходження пакетів λ_{gp} дорівнює 1,7241 пакет/с і загальний середній розмір пакета v_g дорівнює 2727 біт. Використовуючи ці значення для отримання ймовірності втрати пакетів (формула 3.10), ми

отримуємо ймовірність DDoS-атаки з виснаженням пропускної здатності P_B дорівнює 0,047%.

Виконання моделі OPNET IT Guru очікуваного значення використання каналу та зразка означає є 0,070%, поки максимум використання значення є 0,940, в нашому випадку 0,013 і стандарт відхилення є 0,115.

Порівнюючи запропоновану модель і експериментальні результати OPNET (рис. 3.8), наша модель дає меншу ймовірність успіху, ніж очікуваний відсоток використання каналу. Різниця становить -0,023 або -33% від очікуваного зв'язку OPNET використання.

Додавши до досліджуваної ситуації агентів атаки зі збільшеним розміром пакета порівняно з легітимним трафіком (ситуація «Атака 1»), середня нормальна швидкість надходження пакетів λ_{np} дорівнює 1,548 пакет/с, середній нормальний розмір пакета v_n дорівнює 2742 біт, середня швидкість надходження пакетів атаки λ_{an} становить 12,84 пакетів/с, середня атака пакет розмір v_a є 19526 біти, загальний середній прибуття пакету швидкість λ_{gp} є дорівнює 14,39 пакет/с і загальний середній розмір пакета v_g дорівнює 17720 біт. Ймовірність DDoS-атаки зі зменшенням пропускної здатності P_B дорівнює 2,487%, при виконанні моделі OPNET IT Guru очікуване значення використання посилання та середнє значення вибірки становлять 2,841%, тоді як максимальне значення використання становить 6,3196, дисперсія – 1,044, а стандартне відхилення – 1022.

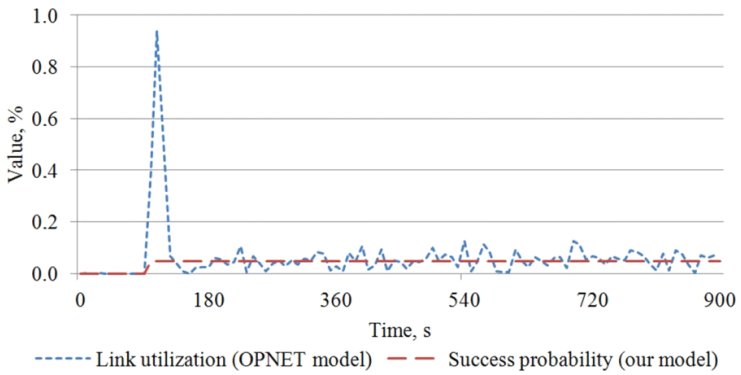


Рис. 3.8. Ймовірність успіху DDoS-атаки, без нападу

Запропонована ймовірність успіху моделі становить 0,388 позиції або 13% менше, ніж спостережуване використання каналу в інструменті OPNET. (Рис 3.9.)

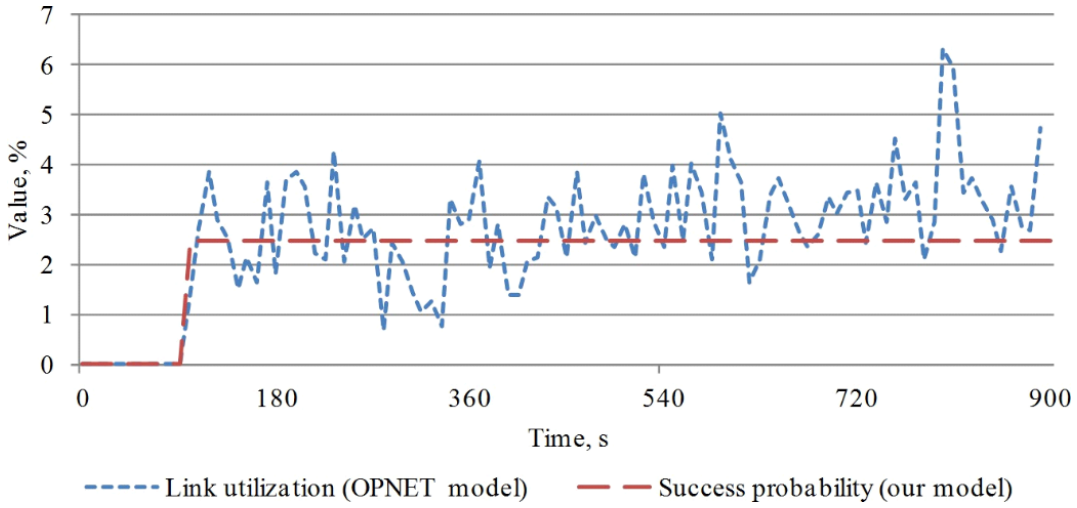


Рис. 3.9. Ймовірність DDoS-атаки, яка буде мати успіх порівняння з ситуацією «Атака 1».

Збільшення потужності атаки до ситуації «Атака 2», середня нормальна швидкість надходження пакетів λ_{np} дорівнює 0,654 пакет/с, середній нормальний розмір пакета ν_{n} дорівнює 2792 біт, середня швидкість надходження пакетів атаки λ_{an} становить 23,62 пакетів/с, середнє напад пакет розмір ν_{a} є 19832 біти, загальний середній пакет прибуття швидкість λ_{gp} дорівнює 24,27 пакет/с і загальний середній розмір пакета ν_{g} дорівнює 19373 біт. Це пропускна здатність виснаження при DDoS-атаці ймовірність P_B рівні до 4,491 % (Рис. 3.10), під час виконання моделі OPNET IT Guru очікуване використання каналу значення та вибіркове середнє становить 4,902 %, тоді як максимальне значення використання становить 8,728, дисперсія — 1,358, а стандартне відхилення — 1,165.

Запропонована ймовірність успіху моделі становить 0,411 позиції або на 8% менше, ніж спостережене використання каналу в інструменті OPNET.

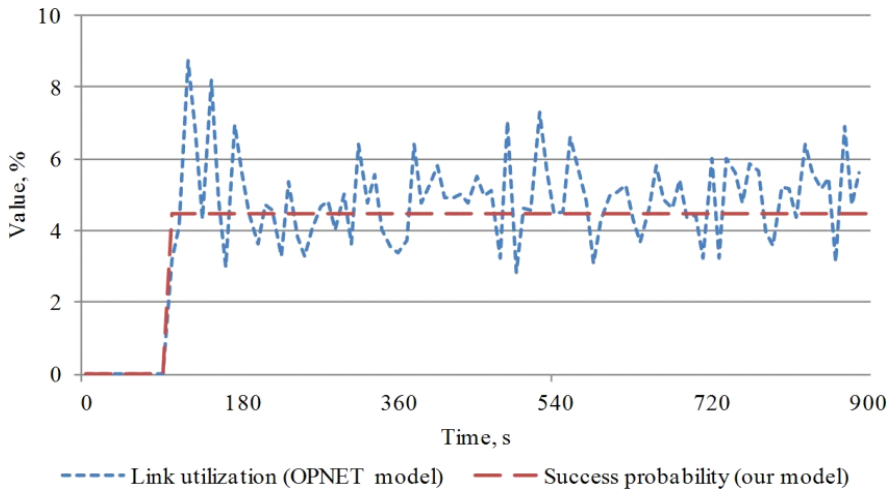


Рис. 3.10. Ймовірність DDoS-атаки, яка буде мати успіх порівняння з ситуацією «Атака 2».

Існує тісний зв'язок між використанням каналу зв'язку та запропонованою нами ймовірністю успішної моделі DDoS-атаки з виснаженням пропускної здатності (рис. 3.11).

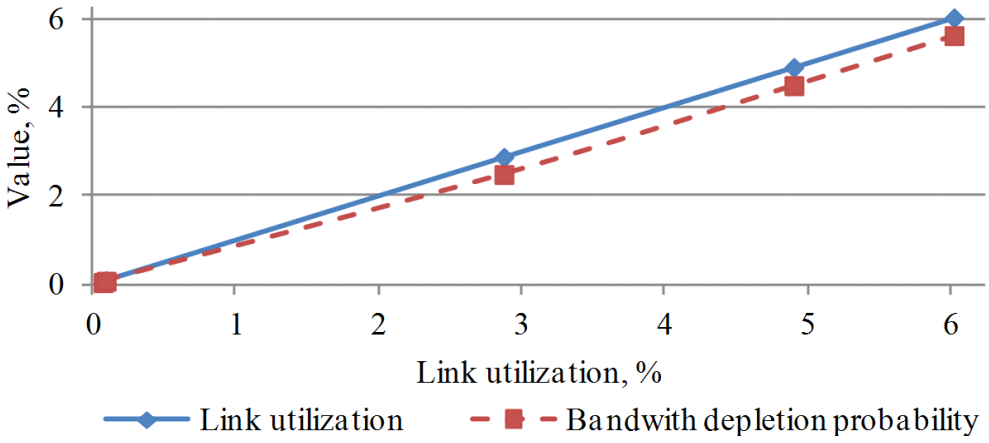


Рис. 3.11. Пропускна здатність виснаження успіху DDoS-атаки, проти використання підсилення

Однак запропонована нами ймовірність успіху атаки з виснаженням пропускної здатності менша, ніж імовірність використання каналу, представленого OPNET. Щоб зробити ці значення близькими один до одного, середній розмір пакета в нашій модель слід додати доп

біти для представлення інтервалів між даними, надісланими через посилання.

Модель виснаження процесора та час обробки

Для оцінки ймовірності успіху DDoS-атаки на роботу процесора наша запропонована модель використовує критичне обмеження часу t_w, і тому ймовірність успіху атаки не є відповідною використанню ЦП. Щоб порівняти запропонований нами результат моделі з результатом, отриманим за допомогою інструменту моделювання OPNET, ми використовуємо середній час обслуговування запиту. Середню кількість циклів для запиту (Таблиця 3.3) було отримано шляхом аналізу завантаження запиту та часу обробки завдання для різних сервісів, а також параметрів процесора жертви.

Середня частота надходження на службову роботу λ_c в системі та середнє число циклів, необхідних для його обробки, c_c вважалися рівними нулю через недоступність щоб змінити цю властивість в інструменті OPNET. Загальна швидкість надходження на роботу λ_{gc} було розраховано шляхом додавання всіх тарифів прибуття для всіх використаних послуг. Середня кількість циклів для загальної обробки завдання c_g розраховувався відповідно до логіки формули (2.20), але з урахуванням усіх використаних послуг, а не легітимних потоків і потоків атак.

Дана обробка запиту часу більше ніж запит швидкості надходження, отже, система знаходиться в стабільному стані, і середній час обслуговування може бути обчислений за формулою (2.22). Розрахований час обробки в нашій моделі більший за отриманий час обробки за OPNET інструментом (Таблиця 3.4), тим не менш, його значення є не більшим ніж максимальне значення часу обробки, отримане із засобу OPNET (рис. 3.12).

Таблиця 3.4.

Запит обробки часу: порівняння із використанням запропонованої моделі та OPNET інструменту

Ситуація / Властивості	Без нападу	Атака 1	Атака 2
наша модель запропоновано час обслуговування запиту, с	$1{,}635 \cdot 10^{-4}$	$6{,}968 \cdot 10^{-4}$	$6{,}926 \cdot 10^{-4}$
OPNET модель середній час виконання завдання, с	$1{,}335 \cdot 10^{-4}$	$4{,}253 \cdot 10^{-4}$	$2{,}815 \cdot 10^{-4}$
OPNET модель максимум час виконання завдання, с	$1{,}011 \cdot 10^{-3}$	$1{,}333 \cdot 10^{-2}$	$4{,}088 \cdot 10^{-2}$
OPNET модель стандарт відхилення часу виконання завдання	$1{,}404 \cdot 10^{-4}$	$2{,}163 \cdot 10^{-3}$	$4{,}466 \cdot 10^{-3}$
OPNET модель дисперсія часу обробки завдання	$2.000 \cdot 10^{-8}$	$4{,}680 \cdot 10^{-6}$	$1{,}995 \cdot 10^{-5}$

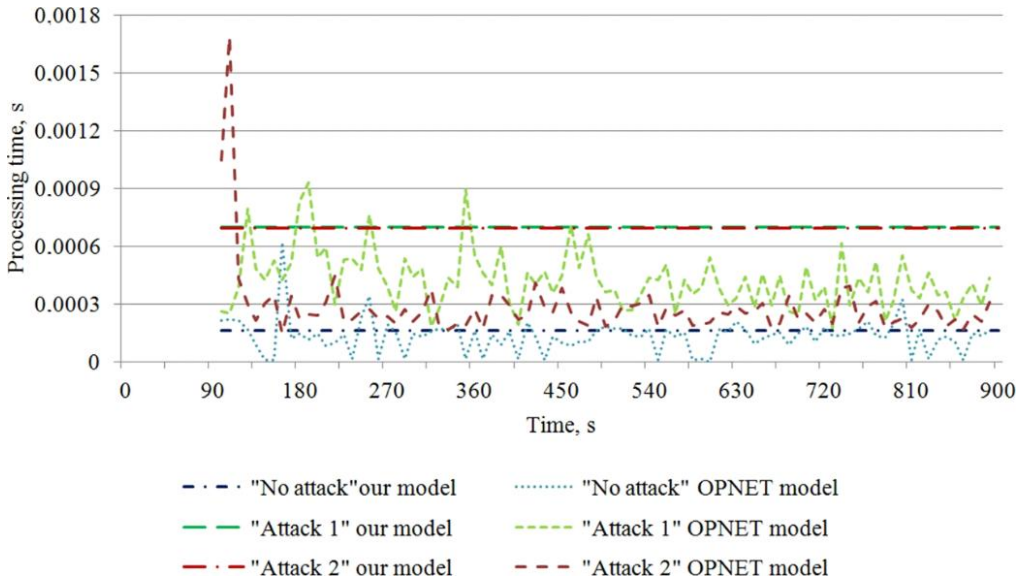


Рис. 3.12. Запит обробки часу: порівняння із використанням запропонованої моделі і OPNET інструменту

За допомогою даного експеременту, запропонована модель показала показники, які вище викладені «Атака 1” та «Атака 2” незважаючи на більші вхідні запити швидкость, очікуваний час обслуговування нашої моделі дуже схожий на час обох ситуацій.

Наша модель DDoS-атаки з вичерпанням пам’яті враховує розмір буфера для зберігання відкритого з’єднання. Зазвичай використовується додатковий буфер, тому ми розглядаємо ці два буфери як один. Однак інструмент моделювання OPNET не відображає використання другого буфера, що ускладнює порівняння нашої моделі з урахуванням відсотка використання буфера.

Для експериментів із моделлю DDoS-атаки на виснаження пам’яті ми аналізуємо різні ситуації, вибираючи службу, щоб мати можливість зберігати від 16 до 64 відкритих з'єднання, додатковий розмір буфера від 4 байт до 100 байт та ін. А також враховуємо загальну середню швидкість приходу сесії λ_{gs}. Ми не використовуємо підроблені джерела DDoS-атак, тому загальний середній час обслуговування t_{gs} отримано з експериментальних моделей OPNET (табл. 3.5).

Для перевірки моделі DoS-атаки з вичерпанням пам’яті ми використовуємо розраховане значення порівняння, яке представляє середню кількість сеансів, обслугованих за одну секунду (формула 11).

Таблиця 3.5.

Експериментальні дані, виснаженням пам'яті під час DDoS-атак

Ситуація Властивості	Ситуація 1	Ситуація 2	Ситуація 3	Ситуація 4
Активний підключення поріг H (сесії)	16	64	32	32
Отримати буфер M (сесії)	64	16	4	100
Загальний інцидент прибуття сесії швидкість λ_{gs} (сеансів/с)	10.86	14.49	5,403	65,25
Загальний середній час обслуговування t_{gs} (s)	1,321	9,926	51.17	32.34
Розраховано значення	0,179	1,798	7,680	15,99
Запит падіння ймовірність $П_{ім}$	$6{,}5\cdot10^{-17}$	0,452	0,870	0,937

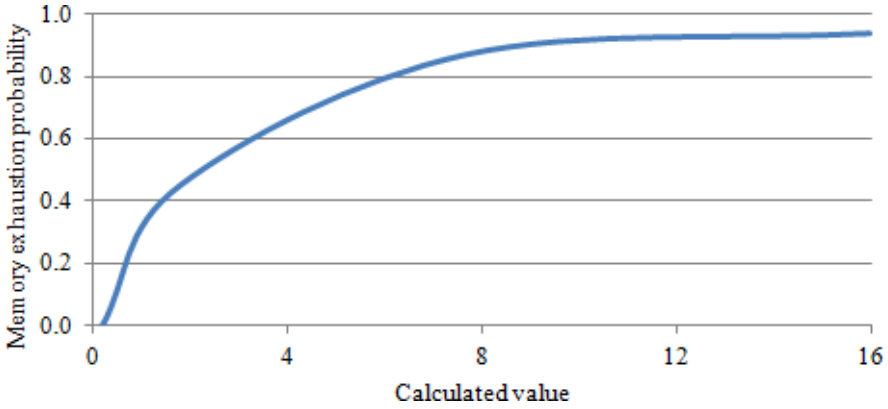


Рис. 3.13. Ймовірність виснаження пам’яті

Порівняння ймовірності виснаження пам'яті та розрахункового значення показало логарифмічним розподілом ймовірності виснаження пам'яті. Він представляє реальну ситуацію, коли збільшення часу обслуговування сеансу не має лінійного впливу на використання буфера та на ймовірність виснаження пам'яті.

Експерименти з модель упередження низькошвидкісних HTTP DDoS-атак, пов’язаної з виснаженням роботи процесора та пам’яті

Моделі виснаження пам'яті та роботи ЦП дозволяють проаналізувати лише деякі частини загальної атаки. Реальна ситуація одночасно включає в себе різні елементи різних моделей. У результаті можна отримати більш точні результати за допомогою комбінованих моделей.

Ми усунули частину виснаження пропускної здатності у формулах (3.1), щоб отримати ймовірність успішної DDoS-атаки, пов’язаної з виснаженням загальної пам’яті та процесора.

Враховуючи ці дві моделі як окремі системи, ймовірність комплексної DDoS-атаки P із виснаженням ресурсів має дорівнювати ймовірності того, що DDoS-атака з виснаженням пам’яті PM або ПК з виснаженням роботи ЦП буде успішною:

$$P = 1 - (1 - P_M) \cdot (1 - P_{CPU}) \quad (3.1)$$

Запити не втрачаються, доки не буде досягнуто пам'яті сховища. Деякі запити можуть бути втрачені через брак місця в буфері. Ті, що мають достатньо місця в пам'яті, обробляються процесором. Оскільки час виконання запиту залежить від характеристик запиту і розміру черги в пам'яті, деякі запити можуть вважатися непотрібними (втраченими), оскільки користувач більше не чекає на них. Ми розглянули загрозу DDoS-атаки з виснаженням пам'яті та процесора як одну систему з двома підсистемами, які тісно залежать одна від одної. Тому ми провели експеримент, щоб дослідити, як постійна швидкість вхідного трафіку впливає на властивості підсистеми пам'яті. Загальна швидкість вхідного трафіку (як легального, так і атакуючого) λ була обрана трохи більшою за максимальний розмір буферу пам'яті M. Властивості моделі та результати експерименту показали, що (незважаючи на те, що інтенсивність вхідного трафіку λ більша за розмір буферу M) вхідний трафік на початку не був настільки великим, щоб обслужити більшість запитів. Це пов'язано з більшим часом обслуговування запитів через характеристики процесора. Однак, середній час обслуговування запитів з часом збільшується (Рис. 3.14.), як і середній розмір черги (Рис. 3.15).

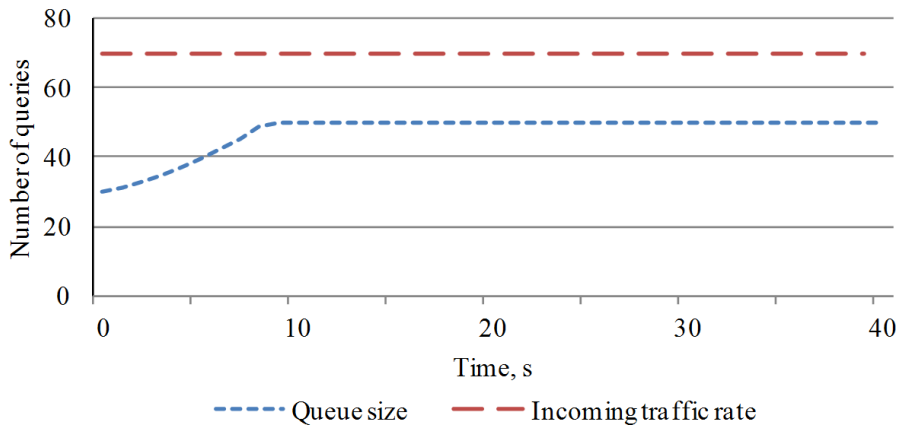


Рис. 3.14. Співвідношення залежность запитів на певному проміжку часу

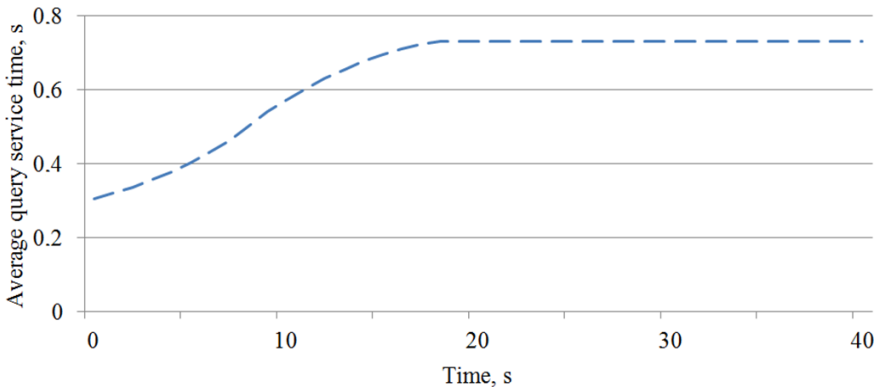


Рис. 3.15. Час обслуговування запитів при перевищенні буферу

Це відбувається через те, що деякі запити обробляються негайно (поки обробляється один запит, може оброблятися інший), а деякі запити залишаються в буфері і чекають свого часу на обробку. Таким чином, зі збільшенням розміру черги збільшується і час обслуговування. Однак, як видно з рисунків 3.14 та 3.15, коли розмір черги залишається постійним, середній час обслуговування запиту продовжує зростати протягом деякого часу. Це може бути пов'язано з тим, що система починає відкидати деякі запити, або з тим, що легальні користувачі більше не чекають на обслуговування певних запитів. Таким чином, процесор починає обробляти непотрібні запити. Однак через деякий час досягається стаціонарний стан і час обслуговування залишається практично незмінним. Зі збільшенням розміру черги та середнього часу обслуговування запитів зростає ймовірність успішної атаки (див. рис. 3.16).

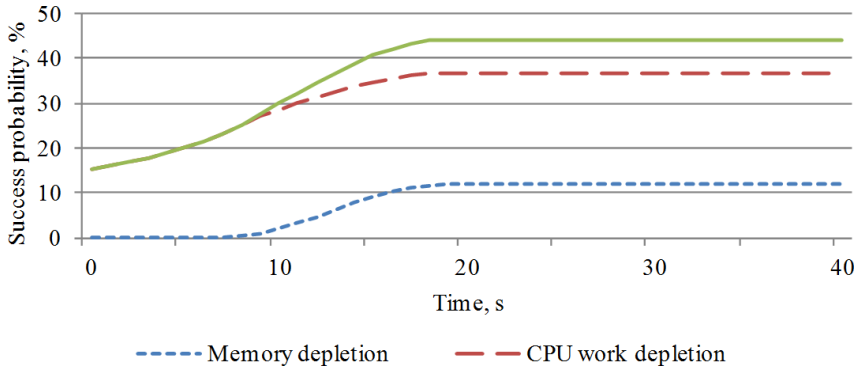


Рис. 3.16. Зміни вірогідності успіху низькошвидкісних DDoS-атак з виснаженням ресурсів, якщо в момент нападу швидкість вхідного трафіку є постійною.

Ймовірність успіху комбінованих атак вища, ніж для будь-якого з компонентів. Рисунок 3.16. показує, що ймовірність успіху низькошвидкісних DDoS-атак, спрямованої на вичерпання ресурсів процесора, корелює з середнім часом обслуговування. Однак залежність між ймовірністю успіху DDoS-атаки на вичерпання пам'яті та середнім розміром черги менш очевидна. На це впливає той факт, що вона залежить як від розміру черги, так і від часу обслуговування.

Другий експеримент було проведено з використанням різних функцій швидкості вхідного трафіку атак. Він досліджував, як змінюються властивості моделі при лінійному збільшенні інтенсивності атакуючого трафіку. При аналізі розміру черги тенденція дуже схожа на випадок постійної інтенсивності атакуючого трафіку, але починається з менших значень (через менший атакуючий трафік) і зростає швидше (Рисунок 3.17.). Однак при аналізі середнього часу обслуговування (Рисунок 3.18.) спостерігається нова тенденція, де середній час обслуговування збільшується на початку, коли швидкість зміни трафіку атак з часом велика, але починає зменшуватися, коли швидкість зміни мала.

Ці експерименти показують, що можна використовувати різноманітні характеристики атаки та функції вхідного трафіку атаки. Ми зосередилися на двох найпоширеніших функціях швидкості атакуючого трафіку, зосередившись на характеристиках атаки виснаження оперативної пам'яті та виснаження процесора.

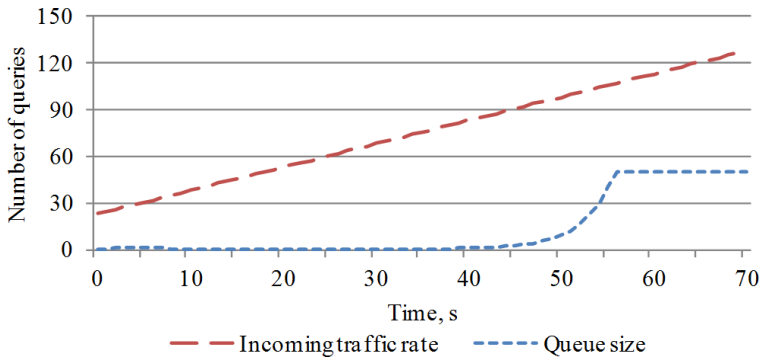


Рис. 3.17. Порівняння швидкості вхідного трафіку з розміром черги під час використання збільшення вхідного трафіку

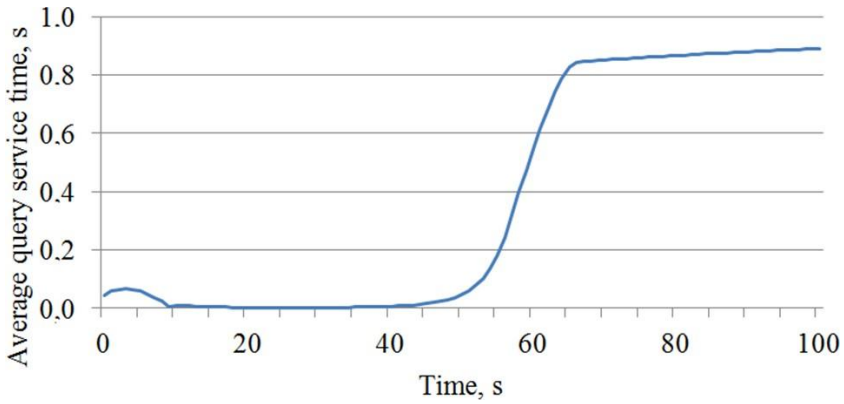


Рис. 3.18. Зміни середнього часу обслуговування під час збільшення швидкості вхідного трафіку

Розмір цього піку на початку атаки залежить від різниці між кількістю разів виконанньь легітимних та атакуючих запитів на центральному процесорі. Цей пік також впливає на ймовірність успіху атаки (Рис. 3.19.).

Моделі виснаження пам'яті та виснаження процесора є підмножинами DDoS-моделі виснаження ресурсів. Однак ці моделі дуже тісно пов'язані між собою і обидві використовують характеристики атаки, отримані одна від одної. Більшість комбінованих характеристик атак на виснаження ресурсів безперервно реагують на зміни вхідного трафіку, але не миттєво. Ці ефекти можуть призводити до різних піків коливань, оскільки розмір черги, час обслуговування або ймовірність успіху атаки змінюються з часом.

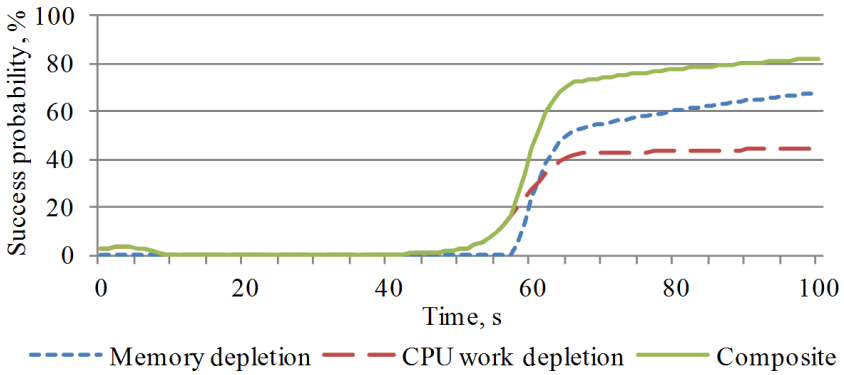


Рис. 3.19. Ймовірність успішної низькошвидкісної HTTP DdoS-атаки з вичерпанням ресурсів відносно часу коли при нападі швидкість вхідного трафіку збільшується

Експерименти з комбінованими моделями низькошвидкісних HTTP DDoS-атак на пропускну здатність та вичерпання пам'яті.

Найпоширенішою ситуацією DDoS-атаки є ситуація, коли атакуючий трафік споживає як пропускну здатність, так і ресурси пам'яті. Ось чому важливо досліджувати моделі низькошвидкісних HTTP DDoS-атак з вичерпанням пропускної здатності та пам'яті, а також характеристики фільтрації системи при аналізі DDoS-атак.

3.4. Експериментальне дослідження системи протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси

Вхідний трафік може бути заблокований через недостатню пропускну здатність. Решта трафіку блокується системою фільтрації опрацьовується та відправляється до блоку навчання моделі ШІ. Якщо ж ємності буфера для зберігання відкритих з'єднань недостатньо пакети можуть відкидатися.

Щоб представити повну ймовірність атаки, ми модифікуємо формулу 3.2, щоб додати ймовірність фільтрації законного трафіку P_{Fn}:

$$P = 1-(1-P_B)\cdot(1-P_{Fn})\cdot(1-P_M) \quad (3.2)$$

Запропонована модель упередження ниськошвидкісних DDoS-атак була використана для тестування різних ситуацій. Метою цих експериментів було визначити вплив різних характеристик атаки на успішність низькошвидкісних HTTP DDoS-атак. Для аналізу цих експериментів були обрані стандартні ситуаційні параметри:

- стабільний трафік 20 Мбіт/с (100 запитів в секунду по 200 біт кожен).

- атакуючий трафік 10 Мбіт/с (50000 запитів в секунду по 200 біт кожен).

- канал з пропускною здатністю 100 Мбіт/с.

- фільтрує 20% атакуючого трафіку і 2% легального трафіку.

- легітимні запити виконуються за 200 мс.

- атакуючі запити виконуються за 2000 мс. Буфер може зберігати інформацію для 50 з'єднань.

Ці атаки та параметри жертви призвели до вичерпання пропускної здатності на 8,7%, фільтрації легальних запитів на 2% та вичерпання пам'яті на 39,3%. Комбінована DDoS-атака мала ймовірність успіху 45,7%. Зміна характеристик фільтрації показує, що ймовірність блокування легітимних запитів є дуже важливою і лінійно збільшує ймовірність успіху комбінованої DDoS-атаки. З іншого боку, фільтрація атакуючого трафіку змінює пам'ять та ймовірність комбінованої DDoS-атаки нелінійно (рис. 3.21.).

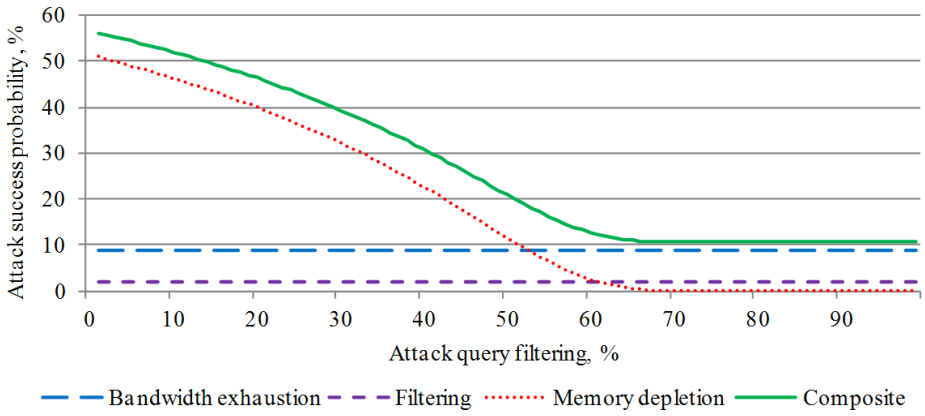


Рис. 3.21. Фільтрація запитів атак на рахунок вичерпання пропускної здатності

Аналогічна тенденція спостерігається і щодо впливу часу обслуговування на успішність атаки. Зі збільшенням середнього часу обслуговування (нормального та атакуючих запитів) ймовірність вичерпання пам'яті зростає, але вплив на комбінований показник успішності атаки не є пропорційним (рис. 3.22.).

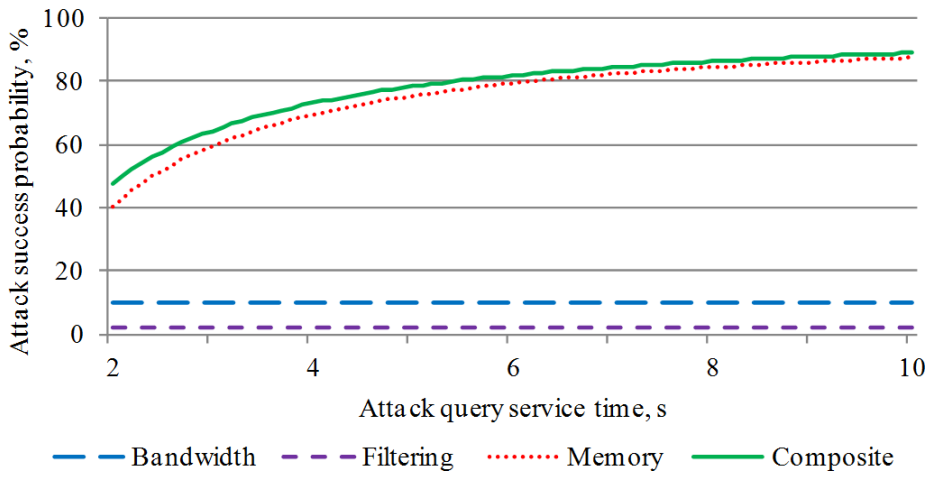


Рис. 3.22. Успішність атаки при збільшенні середнього часу обслуговування

У попередніх експериментах змінювали лише ймовірність виявлення пам'яті та комбінованої атаки. Однак відмінності в характеристиках трафіку також впливають на ймовірність вичерпання пропускної здатності. З підвищенням нормальної та інтенсивності атаки ймовірність успіху атака зростає, але в нашому експерименті підвищення ймовірності вичерпання пропускної здатності не така значна, як ймовірність вичерпання пам’яті (див. Рис. 3.23.). Вичерпання пропускної здатності має незначний вплив на час безвідмовної роботи, якщо трафік атаки досяг певного рівня; вплив ймовірності виснаження пам'яті зростає з трафіком атаки. Для великих потоків стає досить чутливим до масштабів атаки (див. Рис 3.24).

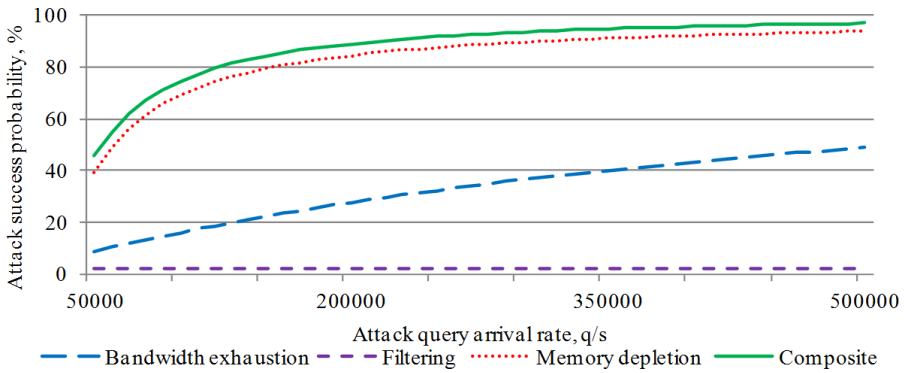


Рис. 3.23. Ймовірність успіху атаки, залежність від частоти надходження запитів до середнього часу обслуговування

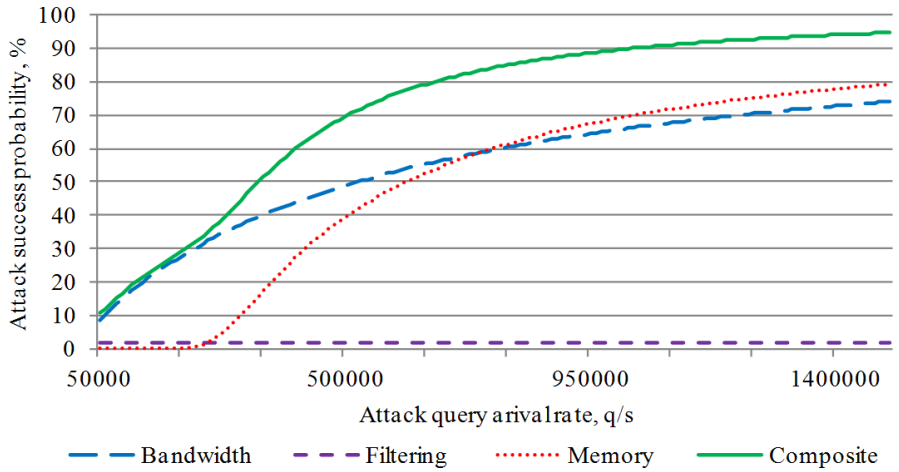


Рис. 3.24. Ймовірність успіху атаки, залежність від прибуття пакетів до короткого часу обслуговування

Ці експерименти показали, що на успішність низькошвидкісних HTTP DDoS-атак можуть впливати різні складові або комбінація різних параметрів атаки і жертви. Використовуючи цю модель, можна виявити деякі факти про ймовірність успіху низькошвидкісних HTTP DDoS-атак:

- погано налаштовані системи фільтрації можуть завдати більшої шкоди, ніж сама DDoS-атака.

- атаки на вичерпання пам'яті більш чутливі до змін у вхідному трафіку, що може бути основною причиною високої комбінованої ймовірності успіху атаки.

- зміна значень атрибутів DDoS-атаки та жертви має нелінійний вплив на ймовірність успіху атаки, а також на комбіновану ймовірність успіху низькошвидкісних HTTP DDoS-атак.

Експерименти з моделями при низькошвидкісних HTTP DDoS-атаках з вичерпанням пропускної здатності, та додатковими особливостями.

Можна виділити три основні категорії протидії DDoS-атакам [133]: захист від атаки (зазвичай збільшення ресурсів), зменшення наслідків атаки (зазвичай фільтрація атакуючого трафіку) та захист після атаки (зазвичай моніторинг джерел атаки). Зусилля по боротьбі з DDoS-атаками

будуть успішними, якщо принаймні один з цих трьох елементів буде достатньо сильним. Знаючи ймовірність захисту від атаки P_{pr}, ймовірність зменшення наслідків атаки P_{mt} та ймовірність запобігання після атаки P_{pv}, можна визначити комбіновану ймовірність стійкості після DDoS-атаки P_s:

$$P_s = 1 - \left(\overline{P_{pr}} \cdot \overline{P_{mt}} \cdot \overline{P_{pv}} \right) \tag{3.3}$$

Ймовірність атаки. Упередження DDoS-атак поєднує в собі всі методи і способи, які допомагають відстежити джерело атаки. Ймовірність успіху упереджень P_{pv} залежить від ймовірності P_{ta} відстеження організаторів атаки, а також залежить від типу DDoS-атаки і типу управління ботнетом. Ця ймовірність також змінюється з часом. Це пов'язано з тим, що відстежити зловмисника легше, коли атакуючий агент активний, а ймовірність відстеження зменшується, коли агент ботнету зникає (коли агент вимикається або видаляється з ботнету). Таким чином, часова ймовірність відстеження зловмисника для агента ботнету P_{ta} - це ймовірність відстеження зловмисника, який аналізує активного агента pta, коли час t менший за середній час життя агента T_w, і ймовірність відстеження агента, який не існує, в іншому випадку. Ймовірність відстеження зловмисника, який аналізує P_{tn}, повинна дорівнювати ймовірності відстеження зловмисника, який аналізує P_{ta}:

$$P_{Ta}^{(t)} = \begin{cases} P_{ta} & , t < T_w \\ P_{tn} & , t \geq T_w \end{cases} \tag{3.4}$$

$P_{Ta}^{(t)}$ представляє ймовірність того, що атаку можна відстежити, проаналізувавши лише одного агента ботнету. DDoS-атаки, з іншого боку, мають велику кількість агентів. Деякі з них активні постійно, тоді як інші з часом стають неактивними. Тому ймовірність відстеження P_{ta} організатора атаки повинна дорівнювати ймовірності того, що хоча б один

проаналізований агент веде до фактичного організатора атаки. У той час як дослідники-люди можуть проаналізувати лише невелику частину атакуючих агентів за один проміжок часу, комп'ютерні системи можуть аналізувати величезну кількість джерел даних одночасно. Тому кількість активних $nt < tw(t)$ and already not existing $nt >= tw(t)$ проаналізованих агентів ботнету з моменту початку DDoS-атаки допомагає знайти загальну ймовірність відстеження організаторів атаки:

$$P_{TA}^{(t)=1} - \bigcap_{k=1}^{n} P_{Tak}(t_k) = 1 - \left(1 - P_{ta}\right)^{n_{t<tw}(t)} \cdot \left(1 - P_{tn}\right)^{n_{t\geq tw}(t)} \tag{3.5}$$

На етапі розтину ймовірності, що зловмисників відстежують шляхом одночасного аналізу атакуючих агентів. Також важливо враховувати відношення обсягу атакованих запитів до всіх вхідних запитів $\rho_{n^{(t)}}$ (див. формулу 3.6). Цей коефіцієнт допомагає відобразити складність визначення того, які запити є легітимними (не дають результатів відстеження або дають хибні результати), а які є атакуючими (дають результати відстеження), і оцінює справжню ймовірність відстеження зловмисника, і саме його слід використовувати для цього.

$$\rho_{n^{(t)}} = \frac{\sum n_a(t)}{\sum n_a(t) + n_n \cdot t} \tag{3.6}$$

Також слід враховувати час t_{tr}, необхідний для успішного відстеження:

$$P_{pv}(t) = \begin{cases} P_{TA}(t) \cdot \dfrac{t}{t_{tr}} \cdot \rho_n(t) & , t < t_{tr} \\ P_{TA}(t) \cdot \rho_n(t) & , t \geq t_{tr} \end{cases} \tag{3.7}$$

Ймовірність пом'якшення наслідків атаки

На етапі пом'якшення наслідків DDoS-атаки робиться спроба зменшити ефект DoS під час атаки. Зазвичай для фільтрації атакуючого трафіку використовуються різні фільтри. Тому ймовірність пом'якшення наслідків DDoS-атаки залежить від частки легітимного трафіку в загальному трафіку, спрямованому на жертву (3.8). Тут частка легітимних запитів, що фільтруються P_{fns}, і атакуючих запитів, що фільтруються P_{fps}, так само важлива, як і трафік легітимних T_n і атакуючих T_a в цей час.

$$P_{mt}(t) = \frac{T_n \cdot (1 - P_{fps})}{T_a \cdot P_{fns} + T_n} \tag{3.8}$$

Легальний трафік (див. Рівняння 3.9) і трафік атак (див. Рівняння 3.10) можна визначити як середній розмір запиту для типів запиту, помножений на кількість вхідних запитів у цей час.

$$T_n(t) = \lambda_{np} \cdot \nu_n \cdot n_n(t) \tag{3.9}$$

$$T_a(t) = \lambda_{ap} \cdot \nu_a \cdot n(t) \tag{3.10}$$

Швидкість отримання запитів від легальних користувачів вважається постійною, і ми не вдаємося в подробиці того, як активність легальних користувачів впливає на успіх DDoS-атак. Однак, необхідна більш детальна статистика щодо представлення трафіку легальних користувачів (Noreika and Drąsutis 2007). З іншого боку, велике значення мають зміни в обсязі атак агента-зловмисника в певний момент часу. Ми спробували дослідити, як різні стратегії вербування агентів та характеристики агентів впливають на ефективність ймовірності виживання під час DDoS-атаки: для опису кількості агентів в DDoS-атаці ми розглядаємо наступні характеристики:

- початкова кількість агентів при атаці n_{in};
- середній час життя одного агента t_{alt};

- час розподілу атакуючих агентів t_{arr} ;
- додаткова функція розподілу агентів (описує, скільки агентів додається в атаку в кожен момент часу) $n_r(t)$;

Всі ці властивості описують, якою є кількість атакуючих агентів $n(t)$ у певний момент часу:

$$n(t)=\begin{cases} n_{in} & ,t=0 \\ n(t-1)+n_r(t) & ,t<t_{arr} and\ t\le t_{alt} \\ n(t-1)+n_r(t)-n_r(t-t_{alt}) & ,t<t_{arr} and\ t>t_{alt} \\ n(t-1)-n_r(t-t_{alt}) & ,t\ge t_{arr} and\ t>t_{alt} \\ n(t-1) & ,t\ge t_{arr} and\ t\le t_{alt} \end{cases} \quad (3.11)$$

Імовірність попередження DDoS. Захист від атак може поєднувати в собі багато дій, але в даному випадку нас цікавить лише те, наскільки жертва готова контролювати виснаження ресурсів. Тому ми обчислюємо ймовірність втрати всіх запитів і використовуємо величину, обернену до ймовірності втрати одного запиту:

$$P_{pr}(t)=1-P_{mt}(t)=1-\frac{\frac{\rho(t)^i}{i!}}{\sum_{j=0}^{i}\frac{\rho(t)^j}{j!}} \quad (3.12)$$

У цьому рівнянні i означає кількість відкритих каналів, пропускна здатність усіх каналів (використовується для множення пропускної здатності) - T_g , а $\rho(t)$ - коефіцієнт використання пропускної здатності:

$$\rho(t)=\frac{T_a(t)\cdot P_{fns}+T_n(t)\cdot(1-P_{fps})}{T_g\cdot i} \quad (3.13)$$

Дослідження стратегій розгортання ботнет-агентів у DDoS-атаках.

Запропонована модель дозволяє проаналізувати ймовірність виживання DDoS-атаки та її компонентів при різних конфігураціях жертв і бот-мереж. Для аналізу ефективності стратегії розподілу агентів ботнету було змодельовано приклад, що відповідає стандартній ситуації. Жертва використовує систему фільтрації, яка відфільтровує в середньому 2% і 30% атакуючого трафіку з 1 МБ/с легального трафіку (40 запитів розміром 25 КБ в секунду). Ботнети та DDoS-атаки організовані таким чином, що знання одного агента атаки дає 0,3% шансів відстежити організатора атаки, і це займає одну годину в рамках завдання, де всі агенти атаки аналізуються одночасно. Жертва використовує один канал пропускною здатністю 5 МБ/с. Для атаки на жертву використовуються чотири функції рекрутування агентів $nr(t)$:

a) під час атаки агентів не виділяється - $nr(t) = 0$;

b) постійна швидкість виділення агентів - $nr(t) = 12$;

c) швидкість виділення агентів лінійно зростає - $nr(t) = 0.04 \cdot t$;

d) швидкість виділення агентів лінійно зменшується - $nr(t) = 20 - 0.0267 \cdot t$.

Якщо до атаки вчасно не залучаються додаткові агенти, то початкова кількість агентів дорівнює 7288, у всіх інших випадках - 100 агентів. 1 агент може відправити жертві в середньому 25 КБ/с трафіку. до жертви, а час його життя становить 5 хвилин.

Розподіл агентів триває 10 хвилин, що означає, що кожна стратегія розподілу агентів використовує однакову кількість агентів (7288). Запропонована модель дозволяє проаналізувати, як змінюється кількість агентів в атаках з використанням різних стратегій розподілу агентів. Вона також дозволяє оцінити, як середній час життя агентів впливає на потужність DDoS-атаки. Аналізуючи чотири обрані нами стратегії розподілу агентів (див. Рис. 3.25).

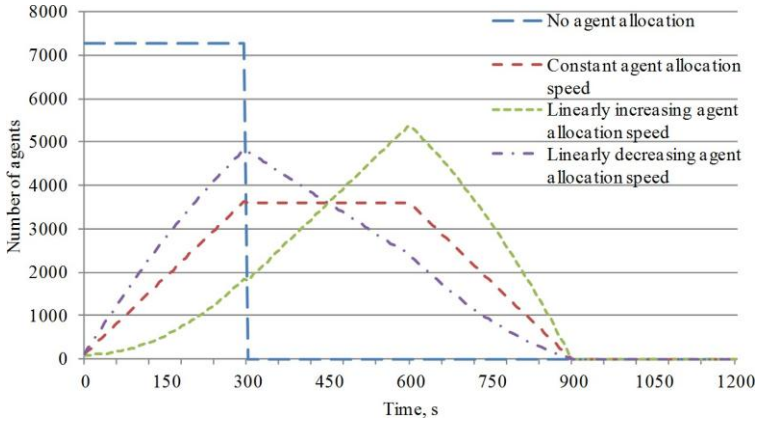


Рис. 3.25. Зміни кількості агентів в DDoS-атаці коли використовуються різні стратегії вербування агентів

За зображення ми бачимо, що за допомогою однієї і тієї ж кількості агентів можна досягти дуже різних варіацій потужності атаки, розподіляючи їх по-різному протягом певного періоду часу:

- підтримуючи швидкість розгортання постійною, можна проводити атаки протягом тривалих періодів часу, незалежно від часу життя агентів, але з особливо малою силою атаки.

- якщо швидкість розміщення агентів збільшується або зменшується лінійно, сила атаки постійно змінюється (збільшується, досягає піку, а потім зменшується) і не може бути стабільною протягом тривалого періоду часу.

Аналізуючи зміну кількості агентів в DDoS-атаці, можна зробити висновок, що максимальна потужність DDoS-атаки може бути досягнута в різні моменти або інтервали атаки. Тому було досліджено ефективність DDoS-атак через різні проміжки часу після ініціації атаки (табл. 3.6). Ефективність DDoS-атаки незалежно від часового інтервалу після ініціації атаки показує, що максимальна ефективність досягається на початковому етапі, коли кількість миттєвих агентів велика. Однак, коли жодного агента не розгорнуто, ефективність DDoS-атаки знижується дуже швидко порівняно з іншими проаналізованими стратегіями.

Таблиця 3.6.

Порівняння з DDoS ефективність в різні часові інтервали і використання різних стратегій розподілу агентів.

Агент стратегія розподілу	Атака успіх ймовірність, %			
	в середині атаки, 300 с	на кінець виділення агента, 600 с	на кінець формування потоку атаки, 900 с	Після закінчення атаки, 1500 с
Немає агентів виділення	91.2	45.7	30.6	18.5
Постійний розподіл агента	75.2	77.5	72,0	43.3
Лінійне збільшення виділення агента	54.7	67,0	67,0	40.3
Лінійно зменшення виділення агента	80.2	79.9	70.2	42.2

Коли кількість використовуваних агентів залишається постійною, досягається не тільки найбільш стабільна ефективність атаки протягом різних часових інтервалів, але й максимальна ефективність атаки під час тривалих періодів часу (якщо після закінчення атаки не відбувається ніякої подальшої діяльності). Однак лінійна варіація заданої швидкості розподілу агентів дає схожі результати, за винятком того, що різниця в стабільній ефективності атаки в часі є більшою. Аналіз еволюції ймовірності виживання атаки з часом при зміні поточної стратегії розподілу агентів показує, що ймовірність виживання атаки експоненціально зменшується при лінійному збільшенні трафіку атаки, в той час як ймовірність виживання атаки експоненціально збільшується при зменшенні трафіку атаки (Рис. 3.26, 3.27, 3.28).

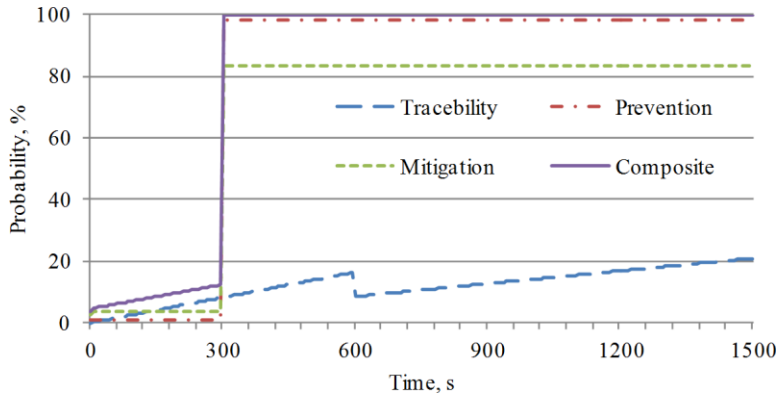


Рис. 3.26. Імовірність низькошвидкісних HTTP DDoS-атак при простежуванні без використаних агентів

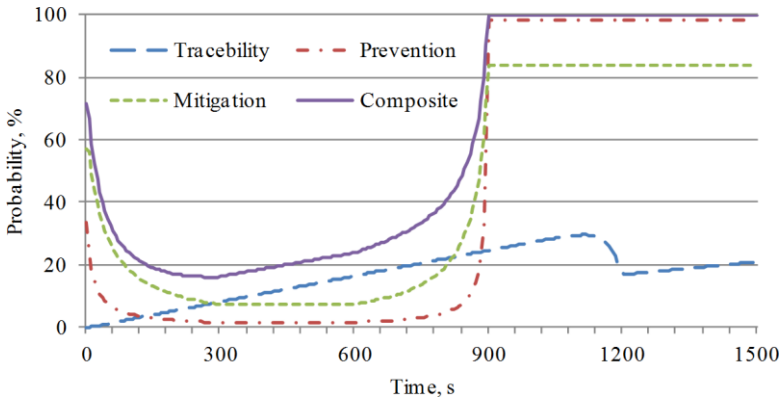


Рис. 3.27. Низькошвидкісна HTTP DdoS-атак, при простежуванні при додаванні постійної кількості агентів щосекунди

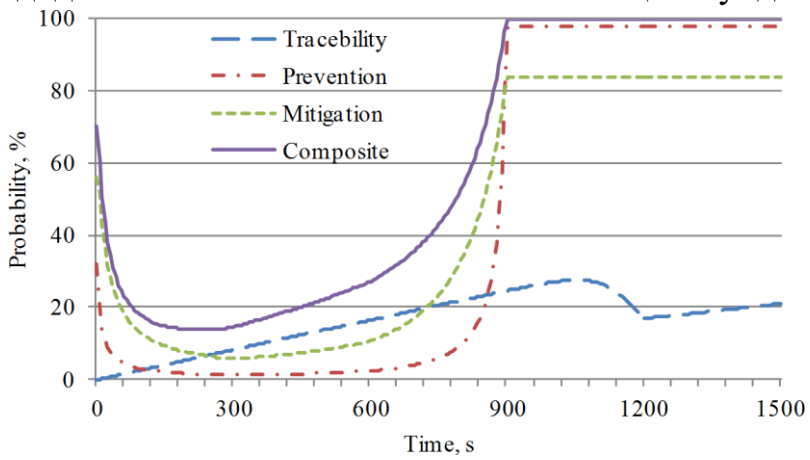


Рис. 3.28. Імовірність вчасного реагування на низькошвидкісну HTTP DDoS-атаку

Дослідження також показало, що імовірність виживання майже повністю залежить від ймовірності запобігання. Однак при аналізі цього та інших випадків виявляється, що ймовірність пом'якшення наслідків може

домінувати. Насправді, ймовірність виживання після запобігання настільки мала, що виживання не є основним компонентом DDoS-атаки. Однак загальна ймовірність виживання може зростати на пізніх стадіях атаки: Порівнюючи зміни ймовірностей запобігання, усунення наслідків та пост-відповіді під час DDoS-атаки, можна помітити, що подібність між запобіганням та усуненням наслідків є абсолютно разючою, тоді як зміни ймовірності пост-відповіді є зовсім іншими. Це можна пояснити тим, що ймовірність запобігання та усунення атаки майже повністю залежить від вхідного трафіку. Однак, хоча вхідний трафік і впливає на ймовірність після перехоплення, він не настільки важливий, як характеристики фільтрації або час, що минув з моменту початку атаки.

Це дослідження надає можливість зрозуміти, що ймовірність запобігання та пом'якшення наслідків атаки набагато більше залежить від трафіку атаки, ніж ймовірність наслідків після атаки. Тому спроби вжити контрзаходів, спрямованих на ефективне відстеження джерела атаки, слід робити лише на ранніх стадіях атаки, якщо є ймовірність того, що атака триватиме довго.

Стратегії розподілу агентів ботнету впливають на часові зміни в динаміці атакуючого трафіку, відповідно, визначаючи потужність атаки та ефективність часових змін. Тому очікуваний прогрес атаки можна оцінити, проаналізувавши, як змінюється атакуючий трафік на початку атаки.

Було проведено ряд експериментів, щоб оцінити діяльність системи. Експеримет відбувався без задіяння системи безпеки, яка фактично заповнювала веб-сервер пакетами TCP SYN. Та з системою безпеки, де було попітне фільтрування трафіку.

Моделювання власної мережі, все підключення відбувалось за допомогою 16-портового комутатора, веб-сервера та 15 машин, які використовувалися як зловмисники, або клієнти. Модель комутатора —

16-портовий гігабітний комутатор Cisco Linksys SR2016T-EU 10/100/1000 (SR2016T-EU) [13, 122].

16 портів перемикаються зі швидкістю 32 Гбіт/с. Пропускна здатність становить 23,8 млн пакетів в секунду.

Конфігурація хостів (клієнтів і зловмисників) взаємодія з HTTP-сервером.

Процесор: Intel® Celeron® 2,00 ГГц

Частота процесора: 2,00 ГГц

Оперативна пам'ять: 512 Мб

Мережева карта: 100 Мбіт/с Ethernet

ОС: CentOS Linux версія 6.0; Linux версія 2.6.32-71.29.1.el6.i686 gcc версія 4.4.4 20100726 (Red Hat 4.4.4-13)

Рисунок 3.29., топологія експериментальної мережі. Він містить атакуючі хости, веб-клієнти та веб-сервери, пов’язані з комутатором Cisco. Дана схема візуально допомагає зрозуміти розміщення та зв'язок між елементами побудованої системи. Для кращого розуміння виникнення мережевих атак.

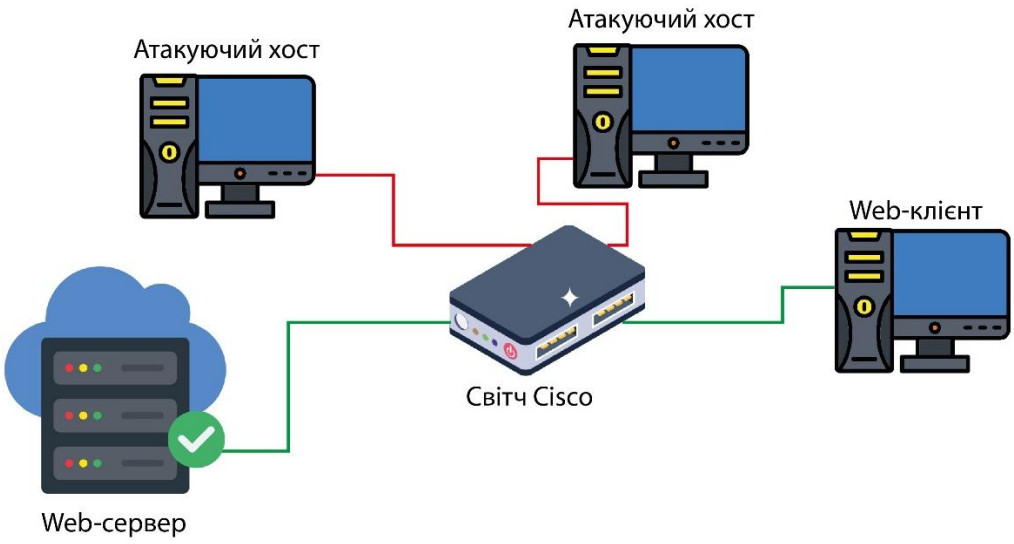


Рис. 3.29. Топологія експериментальної мережі

Щоб виміряти вхідний і вихідний трафік, було інстальовано та застосовано програму IPTraf на веб-сервері. Він підраховував пакети трафіку в пакетах за секунду (пакетів/сек). Трафік, зафіксований IPTraf, пульсує, тому в таблиці показано середнє значення. Комп'ютери, які є хостами-атаками, генерують пакети TCP SYN. Таким чином вони імітують SYN-флуд. Ось використана команда. А при запуску з одного хоста (без систем захисту) реєструється веб-сервер, який використовує 47 тисяч пакетів у секунду. Він може відповісти лише на 11 тисяч пакетів за секунду. Це свідчить про те, що система має ресурс, щоб відповісти менше ніж на кількість отриманих запитів. Коли виявлено атакуючих два хости, у сервера знову закінчуються ресурси — в результаті сервер бере 32 КБ і повертає 7 КБ. Це свідчить про те, що системний ресурс вичерпано, атака досягла своєї мети TCP SYN flood (DDoS-атака). Під час використання системи захисту використовується параметр «розмір черги напіввідкритого підключення», тобто: net.ipv4.tcp_max_syn_backlog (B) зі значенням для замовчування 1024 B. Коли при фільтруванні законного трафіку це значення повинно забезпечувати найкращу якість обслуговування для певного клієнта в секунду, наприклад, 400.

Таблиця 3.7

Вплив параметра розміру черги на напіввідкриті з’єднання

Розмір черги напіввідкритого з’єднання	1024	2048	4096	8191
пакети вхідного трафіку/с	16000	20000	25000	25000
пакети вихідного трафіку/с	4400	5000	5500	5500

Якщо при заповненні пакетами збільшити буфер, тоді система може обробляти більше трафіку, тобто матиме більше ресурсів, щоб протистояти атаці, і фактично вдасця збільшити кількість обслуговуваного трафіку.

В ході експерименту було збільшено об’єм буферу на 4096 і 8192, після чого можна зробити висновок, що система справляється з вхідними пакетами трафіку, одже більше не потрібно збільшувати буфер (табл. 3.7).

Тому пізніше було обрано значення.

net.ipv4.tcp_max_syn_backlog=4096.

Під час використання захисту враховуйте параметри net.ipv4.tcp_synack_retries. Він контролює кількість повторних передач, встановлюючи час збереження напіввідкритих з’єднань у буфері. За замовчуванням встановлено 5 відліків, що означає видалення напіввідкритого з'єднання через 3 хвилини. Дані наведені в таблиці 3.8.

Таблиця 3.8

Вплив параметра tcp_synack_retries на час передачі
та повний час напіввідкритих з’єднань

tcp_synack_retries значення, кількість	Час повторної передачі t, с	Загальний час зберігання напіввідкритих з'єднань у черзі, с
1	на 3-й секунді	9 секунд
2	на 3-й і 9-й секундах	21 секунда
3	на 3, 9 і 21 сек.	45 секунд
4	3-та, 9-та, 21-ва, 45-та сек.	90 секунд
5	3-та, 9-та, 21-ва, 45-та, 90-та	180 секунд

Таблиця 3.9

Контроль кількість повторних передач

Параметр кількості повторних передач	5	4	3	2	1
пакети вхідного трафіку/с	21000	22000	23000	24000	25000
пакети вихідного трафіку/с	4500	4650	4800	5000	5500

Зміна проведено таким чином, що передача реалізується на третій секунді, а загальний час утримання напіввідкритих з’єднань у черзі

становить 9 секунд. Коли заповнити пакети та зменшити кількість повторних передач, що призвело до скорочення часу утримання напіввідкритих з'єднань у черзі, тоді система здатна обробляти більше трафіку. Тому значення net.ipv4.tcp_synack_retries=1 вибирається пізніше. Дані наведені в табл. 3.9.

Під час експерименту було виявлено, що сервер виходить з ладу будь-якої форми захисту, якщо 7 хостів запустять свою атаку, і за допомогою певних стандартних системи він залишиться непрацездатним, навіть якщо всі 15 машин будуть атаковані. Дані експерименти, проведені для створення генерування вхідного та вихідного трафіку веб-сервера без системи захисту, наведені в табл. 3.10, діаграму допустимого та вхідного трафіку можна побачити на рис. 3.30.

Таблиця 3.10

Генерування вхідного і вихідного трафіку веб-сервера без системи захисту

Штурмові машини відсутні	Пакети вхідного трафіку/с	Пакети допустимого трафіку/с
1	47000	11000
2	32000	7000
3	30000	6000
4	28000	5000
5	25000	4000
6	22000	3000
7	17000	1000
8	10000	900

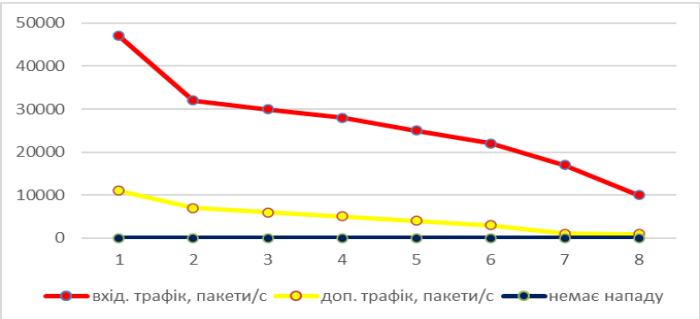


Рис. 3.30. Генерування пакетів вхідного та допустимого трафіку веб-сервера, без системи захисту

Дані експериментального виявлення генерування вхідного і вихідного трафіку веб-сервера з системою захисту наведено в табл. 3.11, діаграму пакетів допустимого та вхідного трафіку представлено на рис. 3.31.

Таблиця 3.11

Генерування вхідного та вихідного трафіку веб-сервера з використанням системи захисту

Штурмові машини відсутні	Пакети вхідного трафіку/с	Пакети допустимого трафіку/с
1	25000	5500
2	19000	3600
3	17000	3500
4	16000	3400
5	14500	2500
6	13000	1550
7	9800	1200
8	9400	1100
9	8600	900
10	8000	850

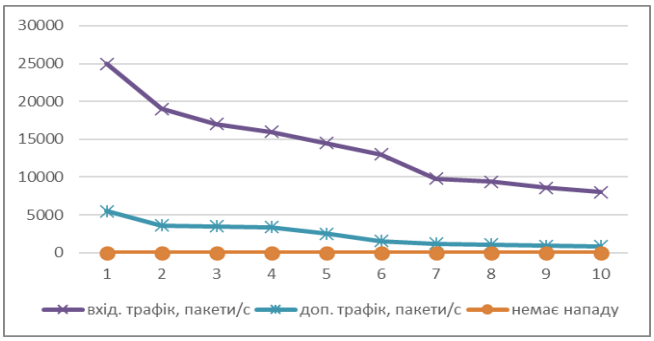


Рис. 3.31. Генерація вхідного і вихідного трафіку веб-сервера з використанням системи захисту

Класифікація DoS-атак, запропонована Я. Мірковичем, охоплює найбільшу кількість категорій, а наша таксономія має найнижчий рівень категорій. Однак, експерименти з використанням нашої таксономії DoS-атак демонструють, що запропонована таксономія підходить для безперервних DoS-атак: в середньому в нашій таксономії виділено на 8,6% більше категорій, ніж в таксономії, запропонованій J.Mirkovich. Наші результати підтверджують, що найбільш важливими характеристиками

класифікації низькошвидкісних HTTP DDoS-атак є не кількість властивостей, а їх структура та чіткість.

Аналіз існуючих таксономій DoS- та DDoS-атак показав, що вони, як правило, використовують імовірнісні елементи для опису випадковості інтернет-трафіку було показано, що це дійсно так. З 21 проаналізованої моделі лише сім не використовували імовірнісні уявлення, і всі вони були введені до 2007 року. Це свідчить про те, що агентні моделі не можуть точно відображати величезну кількість даних про DDoS-атаки і що замість них слід використовувати імовірнісні моделі.

Комбінована ймовірність успіху DDoS-атаки - це ймовірність того, що легітимний запит користувача буде втрачено принаймні в одному з компонентів моделі (3. ймовірність того, що легітимний запит користувача буде втрачено (або заблоковано в моделі виснаження пропускної здатності, пам'яті або роботи процесора) принаймні в одному з компонентів моделі. Це надає моделі гнучкості та масштабованості. Таким чином її можна застосовувати для нових типів низькошвидкісних HTTP DDoS-загроз.

Експерименти в локальній мережі не містять у собі всі особливості DDoS-атаки, і інформація після виникнення маштабних DDoS-атак не завжди є чіткою. Тому для перевірки запропонованої моделі DDoS-атаки було застосовано інструмент моделювання OPNET. Ця перевірка підтвердила, що дані моделі схожі на результати моделювання OPNET. Отже, запропоновану модель DDoS-атаки можна використати для оцінки теоретичної ймовірності успішних атак [120, 121, 135, 136].

Врахувавши всі попередні дослідження були проведені корегування та налаштування системи протидії низькошвидкісним DDoS-атакам. Де враховувались особливості саме низькошвидкісних DDoS-атак. За допомогою методу раннього виявлення, моделі упередження та модулю виснаження пам’яті при DDoS-атаці вдалося досягти наступних результатів, див рис. 3.32 та 3.33.

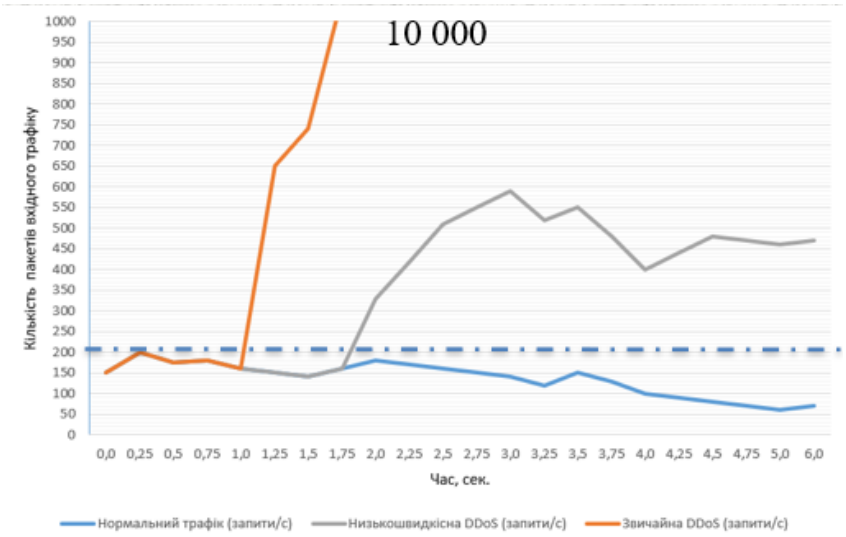


Рис. 3.32. Згенерований вхідний і вихідний трафік веб-сервера без системи захисту

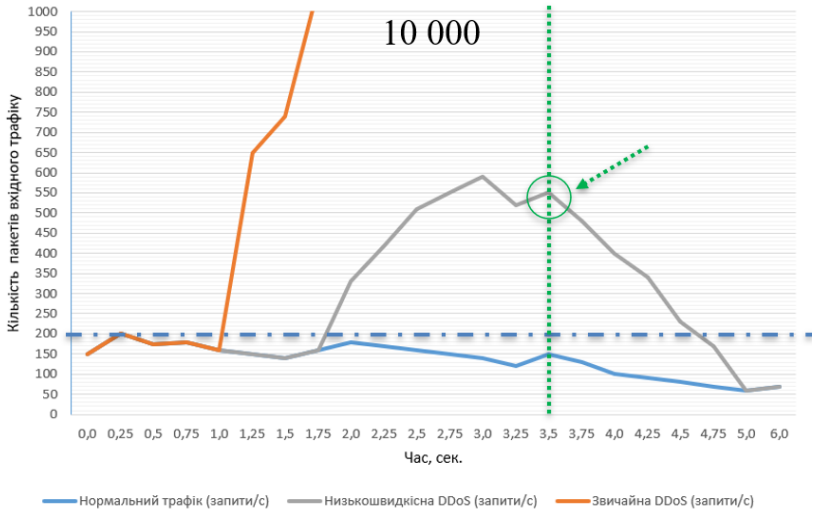


Рис. 3.33. Згенерований вхідний і вихідний трафік веб-сервера з використанням системи захисту

На даних графіках видно як за допомогою моделі упередження низькошвидкісних DDoS-атак в якому влаштований ШІ. Штучний інтелект в даній моделі працює за вказаними особливостями, які в результаті фільтрації трафіку опрацьовуються. При виявленні аномалій в пакета заражені пакети блокуються, опрацьовуються, а інформація про них надсилається до блоку з даними про навчання. Таким чином дані про

навчання будуть використовуватись при наступному колі фільтрації трафіку.

Під час досліджень виконувались моніторинги серверів на різних платформах див рис. 3.34, 3.35, 3.36

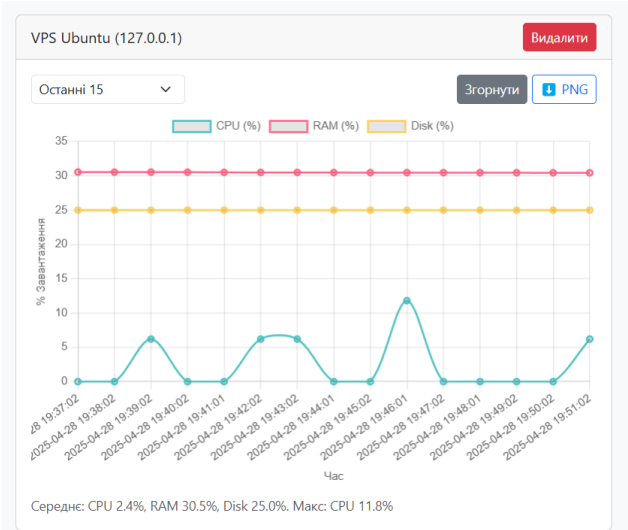


Рис. 3.34 Моніторинг серверів на платформі Ubuntu

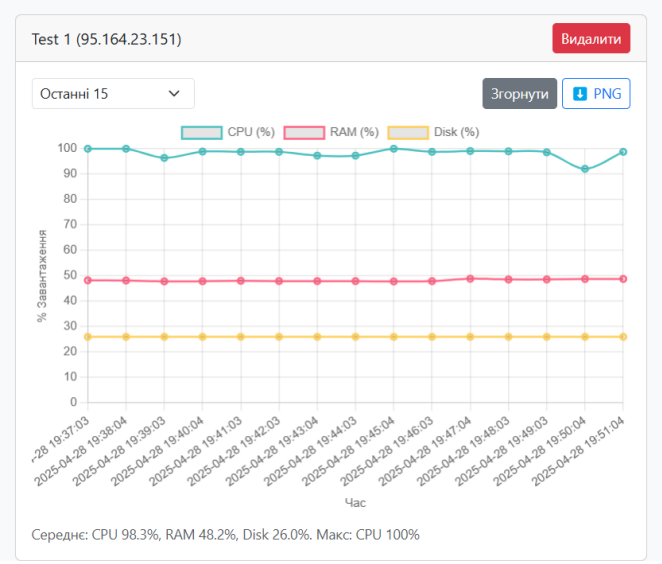


Рис. 3.35 Моніторинг серверів на платформі Windows

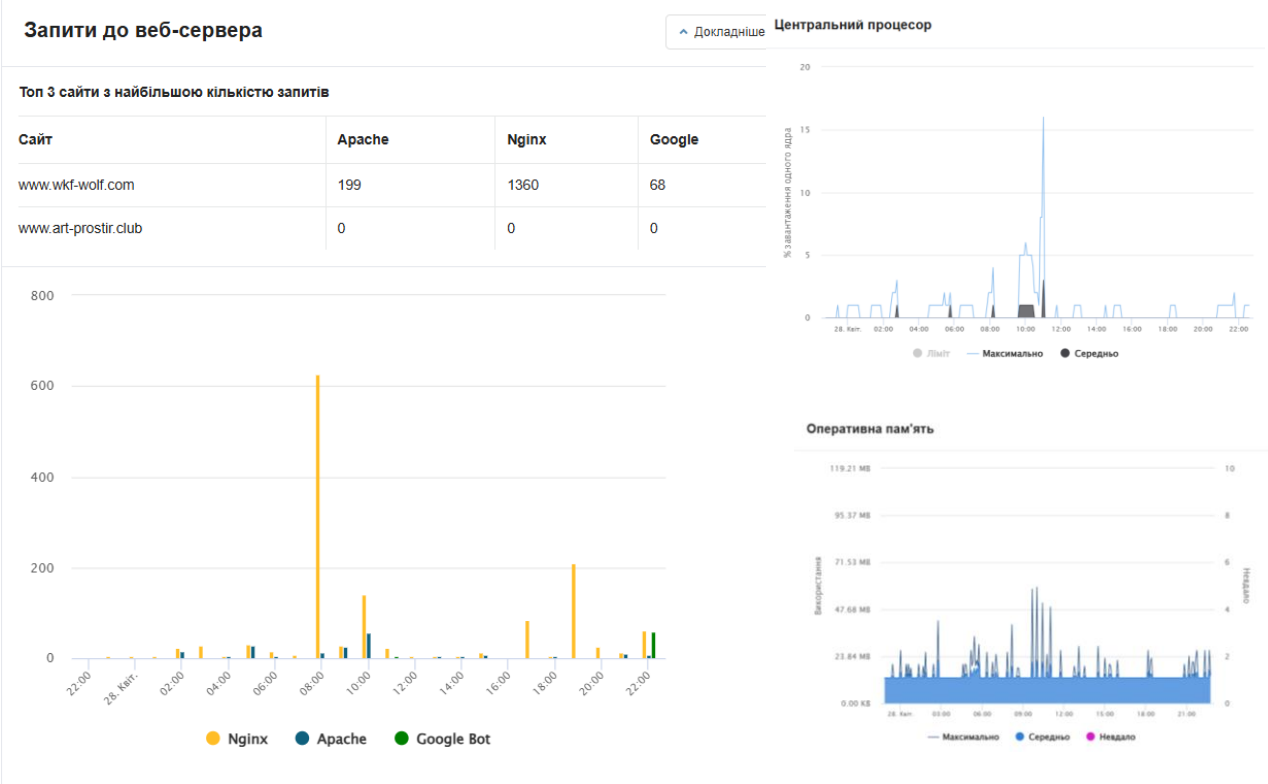


Рис. 3.36 Моніторинг серверів на платформі Apache

Таблиця 3.12

Експерементальні результати протестовані на серверах, які розгорнуті на різних платформах.

Платформи	Пакети		
	Виявлено (%)	Просочились (%)	Відфільтровано (%)
HTTP-сервер, який розгорнутий на кафедрі	100	5	70
Linux	83	5	70
HTTP-сервер Apache	75	3	65

В табл. 3.12 представлені експерементальні результати, які протестовані на серверах розміщених на різних платформах. Розроблені підходи та методи дозволять ефективно виявляти та блокувати низькошвидкісні HTTP DDoS-атаки, які важко ідентифікувати традиційними системами захисту. Що забезпечує стабільну роботу веб-сервісів і запобігатиме їхній нестабільній роботі або повному виведенню з ладу.

Висновки до розділу 3

Були проведені експерименти на різних конфігураціях системи, які показали, що комбінована модель DDoS-атак може бути легко модифікована шляхом видалення несуттєвих компонентів, таких як підсистеми фільтрації та відстеження, а також створенням нових ефективніших компонентів системи. Завдяки таким змінам дана модель, або система в цілому буде ефективною при застосованні до нових типів низькошвидкісних HTTP DDoS-атак.

Проаналізовано стратегії призначення агентів бот-мережі для моделей DDoS-атак на вичерпання пропускної здатності. Розглянуто різні стратегії. Ненульові стратегії призначення агентів показали, що існує щонайменше три фази атаки. Тому зловмисникам необхідно враховувати оптимальну конфігурацію для досягнення бажаних результатів (наприклад, швидкі та потужні атаки, повільні атаки і т.д.).

Запропоновану класифікацію DDoS-атак легше використовувати на практиці з точки зору жертви, тоді як для більш детальної класифікації потрібна певна інформація, відома виключно зловмиснику.

Запропонована класифікація протидії DDoS-атак стоїть на першому місці за кількістю категорій та критеріїв у порівнянні з іншими подібними класифікаціями. Використання цієї класифікації для різних типів протидії DDoS- та низькошвидкісних HTTP DDoS-атак, посідає одне із перших місць в порівнянні з іншими класифікаціями. Це доводить достатню чіткість класифікації та рівнів деталізації.

Модель DDoS-атаки з виснаженням роботи процесора представляє ситуацію в стабільному стані, тоді як OPNET є інструментом моделювання дискретних подій, тому можна побачити варіації часу обслуговування запитів. В результаті модель не можна використовувати для представлення змін часу обслуговування запиту.

Модель DDoS-атаки з вичерпанням пам’яті була розроблена як

система з одним буфером пам’яті для зберігання інформації про відкрите з’єднання. Другий буфер можна використовувати для постановки запиту в чергу перед входом у перший буфер. Ця запропонована модель може бути адаптована до представлення, що добре демонструє розширюваність моделі.

Проведено експериментальне дослідження розробленої системи протидії низькошвидкісним HTTP DDoS-атак. В ході експеременту використовувались сервери, які розгорнуті на різних платформах, що надало можливість порівняти ефективність роботи системи. Результати експерементальних досліджень подані в таблиці 3.12, де бачимо що система надає зменшення ризику успішного проведення низькошвидкісних HTTP DDoS-атак, підвищення стабільності роботи веб-ресурсів.

Розроблені підходи та методи дозволять ефективно виявляти та блокувати низькошвидкісні HTTP DDoS-атаки, які важко ідентифікувати традиційними системами захисту. Що забезпечує стабільну роботу веб-сервісів і запобігатиме їхній нестабільній роботі або повному виведенню з ладу.

Результати дослідження можуть бути впроваджені в різних галузях, таких як фінанси, електронна комерція, освіта або державні організації, де стабільність веб-ресурсів є критично важливою.

ВИСНОВКИ

У дисертації зроблено теоретичне узагальнення та пропонується нове рішення актуальної наукової проблеми розробки системи протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурсі. Отримані науково-практичні результати мали фундаментальне теоретичне та прикладне практичне значення для подальшого розвитку галузі знань «Інформаційні технології» та спеціальності 125–Кібербезпека як в Україні, так і за кордоном.

Основними науковими та практичними результатами одержаними в дисертації є:

1. Проведений аналіз за темою дослідження показав, що в умовах постійного зростання інтенсивності та складності кібератак на інформаційну інфраструктуру, захист вебресурсів від низькошвидкісних (low-rate) HTTP DDoS-атак набуває критичного значення для забезпечення стабільної роботи стратегічно важливих онлайн-сервісів й досі залишається актуальним питання розробки та вдосконалення національних систем протидії, здатних ефективно виявляти та нейтралізовувати саме цей малопомітний, але руйнівний тип кібервпливу. Доведено, що суворо зростаючі вимоги до безперебійності роботи та якості обслуговування (QoS) вебресурсів з одного боку, та стрімка еволюція на практиці методик низькошвидкісних HTTP DDoS-атак, що імітують легальний трафік і ухиляються від традиційних систем захисту (таких як прості порогові методи або аналіз пакетів) з іншого, створюють об’єктивне протиріччя.

2. Вперше розроблено модель детектування аномалій трафіку, яка за рахунок аналізу часових інтервалів запитів, глибинного інспектування HTTP-заголовків, оцінки географічної дисперсії джерел та виявлення відхилень у шаблонах поведінки користувачів, забезпечує високу точність

розрізнення шкідливої активності від легальних сплесків навантаження, мінімізуючи кількість хибно-позитивних спрацьовувань.

Розроблено модель упередження низькошвидкісних HTTP DDoS-атак для виявлення аномалій трафіку, яка за рахунок методу часового вікна, блоку структурних ознак та використання ШІ, дає можливіть виявлення аномалій у реальному часі та сповіщенням про онлайн-дані та дає можливість зменшити навантаження на сервер від 40 до 60 %.

3. Вперше розроблено метод попереднього виявлення кіберінцидентів, який за рахунок поєднання сигнатурного аналізу з аномальною детекцією в реальних умовах, що дозволяє формувати цілісну картину загрози, навіть за умови використання зловмисниками приховування та зміни джерела коду. Запропонований метод раннього виявлення низькошвидкісних DDoS-атак на основі аналізу груп пакетів довів свою ефективність у порівнянні з традиційними підходами.

4. Створено систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси, яка використовує топологічний аналіз мережевих потоків і побудову графів взаємозв'язків між підозрюваними джерелами, що дало можливість автоматично ідентифікувати потенційні траєкторії поширення атаки в межах інфраструктури, враховувати динаміку зміни шаблонів трафіку та інтегрувати дані про вразливості веб-ресурсів та забезпечує не лише своєчасне блокування шкідливих сесій на рівні мережевих елементів або WAF, але й дозволяє прогнозувати й запобігати ускладнення атаки шляхом упередження, оптимізації правил модуля штучного інтелекту, резервування ресурсів та перенаправлення трафіку.

5. Експериментальне дослідження показало адекватність роботи системи протидії низькошвидкісних HTTP DDoS-атак на веб-ресурсів. Використання адаптивної моделі ШІ для виявлення аномалій дозволило підвищити блокування низькошвидкісних HTTP DDoS-атаки на ≈ 73% .

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lukova-Chuiko N. V., Musienko A. P., Koval M. O. Використання мереж петрі для побудови моделі виявлення зовнішніх впливів на інформаційну систему. Системи управління, навігації та зв'язку. Збірник наукових праць. 2018. Т. 2, № 48. С. 77–82. URL: https://doi.org/10.26906/sunz.2018.2.077

2. Стасюк А. И., Корченко А. А. БАЗОВА МОДЕЛЬ ПАРАМЕТРІВ ДЛЯ ПОБУДУВАННЯ СИСТЕМ ВИЯВЛЕННЯ АТАК. Ukrainian Information Security Research Journal. 2012. Т. 14, № 2 (55). URL: https://doi.org/10.18372/2410-7840.14.2183

3. Mirkovich, J.; Dietrich, S.; Dittrich, D.; Reiher, P. 2005. Internet Denial of Service: Attack and Defense Mechanisms. New Jersey: Prentice Hall.

4. Mirkovic, J.; Reiher, P. 2002. A taxonomy of DDoS Atack and DDoS defense Mechanisms, ACM SIGCOMM Computer Communication Review, 34 (2). 13.

5. Specht, S. M.; Lee, R. B 2004. Distributed Denial of Service: Taxonomy of Attacks, Tools and Countermeasures, in Proc. of – 17th International Conference on Parallel and Distributed Computing Systems, San Francisco.

6. A. N. NETWORK INTRUSION DETECTION SYSTEMS BASED ON DEEP LEARNING NEURAL NETWORKS. Scientific papers of Donetsk National Technical University. Series: Informatics, Cybernetics and Computer Science. 2023. Vol. 2, no. 37. P. 15–21. URL: https://doi.org/10.31474/1996-1588-2023-2-37-15-21

7. Karig, D.; Lee, R. 2001. Remote Denial of Service At-tacks and Countermeasures, Princeton University Department of Electrical Engineering Technical Report CE-L2001-002.

8. Asosheh, A.; Ranezani, N. 2008. A comprehensive faxonomy of DDoS attacks and defense mechanism applying in a smart classification, WSEAS Transactions on Communications 7 (4): 281–290.
Електронний ресурс: https://www.cloudflare.com/ru-ru/learning/ddos/http-flood-ddos-attack/

9. Douligeris, C.; Mitrokots, A. 2004. DDoS atacks and defense mechanisms: classification and state-of-the-art, Computer Networks, 4(2004): 643–666.

10. Модель та методи виявлення широкомасштабної атаки в середовищі iot / O. Liashenko та ін. Системи управління, навігації та зв'язку. Збірник наукових праць. 2024. Т. 1, № 75. С. 127–132. URL: https://doi.org/10.26906/sunz.2024.1.127 (дата звернення: 19.05.2025).

11. Holdiy A., Shpur O., Masyuk A. DEVELOPMENT OF A MODEL OF A CYBER THREATS DETECTION SYSTEM WITH SUPPORT AND UPDATE OF ATTACK DETECTION RULES. Information and communication technologies, electronic engineering. 2024. Vol. 4, no. 2. P. 60–71. URL: https://doi.org/10.23939/ictee2024.02.060

12. Salah, K. 2010. Queuing Analysis of Network Firewalls, in Proc. of – IEEE Global Communications Conference, Miami

13. A. Kuzmanovic Дослідження механізмів "shrew attacks" та їх впливу на веб-інфраструктуру 2008 URL:
https://core.ac.uk/download/pdf/38468786.pdf

14. he Security Impact of HTTPS Interception / Z. Durumeric et al. *Network and Distributed System Security Symposium*, San Diego, CA. Reston, VA, 2017. URL: https://doi.org/10.14722/ndss.2017.23456

15. Staniford, S.; Paxson, V.; Weaver, N. 2002. How to 0wn the Internet in Your Spare Time, in Proc. of – 11th USENIX Security Symposium, San Francisco.

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

17. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

18. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/2657-12/ed20241115#Text

19. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 31.12.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

20. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Дата оновлення: 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

21. Lukyanenko T. Y. Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. Modern Information Security. 2022. Vol. 2, no. 50. URL: https://doi.org/10.31673/2409-7292.2022.021521

22. Opanasenko M. I. The technology of ensuring cyber security of the cloud environment based on the Cisco Cloudlock solution. Modern Information Security. 2023. Vol. 53, no.1. URL: https://doi.org/10.31673/2409-7292.2023.010010

23. Assessment of the quality of the technical state monitoring system special purpose telecommunication networks. Connectivity. 2024. Vol. 170, no. 4. URL: https://doi.org/10.31673/2412-9070.2024.041923

24. Савченко В.А., Поночовний П.М., Аверічев І.М. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. // Прикладні

проблеми комп`ютерних наук, безпеки та математики. Луцьк: Волинський національний університет імені Лесі Українки, 2024. №3. – С.71-76 покликання на матеріал:
https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127

25. Ponochovny P. LOW-SPEED HTTP DDOS ATTACK PREVENTION MODEL FOR END USERS. Cybersecurity: Education, Science, Technique. 2024. Vol. 2, no. 26. P. 291–304. URL: https://doi.org/10.28925/2663-4023.2024.26.695

26. Early detection and defense methods for variable ddos attacks based on packet group processing analysis. Scientific Notes of the State University of Telecommunications. 2024. Vol. 6, no. 1. URL: https://doi.org/10.31673/2786-8362.2024.027035

27. Поночовний П., Пепа Ю. Реалізація системи захисту серверів з урахуванням аномалій в пакетах. Measuring and computing devices in technological processes. 2025. № 1. С. 44–51. URL: https://doi.org/10.31891/2219-9365-2025-81-6

28. Рижаков М., Поночоаний П. Модель трансформації на основі штучного інтелекту з елементами захисту від DDoS-атак // Прикладні проблеми комп'ютерних наук, безпеки та математики – 2025. № 4. С. 14-32. покликання на матеріал:
https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128

29. П. Поночовний. Впровадження систем штучного інтелекту у сфери безпеки і оборони, науки і освіти, економіки, медицини // С34 Системи та засоби штучного інтелекту: тези доповідей Міжнародної наукової молодіжної школи. – Київ: ІПШІ «Наука і освіта», 2023. – С. 30-33, покликання на матеріал: https://www.ipai.net.ua/docs/AIIS-2023-school.pdf

30. Пепа Ю. В., Поночовний П. М., Вплив сторонніх факторів на обробку сигналів // XIII міжнародна науково-практична конференція

«Математика. Інформаційні технології. Освіта, 2024, м. Луцьк – с.157-159, покликання на матеріал: https://drive.google.com/file/d/16GSq2WkNNsnEs6KRBkfCGdcYCKwi1bwO/view

31. Петро Поночовний (Ponochovnyy P. M.), Ігор Аверічев (Avierichev I.M.), Критерії виявлення повільних DDoS-атак // XIII Міжнародна науково-технічна ITSec-2024 Безпека інформаційних технологій, 2024, м. Львів – с.175-176, покликання на матеріал: https://drive.google.com/file/d/1N1orbCGW37_pIRTzbHWuEgO3M8lw9B6r/view?usp=drive_link

32. Поночовний П. М., Іванченко І. С. Експериментальне дослідження системи реалізації захисту серверів з урахуванням аномалій в пакетах // II міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024, м. Київ – С. 173 – 177 покликання на матеріал: https://duikt.edu.ua/uploads/p_2661_99635945.pdf

33. Yuriy PEPA, Petro PONOCHOVNYI, Oleksandr LEVKUSHA METHOD FOR DETERMINING VULNERABILITIES TO DDOS ATTACKS ON CONTENT MANAGEMENT SYSTEMS // The IV International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things “TTSIIT - 2025”, KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE -30-31 січня 2025, Ukraine-Iraq-Poland C. – 95-100. Режим доступу: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

34. Поночовний П.М. Автоматизоване реагування на кіберінциденти за допомогою ШІ: міф чи реальність сучасних SOC? // XIIV Міжнародна науково-технічна ITSec-2025 Безпека інформаційних технологій, 2025, м. Тернопіль – с.156-159. Режим доступу:

https://drive.google.com/drive/u/0/folders/1f_WDoOIyqDmVMa5eJZDJ-ABFERbSdEWG

35. Committee on National Security Systems 2010. CNSS Instruction No. 4009: National Information Assurance (IA) Glossary.

36. CCITT X.800, 1991. Data Communication Networkds: Open Systems Interconnection (OSI); Security, Structure and Applications. Security Architecture for Open Systems Interconnection for CCITT Applications.

37. CERT [online]. 1999. Denial of Service Attacks: Available from internet: http://www.cert.org/tech_tips/denial_of_service.html .

38. Bright Hub [online], 2010. Common Security Terms Dictionary: C to D: Available from internet: http://www.brighthub.com/computing/smb-security/articles/8391.aspx

39. Mirkovich, J.; Dietrich, S.; Dittrich, D.; Reiher, P. 2005. Internet Denial of Service: Attack and Defense Mechanisms. New Jersey: Prentice Hall.

40. Fadlallah, A.; Serhrouchmi, A. 2005. Denial of service attack and defense schemes, Analysis and Taxonomy, in Proc. of – 3-rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia.

41. Committee on National Security Systems 2010. CNSS Instruction No. 4009: National Information Assurance (IA) Glossary.

42. Mahathi, K.K. 2008. Botnets: Overview and Case Study, IAS Program Master Project Defense.

43. Stone-Gross, B.; Cova, M.; Cavallaro, L.; Gilbert, B.; Szydlowski, M.; Kemmerer, R.; Kruegel, C; Vigna, G. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover, in Proceedings of the ACM CCS, Chicago.

44. Lin, S.; Chiueh, T. 2006. A Survey on Solutions to Distributed Denial of Service Attacks, Stony Brook University.

45. Feily, M.; Shahrestani, A; Ramadass, S. 2009. A Survey of Botnet and Botnet Detection, in Proc. of – Third International Conference on Emerging Security Information, Systems and Technologies, Athens.

46. Naseem, F.; Shafqat, M.; Sabir, U.; Shahzad, A. 2010. A Survey of Botnet Technology and Detection, International Journal of Video & Image Processing and Network Security, 10 (1):13–17.

47. Gu, Q.; Liu, P. 2008. Denial of Service Attacks, The Handbook of Computer Networks 3, Distributed Networks, Network Planning, Control, Management, and New Trends and Applications.

48. Zou, C. C.; Towsley, D.; Gong, W. 2006. On the performance of Internet worm scanning strategies, Elsevier Journal of Performance Evaluation, 63(7): 700–723.

49. Aycock, J. 2006. Computer Viruses and Malware. New York: Springer.

50. Wang, P.; Sparks, S.; Zou, C. C. 2007. An Advanced Hybrid Peer-to-Peer Botnet, in Proc. of – The first conference on First Workshop on Hot Topics in Understanding Botnets, Cambridge.

51. Morparia, J. 2008. Peer-to-Peer Botnets: Analysis and Detection, San Jose State University.

52. Wang Y.; Lin C.; Li Q.; Fang Y. 2007. A queueing analysis for the denial of service (DoS) attacks in computer networks, Computer Networks, 54: 3564–3573.

53. Juknius, J.; Čenys, A. 2008. BotNet prevencija interneto paslaugų tiekėjų lygmenyje, in Proc. of – Science – Future of Lithuania, Vilnius.

54. Grizzard, J. B.; Sharma, V.; Nunnery, C.; Dagon, D. 2007. Peer-to-Peer Botnets: Overview and Case Study in Proc. of – The first conference on First Workshop on Hot Topics in Understanding Botnets, Cambridge.

55. Chang R. K. C. 2002. Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial, IEEE Communications Magazine. 40: 42-51.

56. Burdach, M. 2010 [online]. Hardening the TCP/IP stack to SYN attacks. Symantec: [cited 14 March 2011]. Available from internet: http://www.securityfocus.com/infocus/1729

57. Lemon, J. 2002. Resisting SYN flood DoS attacks with a SYN cache, in Proc. of – USENIX BSDCon 2002, San Francisco.

58. Bernstein, D. J. 1999 [online]. SYN cookies. Cr.yp.to: [cited 14 March 2011]. Available from internet: http://cr.yp.to/syncookies.html

59. Pastore, M.; Dulaney, E. 2006. CompTIA Security+ Study Guide: Exam SY0-101, Wiley.

60. Choudary, K.; Shilpa, M. 2011. Smurf Attacks: Attacks using ICMP, International Journal of Computer Science and Technology, 2 (1):75–77.

61. Sonic WALL, Inc. 2001 [online]. Denial of Service Attacks: An Emerging Vulnerability for the "Connected" Network. SonicWALL: [cited 14 March 2011]. Available from internet: ftp://ftp.sonicwall.com/pub/info/Denial_Of_Service_Attacks.pdf

62. Securing My Network [online]. 2011. Are you Denied Access to Any Website or Internet? Securing My Network. Available from internet: http://www.securingmynetwork.com/network-security-articles/denial-of-service-attack.php

63. Mavituna, F. 2008 [online]. DoS Attacks Using SQL Wildcards. Portcullis Computer Security. Available from internet: http://www.portcullis-security.com/uplds/wildcard_attacks.pdf

64. Laikas.lt 2011 [online]. Ažiotažas dėl bilietų į „EuroBasket 2011" sutrikdė pardavimų sistemos darbą. Laikas.lt. Available from internet: http://www.laikas.lt/lt/info/3917/aziotazas-del-bilietu-i-eurobasket-2011-sutrikde-pardavimu-sistemos-darba/

65. Karig, D.; Lee, R. 2001. Remote Denial of Service At-tacks and Countermeasures, Princeton University Department of Electrical Engineering Technical Report CE-L2001-002DoS attack taxonomy proposed by A. Fadlallah (Fadlallah and Serhrouchmi 2005)

66. Mirkovich, J.; Dietrich, S.; Dittrich, D.; Reiher, P. 2005. Internet Denial of Service: Attack and Defense Mechanisms. New Jersey: Prentice Hall. DoS attack taxonomy proposed by S. Specht (Specht and Lee 2004)

67. Asosheh, A.; Ranezani, N. 2008. A comprehensive faxonomy of DDoS attacks and defense mechanism applying in a smart classification, WSEAS Transactions on Communications 7 (4): 281–290.

68. Douligeris, C.; Mitrokots, A. 2004. DDoS atacks and defense mechanisms: classification and state-of-the-art, Computer Networks, 4(2004): 643–666

69. Specht, S. M.; Lee, R. B 2004. Distributed Denial of Service: Taxonomy of Attacks, Tools and Countermeasures, in Proc. of – 17th International Conference on Parallel and Distributed Computing Systems, San Francisco

70. Fotopoulou, M.; Petridis, S.; Karachalios, I.; Rakopoulos, D. A Review on Distribution System State Estimation Algorithms. Appl. Sci. 2022, 12, 11073. [Google Scholar] [CrossRef]

71. Yang, H.; He, X.; Wang, Z.; Qiu, R.C.; Ai, Q. Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction. IEEE Trans. Smart Grid 2022, 7, 3174–3187. [Google Scholar] [CrossRef]

72. Vinicius, D.; Pedro, R.; Damien, M.; Mario, M. Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. IEEE Access 2022, 10, 76648–76668. [Google Scholar]

73. Zhao, J.; Jing, X.; Yan, Z.; Pedrycz, W. Network traffic classification for data fusion: A survey. Inf. Fusion 2021, 72, 22–47. [Google Scholar] [CrossRef]

74. Kaur, S.; Kumar, K.; Aggarwal, N.; Singh, G. A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions. Comput. Secur. 2021, 110, 102423. [Google Scholar] [CrossRef]

75. Deb, R.; Roy, S. A comprehensive survey of vulnerability and information security in SDN. Comput. Netw. 2022, 206, 108802. [Google Scholar] [CrossRef]

76. Yuan, J.; Mills, K. Monitoring the macroscopic effect of DDoS flooding attacks. IEEE Trans. Dependable Secur. Comput. 2005, 2, 324–335. [Google Scholar] [CrossRef]

77. Galeano-Brajones, J.; Carmona-Murillo, J.; Valenzuela-Valdés, J.F.; Luna-Valero, F. Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors 2020, 20, 816. [Google Scholar] [CrossRef]

78. Biswas, R.; Kim, S.; Wu, J. Sampling Rate Distribution for Flow Monitoring and DDoS Detection in Datacenter. IEEE Trans. Inf. Forensics Secur. 2021, 16, 2524–2534. [Google Scholar] [CrossRef]

79. Tsobdjou, L.D.; Pierre, S.; Quintero, A. An Online Entropy-Based DDoS Flooding Attack Detection System With Dynamic Threshold. IEEE Trans. Netw. Serv. Manag. 2022, 19, 1679–1689. [Google Scholar] [CrossRef]

80. Liu, Z.; Hu, C.; Shan, C. Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method. Comput. Secur. 2021, 109, 102392. [Google Scholar] [CrossRef]

81. Li, R.; Wu, B. Early detection of DDoS based on φ-entropy in SDN networks. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Darmstadt, Germany, 12–14 June 2020; pp. 731–735. [Google Scholar]

82. Ahalawat, A.; Babu, K.S.; Turuk, A.K.; Patel, S. A low-rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop. J. Inf. Secur. Appl. 2022, 68, 103212. [Google Scholar] [CrossRef]

83. Wang, X.; Zhong, X.; Li, L.; Zhang, S.; Lu, R.; Yang, T. TOT: Trust aware opportunistic transmission in cognitive radio Social Internet of Things. Comput. Commun. 2020, 162, 1–11. [Google Scholar] [CrossRef]

84. Abidi, R.; Azzouna, N.B. Self-adaptive trust management model for social IoT services. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Nicosia, Cyprus, 31 October 31–2 November 2021; pp. 1–7. [Google Scholar]

85. Magdich, R.; Jemal, H.; Nakti, C.; Ben Ayed, M. An efficient Trust Related Attack Detection Model based on Machine Learning for Social Internet of Things. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Nicosia, Cyprus, 28 June–2 July 2021; pp. 1465–1470. [Google Scholar]

86. Abdelghani, W.; Amous, I.; Zayani, C.A. Dynamic and scalable multi-level trust management model for Social Internet of Things. J. Supercomput. 2022, 78, 8137–8193. [Google Scholar] [CrossRef]

87. Balarezo, J.F.; Wang, S.; Chavez, K.G.; Al-Hourani, A.; Kandeepan, S. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Eng. Sci. Tech. Int. J. 2022, 31, 101065. [Google Scholar] [CrossRef]

88. Baskar, M.; Ramkumar, J.; Karthikeyan, C. Low rate DDoS mitigation using real-time multi threshold traffic monitoring system. J. Ambient Intell. Humaniz. Comput. 2021, 1–9. [Google Scholar] [CrossRef]

89. Engström, V.; Lagerström, R. Two decades of cyberattack simulations: A systematic literature review. Comput. Secur. 2022, 116, 102681. [Google Scholar] [CrossRef]

90. Cil, A.E.; Yildiz, K.; Buldu, A. Detection of DDoS attacks with feed forward based deep neural network model. Expert Sys. Appl. 2021, 169, 114520. [Google Scholar] [CrossRef]

91. Doriguzzi-Corin, R.; Millar, S.; Scott-Hayward, S.; Martínez-del-Rincón, J.; Siracusa, D. Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. IEEE Trans. Netw. Serv. Manag. 2020, 17, 876–889. [Google Scholar] [CrossRef]

92. Wei, G.; Wang, Z. Adoption and realization of deep learning in network traffic anomaly detection device design. Soft Comput. 2021, 25, 1147–1158. [Google Scholar] [CrossRef]

93. Fouladi, R.F.; Ermiş, O.; Anarim, E. A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN. Comput. Netw. 2022, 214, 109140. [Google Scholar] [CrossRef]

94. Asad, M.; Asim, M.; Javed, T.; Beg, M.O.; Mujtaba, H.; Abbas, S. DeepDetect: Detection of Distributed Denial of Service Attacks Using Deep Learning. Comput. J. 2020, 63, 983–994. [Google Scholar] [CrossRef]

95. Zaib, M.H.; Bashir, F.; Qureshi, K.N. Deep learning based cyber bullying early detection using distributed denial of service flow. Multimed. Syst. 2022, 28, 1905–1924. [Google Scholar] [CrossRef]

96. Rehman, S.U.; Khaliq, M.; Imtiaz, S.I.; Rasool, A.; Javed, A.R.; Jalil, Z.; Bashir, A.K. DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). Future Gen. Comput. Sys. 2021, 118, 453–466. [Google Scholar] [CrossRef]

97. Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Perez-Diaz, J.A. SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning. IEEE Access 2021, 9, 108495–108512. [Google Scholar] [CrossRef]

98. Zhou, B.; Li, J.; Ji, Y.; Guizani, M. Online Internet Traffic Monitoring and DDoS Attack Detection Using Big Data Frameworks. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 1507–1512. [Google Scholar]

99. Tayfour, O.E.; Marsono, M.N. Collaborative detection and mitigation of DDoS in software-defined networks. J. Supercomput. 2021, 77, 13166–13190. [Google Scholar] [CrossRef]

100. Haider, S.; Akhunzada, A.; Mustafa, I.; Patel, T.B.; Fernandez, A.; Choo, K.K.R.; Iqbal, J. A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. IEEE Access 2020, 8, 53972–53983. [Google Scholar] [CrossRef]

101. Hwang, R.H.; Peng, M.C.; Huang, C.W.; Lin, P.C.; Nguyen, V.L. An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection. IEEE Access 2020, 8, 30387–30399. [Google Scholar] [CrossRef]

102. Cheng, J.; Liu, Y.; Tang, X.Y.; Sheng, V.S.; Li, M.Y.; Li, J.Q. DDoS Attack Detection via Multi-scale Convolutional Neural Network. Comput. Mater. Contin. 2020, 62, 1317–1333. [Google Scholar] [CrossRef]

103. Kumar, H.; Aoudni, Y.; Ortiz, G.G.R.; Jindal, L.; Miah, S.; Tripathi, R.; Damaševičius, R. Light Weighted CNN Model to Detect DDoS Attack over Distributed Scenario. Secur. Commun. Netw. 2022, 2022, 7585457. [Google Scholar] [CrossRef]

104. Mirkovic, J.; Reiher, P. 2002. A taxonomy of DDoS Atack and DDoS defense Mechanisms, ACM SIGCOMM Computer Communication Review, 34 (2).

105. Електронне джерело: https://b2b.ukrtelecom.ua/bbservices/zashchita-ot-ddos-atak-41

106. Електронне джерело: https://hub.kyivstar.ua/articles/kyyivstar-biznes-proponuye-kliyentam-poslugu-zahystu-vid-ddos-atak

107. Houghton Mifflin Company 2005 [online]. Model – definition of model. Free Online Dictionary, Thesaurus and Encyclopedia Available from internet: http://www.thefreedictionary.com/model

108. Chen, T. M. 2007. Network Traffic Modeling, Chapter in – The Handbook of Computer Networks, Hossein Bidgoli (ed.), Wiley.

109. Pearson, M.; Cleary, J.; Unger, B.; Williamson, C. 1996. Current Techniques for Measuring and Modeling ATM Traffic, Technical Report, Computer Science Department, Waikato University.

110. Frost, V. S.; Melamed, B. 1994. Traffic Modeling For Telecommunications Netwrks. IEEE Communications Magazine, 33: 70–80.

111. Marathe, M.; Hawe, W. 1982. Predicted capacity of Ethernet in a university environment, in Proc. of – Southcon, Orlando.

112. Paxson, V.; Floyd, S. 1995. Wide-Area Traffic: The Failure of Poisson Modeling, IEEE/ACM Transactions on Networking, 3(3): 226–244.

113. Puigjaner, R. 2003. Performance Modelling of Computer Networks, in Proc. of – The 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research, La Paz: 106–123.

114. Beran, J.; Sherman, R.; Taqqu, M.; Willinger, W. 1997. Variable-bit-rate video traffic and long range dependence, IEEE Transactions on Communications, 43:1566–1579.

115. Jerkins, J. L.; Wang, J. L.1997. A measurement analysis of ATM cell-level aggregate traffic, in Proc. of – Global Telecommunications ConferenceGLOBECOM '97.

116. Riedi, R. H.; Vehel, J. L. 1997. Multifractal properties of TCP traffic: a numerical study, Technical Report 3129, INRIA Rocquencourt.

117. Norros, I. 1994. A storage model with self-similar input, Queueing Systems, 16:387-396.

118. Abry, P.; Veitch, D. 1998. Wavelet analysis of long-range-dependent traffic, IEEE Transactions on Information Theory 44.

119. Erramilli, A.; Roughan, M.; Veitch, D.; Willinger, W. 2002. Self-Similar Traffic and Network Dynamics, in Proc. of – the IEEE 90

120. Vishwanath, K. V.; Vahdat, A. 2006. Realistic and responsive network traffic generation, in Proc. of – 2006 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications, Pisa.

121. Cao, J.; Cleveland, W.S.; Gao, Y.; Jeffay, K.; Smith, F. D.; Weigle, M.C. 2004. Stochastic Models for Generating Synthetic HTTP Source Traffic, in Proc. of – IEEE INFOCOM, Hong Kong: 1547–1558.

122. Puigjaner, R. 2003. Performance Modelling of Computer Networks, in Proc. of – The 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research, La Paz: 106–123.

123. Heidari, M. 2006 [online]. The Role of Modeling and Simulation in Information Security The Lost Ring. Mega Security. Available from internet: http://www.megasecurity.org/papers/The_Role_of_Modeling_and_Simulation_in_Information_Security.pdf

124. Meadows, M. 1999. A Formal Framework and Evaluation Method for Network Denial of Service, in Proc of – 12th IEEE workshop on Computer Security Foundations, Washington.

125. Meadows, C. 2001. A cost-based framework for analysis of denial of service in networks, Journal of Computer Security, 9 (1-2): 143–164.

126. Diffie, W.; Oorschot, P. C.; Wiener, M. J. 1992. Authentication and authenticated key exchanges, Designs, Codes, and Cryptography, 2 (2): 107–125.

127. Gong, L.; Syverson, P. 1998. Fail-stop protocols: An approach to designing secure protocols, Chapter inDependable Computing for Critical Applications (ed. Iyer, R. K.; Morganti, M.; Fuchs W. K.; Gligor, V.), IEEE Computer Society.

128. Lafrance, S.; Mullins, J. 2003. An information flow method to detect denial of service vulnerabilities, Journal of Universal Computer Science.

129. Cao, Z.; Guan, Z.; Chen, Z.; Hu, J.; Tang, L. 2007. An economical model for the risk evaluation of DoS vulnerabilities in cryptography protocols, in Proc. of – The Third International Conference on Information Security Practice and Experience, Hong Kong:129–144.

130. Shenker, S. 1994. Making greed work in networks: A game-theoretic analysis of switch service disciplines, in Proc. of – SIGCOMM Symposium on Communications Architectures and Protocols, London: 47–57.

131. Maheswaran, R.; Basar, T. 1998. Multi-user flow control as a nash game: Performance of various algorithms, in Proc. of – 37th IEEE Conference on Decision and Control, Tampa: 1090–1095.

132. Lye, K.; Wing. J. M. 2002. Game strategies in network security, in Proc. of – TheWorkshop on Foundations of Computer Security, Copenhagen.

133. Bencsath, B.; Vajda, I.; Buttyan, L. 2003. A game based analysis of the client puzzle approach to defend against dos attacks, in Proc. of – 2003 International Conference on Software, Telecommunications and Computer Networks, Split: 763–767.

134. Mahimkar, A.; Shmatikov, V. 2005. Game-based analysis of denial-of-service prevention protocols, in Proc. of – 18th IEEE Computer Security Foundations Workshop, Aix-en-Provence.

135. Agha, G.; Gunter, C. A.; Greenwald, M.; Khanna, S.; Meseguer, J.; Sen, K.; Thati, P. 2005. Formal modeling and analysis of DoS using probabilistic rewrite theories, in Proc of – International Workshop on Foundations of Computer Security, Chicago.

136. AlTurki, M.; Meseguer, J.; Gunter, C. A. 2009. Probabilistic modeling and analysis of DoS protection for the ASV protocol. Electronic Notes in Theoretical Computer Science, 234: 3–18.

137. Kim, M.; Stehr, M. O.; Talcott, C. L.; Dutt, N. D.; Venkatasubramanian, N. 2007. A probabilistic formal analysis approach to cross layer optimization in distributed embedded systems, Formal Methods for Open Object-Based Distributed Systems, 4468.

138. Huang Q.; Kobayashi H.; Liu B. 2003. Analysis of a New Form of Distributed Denial of Service Attack, in Proc. of – Conference of Information Science and Systems, Baltimore.

139. Huang Q.; Kobayashi H.; Liu B. 2003. Modeling of Distributed Denial of Service Attacks in Wireless Networks, in Proc. of – IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 1: 41–44.

140. Khan, S.; Traore, I. 2005. Queue-based Analysis of DoS Attacks, in Proc. of – IEEE Workshop on Information Assurance and Security, West Point: 266–273.

141. Aissani, A. 2008. Queueing Analysis for Networks Under DoS Attack, in Proc. of – IAENG International Conference on Communication Systems and Applications, Hong Kong: 500–513.

142. Macia-Fernandez, G.; Diaz-Verdejo, J. E.; Garcia-Teodoro, P. 2006. Mathematical foundations for the design of a low-rate DoS attack to iterative servers (short paper), Lecture Notes in Computer Science, 4307: 282–291.

143. Macia-Fernandez, G.; Diaz-Verdejo, J. E.; Garcia-Teodoro, P. 2009. Mathematical Model for Low-Rate DoS Attacks against Application Servers, IEEE Transactions On Information Forensics and Security, 4 (3): 519–529.

144. Chaturvedi, N.; Mohant, H. 2011. A Mathematical Model for Randomly-Occurring Low-Rate Denial of Service Attack, in Proc. of – First Student Research Symposium in conjunction with Seventh ICDCIT-2011, Bhubaneswar.

145. Електронне джерело: https://www.unb.ca/cic/datasets/ids-2017.html

ДОДАТКИ

Додаток А

Приклад налаштування серверу Apache

<IfModule mod_evasive20.c>

DOSHashTableSize 3097

DOSPageCount 6

DOSSiteCount 100

DOSPageInterval 2

DOSSiteInterval 2

DOSBlockingPeriod 600

</IfModule>

Опис налаштувань:

- DOSHashTableSize: це розмір хеш-таблиці, яка обробляє запити до веб-сервера.
- DOSPageCount: кількість запитів до однієї сторінки з тієї самої IP-адреси протягом заданого інтервалу часу.
- DOSSiteCount: кількість запитів до всіх сторінок домену, тобто якщо більше 100 запитів надійшло з однієї IP-адреси до різних сторінок домену, тоді ця IP-адреса буде заблокована.
- DOSPageInterval: інтервал для директиви DOSPageCount (у секундах).
- DOSSiteInterval: інтервал для директиви DOSSiteCount (у секундах).
- DOSBlockingPeriod: Як довго блокувати відповідний IP (у секундах).
- DOSEmailNotify: можна використовувати для сповіщення, надішле електронний лист про те, що IP-адресу заблоковано.
- DOSSystemCommand: ця директива використовується для виконання деяких команд, коли IP заблоковано. Наприклад, їх можна

використовувати для додавання IP-адреси до таблиці брандмауера (наприклад: "/sbin/iptables -A INPUT -p tcp --dport 80 -s %s -j REJECT" У %s передається з IP-адреси модуль)

- DOSWhiteList: список «білих» IP-адрес, можливо, з масками (наприклад, 127.0.0.*)

Параметри були змінені таким чином:

Для apache (httpd.conf)

Timeout 20

MaxKeepAliveRequests 15

KeepAliveTimeout 2

MinSpareServers 3

MaxSpareServers 64

StartServers 1024

Максимальна кількість клієнтів 2500

MaxRequestsPerChild 100000

MaxConnPerIP 25

Для mod_php

php_admin_flag safe_mode on

php_admin_flag allow_url_fopen off

php_admin_value doc_root /home/hst_mklimat/htdocs

php_admin_flag magic_quotes_runtime on

php_admin_value open_basedir /home/hst_mklimat/htdocs

php_admin_value upload_tmp_dir /home/hst_mklimat/htdocs/tmp

php_admin_value safe_mode_allowed_env_vars PHP_

php_admin_value upload_max_filesize 1024000

php_admin_value max_execution_time 10

php_admin_value post_max_size 1M

php_admin_value memory_limit 1M

php_admin_value admin_flag mysql.allow_persistent off

php_admin_value mysql.max_links 5

php_admin_flag pgsql.allow_persistent off

php_admin_value pgsql .max_links 5

php_admin_value disable_functions mysql_pconnect,pg_pconnect

Для mysql (/etc/my.cnf)

[mysqld]

set-variable = max_connections=15

set-variable = thread_concurrency=8

Програмний захист від низькошвидкісних HTTP DdoS-атак

DDoS Deflate

Додаток Б

Встановлення та налаштувань DDoS Deflate

FREQ=1

NO_OF_CONNECTIONS=50

APF_BAN=1

KILL=1

EMAIL_TO=”root”

BAN_PERIOD=600

Налаштування iptables

Представлені правила безпеки, складені для сервера LAMP.

Політика стандартної мережі:

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

Скидання існуючих схем:

iptables -F

ANTI - SYN FLOOD:

iptables -A INPUT -p tcp --dport 80 --syn -m limit --limit 1/s -j ACCEPT

Блокування етапу SYN (не більше 10 SYN):

iptables -A INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10\ -j DROP

поставте прапорець "New not syn:"

iptables -A bad_tcp_packets -p tcp --dport 80 !--syn -m state --state NEW \-j LOG --log-prefix "New not syn:"

iptables -A bad_tcp_packets -p tcp --dport 80 !--syn -m state --state NEW \-j DROP

ANTI PING OF DEAD:

iptables -A INPUT -p icmp --icmp-type echo-request -m limit\

--limit 1/s -j ACCEPT

Захист від прихованого сканування портів (ANTI - PORT SCANNER):

iptables -A INPUT -p tcp --tcp-flags SYN, ACK, FIN, RST RST \

-m limit --limit 1/s -j ACCEPT

iptables -A INPUT -p tcp --tcp-flags ALL SYN, ACK -j DROP

Припускаючи, що вже пройдено 400 запитів, наступні відхиляються, якщо більше 300 за секунду:

iptables –A INPUT -d $IP_web -p tcp --dport 80 -m state \

--state NEW -m limit --limit 300/c --limit-burst 400 -j DROP

Максимум 10 одночасних підключень до порту 80 з одного IP:

iptables -A INPUT -p tcp --dport 80 -m iplimit --iplimit-above 10 -j DROP

12 в секунду для інтерфейсу eth0 з максимально дозволеною кількістю 24:

iptables --new-chain car

iptables --insert OUTPUT 1 -p tcp --destination-port 80 -o eth0 --jump car

iptables --append car -m limit --limit 12/sec --limit-burst 24 --jump RETURN

iptables --append car --jump DROP

20 сітчастих з'єднань класу C:

iptables -I INPUT -p tcp --dport 80 -m iplimit --iplimit-above 20 --iplimit-mask\ 24 -j DROP

Щоб дозволити будь-який вихідний трафік:

iptables –A INPUT –m state --state ESTABLISHED, RELATED –j ACCEPT

Видалити підроблені пакети, позначені як Bad Guy:

iptables -A INPUT -m recent --rcheck --seconds 60 -m limit --limit 10/sec \

-j LOG --log-префікс "BG"

```
iptables -A INPUT -m recent --update --seconds 60 -j DROP
iptables -A INPUT -i $int_if -s $int_ip -m recent --set -j DROP
```

Видаліть відомі віруси та сканери портів:

```
iptables -A INPUT -i $int_if -m multiport -p tcp --dports \
53,113,135,137,139,445 -j DROP
iptables -A INPUT -i $int_if -m multiport -p udp --dports \
53,113,135,137,139,445 -j DROP
iptables -A INPUT -i $int_if -p udp --dport 1026 -j DROP
iptables -A INPUT -i $int_if -m multiport -p tcp --dports 1433,4899 -j
DROP
```

Додаток В

Код реалізації алгоритму

```
import pandas as pd
import numpy as np
from sklearn.cluster import DBSCAN
import matplotlib.pyplot as plt

# Генерація фіктивних даних (групи пакетів)
np.random.seed(42)
data = {
    'num_packets': np.random.randint(10, 100, 100),  # Кількість пакетів у групі
    'time_window': np.random.uniform(1, 10, 100),  # Часове вікно (сек)
    'unique_ips': np.random.randint(1, 20, 100),  # Унікальні IP-адреси
}
df = pd.DataFrame(data)

# Функція ризику R(G)
alpha, beta, gamma = 0.5, 0.3, 0.2
df['risk'] = (
    alpha * (df['num_packets'] / df['time_window']) +
    beta * (1 - df['unique_ips'] / df['num_packets']) +
    gamma * np.random.exponential(scale=1, size=100)  # Імітація часових інтервалів
)
```

```
        # Нормалізація даних для кластеризації
        from sklearn.preprocessing import StandardScaler
        X = StandardScaler().fit_transform(df[['num_packets',
'time_window', 'risk']])
        # Застосування DBSCAN
        dbscan = DBSCAN(eps=0.5, min_samples=5)
        clusters = dbscan.fit_predict(X)
        df['cluster'] = clusters
        # Візуалізація кластерів
        plt.figure(figsize=(10, 6))
        colors = ['green', 'blue', 'red', 'purple', 'orange']
        for cluster_id in np.unique(clusters):
            if cluster_id == -1:
                label = 'Шум'
                color = 'gray'
            else:
                label = f'Кластер {cluster_id}'
                color = colors[cluster_id % len(colors)]
            plt.scatter(
                df[df['cluster'] == cluster_id]['num_packets'],
                df[df['cluster'] == cluster_id]['time_window'],
                color=color,
                label=label
            )
        plt.xlabel('Кількість пакетів')
        plt.ylabel('Часове вікно (сек)')
        plt.title('Кластеризація груп пакетів (DBSCAN)')
        plt.legend()
                                                    plt.show()
```

Додаток Г

Розподіл ризику атаки

```
        plt.figure(figsize=(10, 6))
        plt.hist(df[df['cluster'] == -1]['risk'], bins=20, alpha=0.5, label='Шум')
        plt.hist(df[df['cluster'] == 2]['risk'], bins=20, alpha=0.5, label='Кластер 2 (атака)')
        plt.xlabel('Ризик атаки (R(G))')
        plt.ylabel('Частота')
        plt.title('Розподіл ризику для кластерів')
        plt.legend()
 plt.show()
```

«ЗАТВЕРДЖУЮ»
Генеральний директор
Товариства з обмеженою
відповідальністю «ЛУЧ»

_____ Євген ЧЕМЕС

А К Т

Комісія у складі:
голови: заступник директора, кандидат технічних наук, доцент –
Шуклін Герман Вікторович;
членів комісії: керівник відділу систем інформаційної безпеки –
Лазебний Владислав Анатолійович;
заступник керівника відділу інформаційної безпеки –
Тимо Володимир Євстратьєвич,

склала Акт, який підтверджує впровадження результатів дисертаційного дослідження аспіранта ПОНОЧОВНОГО Петра Михайловича з Державного університету інформаційно-комунікаційних технологій (тема роботи: «Система протидії низько швидкісним HTTP DDoS-атакам на веб-ресурси» на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» в роботу ТОВ «ЛУЧ» (ЄДРПО 21595641).

Запропонована система протидії HTTP DDoS-атак на веб-ресурси містить модуль аналізу трафіку в реальному часі з просторовими вікнами, що дозволяє розпізнати легальні запити до серверу від підозрілих, а також програмний модуль аналізу аномалій в пакетах даних, що аналізуються за допомогою штучного інтелекту.

Саме програмний модуль аналізу аномалій в пакетах дозволяє знизити навантаження на мережеві карти серверів і уникнути переповнення буферної пам'яті чергами пакетів на поточну обробку.

ТОВ «ЛУЧ» інтегрувало програмний модуль аналізу аномалій в програмовані маршрутизатори мережевої конвергенції Cisco NCS540 та NCS560, що дозволяє більшість операцій фільтрації пакетів даних і повільних DDoS-атак виявляти на ранніх етапах, а не на самому серверному обладнанні. Це суттєво розвантажує роботу серверів і підвищує їх захист від небажаного трафіку з підозрілою чи шкідливою інформацією.

Голова комісії _____ **к.т.н., доцент Герман ШУКЛІН**

Члени комісії _____ **Владислав ЛАЗЕБНИЙ**

_____ **Володимир ТИМО**

ТОВ "СІТОН ДІДЖИТАЛ"
вул. Гарматна, 4, 4-й поверх, офіс 4,
Київ, Україна, 03067
+380 44 239 99 99
info@seeton.digital

ЗАТВЕРДЖУЮ
Директор товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ»

_____ **Дмитро НІКІТЮК**
(підпис)

«03» 03 2025 року

М.П.

АКТ

Комісія у складі:
голови – директор, Нікітюк Дмитро Вікторович;
членів комісії: – керівник відділу систем інформаційної безпеки, Педченко Євгеній Максимович
– заступник керівника відділу систем інформаційної безпеки, Коровайченко Юрій Юрійович

цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри Систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій.

Поночовного Петра Михайловича

на тему: "Система протидії упередження низькошвидкісних HTTP DDOS-атак на веб-ресурси"
на здобуття ступеня доктора філософії за спеціальністю **125 «Кібербезпека»**
впроваджені в діяльності **товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ».**

Система протидії упередження низькошвидкісних HTTP DDOS-атак на веб-ресурси

Під час розробки програмного рішення для виявлення та нейтралізації низькошвидкісних HTTP DDOS-атак, орієнтованого на захист веб-ресурсів українських комерційних організацій та державних установ, використано наукові та прикладні матеріали дисертаційного дослідження Поночовного Петра Михайловича. Ці матеріали висвітлюють методологію ідентифікації атак, що характеризуються низькою частотою запитів, але тривалою часовою активністю, які унеможливлюють коректне функціонування серверів. Розроблена система включає:

- деталізовану структурну модель аналізу трафіку, що дозволяє відрізняти легальні запити від атакувальних на основі аномалій у часових інтервалах, обсягах даних та шаблонах поведінки користувачів.
- алгоритми машинного навчання для динамічного адаптування до нових векторів атак, що забезпечують автоматичне оновлення правил фільтрації без потреби в ручному втручанні.
- програмний модуль для інтеграції із веб-серверами та системами кібербезпеки, що реалізує механізми обмеження трафіку, блокування підозрілих IP-адрес та генерування звітів у реальному часі.

Цей підхід не лише підвищує стійкість інформаційної інфраструктури до складних атак, але й забезпечує сумісність із міжнародними стандартами кібербезпеки, що є критичним для інтеграції українських систем у глобальний цифровий простір.

Голова комісії	Директор	_____ (підпис) Дмитро НІКІТЮК
Члени комісії	Керівник відділу систем інформаційної безпеки	_____ (підпис) Євгеній ПЕДЧЕНКО
	Заступник керівника відділу систем інформаційної безпеки	_____ (підпис) Юрій КОРОВАЙЧЕНКО

«ЗАТВЕРДЖУЮ»
Директор товариства з обмеженою відповідальністю «А.А.Г.»
_____ Андрій ЧУМАК

А К Т

Комісія у складі:
голови: директора, Чумака Андрія Павловича;
членів комісії: керівник відділу систем інформаційної безпеки та захисту інформації;
провідний інженер відділу інформаційної безпеки та захисту інформації, Гримайло Богдан Петрович

цим Актом підтверджує, що результати дисертаційного дослідження аспіранта кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій

ПОНОЧОВНОГО Петра Михайловича

на тему: «Система протидії низько швидкісним HTTP DDoS-атакам на веб-ресурси» на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» впроваджені в діяльність ТОВ «А.А.Г.» (ЕДРПО 35525122).

Аспірант Поночовний П.М. запропонував метод раннього виявлення повільних DDoS-атак та розробив систему протидії.

Розроблена система протидії включає в себе програмний модуль для інтеграції із веб-серверами під час доступу до відео контенту. Цей модуль реалізує механізм аналізу поточного трафіку в реальному часі на основі штучного інтелекту і блокує підозрілі пакети даних з підсистем локальної мережі або із зовнішніх сегментів з підозрілими IP-адресами, що генерують шкідливий трафік.

В роботі ТОВ «А.А.Г.» проведено тестування запропонованого програмного модуля (ефективність блокування повільних DDoS-атак складає ≈ 82%) та інтегровано в роботу ftp-серверів для збереження відео контенту з інтелектуальних систем відео нагляду з дистанційним віддаленим доступом до ftp-серверів.

Голова комісії _____ Андрій ЧУМАК

Члени комісії _____ Андрій ПРАВДИВИЙ

_____ Богдан ГРИМАЙЛО