УДК 004.056 DOI: 10.31673/2412-4338.2021.042840

Савченко В.А., Кожухівський А.Д., Ільїн О.Ю.
Державний університет телекомунікацій, Київ

ДІАГНОСТУВАННЯ ПОЧАТКУ ПОВІЛЬНОЇ HTTP DDOS АТАКИ НА ОСНОВІ ДВОПАРАМЕТРИЧНОГО КОРЕЛЯЦІЙНОГО АНАЛІЗУ ТРАФІКУ

Анотація: *У статті досліджено проблему виявлення повільних DDoS-атак на основі аналізу мережевого трафіку. Виявлення повільної HTTP-атаки є значною проблемою, оскільки поведінка зловмисника може імітувати поведінку законного користувача з повільними ресурсами. Авторами запропоновано чотиризонну архітектуру виявлення атак на основі аналізу двох параметрів: кількості підключень до сервера та середнього часу затримки відповіді клієнта. Запропоновано методику виявлення повільних DDOS атак на основі кореляційного аналізу та прогнозу параметрів. Авторський підхід використовує оригінальну двопараметричну модель кореляційного аналізу за кількістю з'єднань і середньою реальною затримкою в мережі. Розроблено алгоритм виявлення повільної DDoS-атаки на основі прогнозування двох параметрів. Ці параметри використовуються як для аналізу, так і для короткострокового прогнозування поведінки трафіку. Алгоритм прогнозування використовує метод розрахунку апостериорної траєкторії часового ряду залежно від апріорних статистичних спостережень. Прогнозування параметрів поведінки користувача дозволяє заздалегідь виявляти повільні DDoS-атаки на основі алгоритму пошуку невідомих майбутніх значень для часового ряду параметрів. Використання відносних значень NC і ARNL як параметрів прогнозу дає можливість побудувати гнучку систему розпізнавання, адаптовану до специфіки конкретної системи. Здійснено моделювання двопараметричного алгоритму виявлення повільних DDOS атак на основі прогнозування та оцінено його ефективність. Запропонований метод є поєднанням штучного інтелекту та статистичного аналізу та використовує алгоритм самонавчання з достатньою статистикою атак. Експериментальні результати показують, що метод підходить для раннього виявлення атак, таких як Slow HTTP Headers, Slow HTTP Body, Slow HTTP Read. Моделювання параметрів трафіку підтверджує можливості методу для виявлення повільних атак на різних інтервалах часу, оскільки точність прогнозу залежить від своєчасності спостережень. При достатній статистиці спостережень відхилення кривої прогнозу може бути менше 5%.*

Ключові слова*: повільна HTTP DDOS атака, поведінка користувача, кореляційний аналіз, індивідуальна траєкторія, модель прогнозу.*

Savchenko V.A., Kozhukhivskyi A.D., Ilyin O.Yu.
State University of Telecommunications, Kyiv

DIAGNOSING THE START OF A SLOW HTTP DDOS ATTACK BASED ON TWO-PARAMETER TRAFFIC CORRELATION ANALYSIS

Abstract: *The article investigates the problem of detecting slow DDoS attacks based on network traffic analysis. Detecting a slow HTTP attack is a significant challenge because the attacker's behavior can mimic that of a legitimate user with slow resources. The authors proposed a four-zone attack detection architecture based on the analysis of two parameters: the number of connections to the server and the average client response delay time. A technique for detecting slow DDOS attacks based on correlation analysis and parameter forecasting is proposed. The author's approach uses an original two-parameter correlation analysis model based on the number of connections and the average real delay in the network. An algorithm for detecting a slow DDoS attack based on the prediction of two parameters has been developed. These parameters are used both for analysis and for short-term prediction of traffic behavior. The forecasting algorithm uses the method of calculating the posterior trajectory of the time series depending on a priori statistical observations. Prediction of user behavior parameters allows early detection of slow DDoS attacks based on an algorithm for searching for unknown future values for a time series of parameters. Using the relative values of NC and ARNL as prediction parameters makes it possible to build a flexible recognition system adapted to the specifics of a particular system. Simulation of the two-parameter algorithm for*

detecting slow DDOS attacks based on prediction was carried out and its effectiveness was evaluated. The proposed method is a combination of artificial intelligence and statistical analysis and uses a self-learning algorithm with sufficient attack statistics. Experimental results show that the method is suitable for early detection of attacks such as Slow HTTP Headers, Slow HTTP Body, Slow HTTP Read. Simulation of traffic parameters confirms the method's ability to detect slow attacks at different time intervals, since the accuracy of the forecast depends on the timeliness of the observations. With sufficient statistics of observations, the deviation of the forecast curve can be less than 5%.

***Keywords**: slow HTTP DDOS attack, user behavior, correlation analysis, individual trajectory, prediction model.*

Савченко В.А., Кожуховский А.Д., Ильин О.Ю.

Государственный университет телекоммуникаций, Киев

ДИАГНОСТИРОВАНИЕ НАЧАЛА МЕДЛЕННОЙ HTTP DDOS АТАКИ НА ОСНОВЕ ДВОПАРАМЕТРИЧЕСКОГО КОРЕЛЯЦИОННОГО АНАЛИЗА ТРАФИКА

***Аннотация:** В статье исследована проблема выявления медленных DDoS-атак на основе анализа сетевого трафика. Выявление медленной HTTP-атаки представляет собой значительную проблему, поскольку поведение злоумышленника может имитировать поведение законного пользователя с медленными ресурсами. Авторами предложена четырехзонная архитектура обнаружения атак на основе анализа двух параметров: количества подключений к серверу и среднего времени задержки ответа клиента. Предложена методика обнаружения медленных DDOS атак на основе корреляционного анализа и прогноза параметров. Авторский подход использует оригинальную двухпараметрическую модель корреляционного анализа по количеству соединений и средней реальной задержке сети. Разработан алгоритм обнаружения медленной DDoS-атаки на основе прогнозирования двух параметров. Эти характеристики употребляются как для анализа, так и для краткосрочного прогнозирования поведения трафика. Алгоритм прогнозирования использует метод расчета апостериорной траектории временного ряда в зависимости от априорных статистических наблюдений. Прогнозирование параметров поведения пользователя позволяет заранее обнаруживать медленные DDoS-атаки на основе алгоритма поиска неизвестных будущих значений временного ряда параметров. Использование относительных значений NC и ARNL в качестве параметров прогноза позволяет построить гибкую систему распознавания, адаптированную к специфике конкретной системы. Осуществлено моделирование двухпараметрического алгоритма выявления медленных атак DDOS на основе прогнозирования и оценена его эффективность. Предложенный метод представляет собой сочетание искусственного интеллекта и статистического анализа и использует алгоритм самообучения с достаточной статистикой атак. Экспериментальные результаты показывают, что метод подходит для раннего обнаружения атак, таких как Slow HTTP Headers, Slow HTTP Body, Slow HTTP Read. Моделирование параметров трафика подтверждает возможности метода выявления медленных атак на разных интервалах времени, поскольку точность прогноза зависит от своевременности наблюдений. При достаточной статистике наблюдений отклонение кривой прогноза может быть меньше 5%.*

***Ключевые слова:** медленная HTTP DDOS атака, поведение пользователя, корреляционный анализ, индивидуальная траектория, модель прогноза.*

1. Вступ

Типовими проблемами, з якими стикається будь-яка мережева архітектура, включаючи хмарні обчислення, є DDoS-атаки. Під час DDoS-атаки зловмисник намагається вплинути на сервер жертви або запущені програми з скомпрометованих комп’ютерів із різних місць. Зловмисник встановлює зловмисне програмне забезпечення на багатьох комп’ютерах через Інтернет, використовуючи контрольований хост. Зламані машини діють як армія ботів для DDoS-атак. Коли зловмисник хоче атакувати сервер або програму жертви, він надсилає команду на початок атаки хостам ботів, щоб хости ботів почали атакувати жертву. На відміну від традиційних атак (затоплення UDP і SMTP), які обмежують пропускну здатність мережі або атакують мережеві протоколи, повільні атаки DDoS спрямовані на програми.

Загальновідомо, що повільні DDoS-атаки можуть тривати непоміченими протягом тривалого часу через значну схожість з поведінкою легальних користувачів з повільним з'єднанням. Тому через складність процесу їх виявлення такі атаки потребують особливого розгляду [1].

2. Аналіз літературних даних і постановка проблеми

Повільна HTTP DDoS-атака на рівні програм включає багато неповних HTTP-запитів до сервера. Порівняно з іншими атаками, повільні атаки HTTP DDoS достатньо важко виявити, оскільки [2]:

джерелом атаки може бути цілком лояльний користувач;

для атаки не потрібна широка пропускна смуга каналу зв'язку;

атака спрямована на виснаження програмних ресурсів шляхом імітації повільного з'єднання у мережі.

Зараз існує три типи повільних HTTP DDoS-атак:

• Повільний заголовок HTTP або атака Slowloris. Під час такої атаки веб-браузер надсилає HTTP-запити GET разом із HTTP-заголовком.

• Повільна атака HTTP Body або aRe-yoU-Dead-Yet (RUDY). Ця атака містить запити HTTP POST із повним заголовком, але поле довжини містить настільки велике значення, що сервер резервує всі виділені ресурси для отримання всього повідомлення.

• Повільне читання HTTP. Це тип повільної HTTP-атаки, коли зловмисники надсилають HTTP-запити GET із відповідним заголовком і тілом на веб-сервер. Суть атаки полягає в тому, щоб читати відповідь дуже повільно.

Як бачимо, виявлення повільної HTTP-атаки є значною проблемою, оскільки поведінка зловмисника може імітувати поведінку законного користувача з повільними ресурсами. Фільтрування такої поведінки є значним, хоча наслідки можуть бути схожі на звичайні DDoS-атаки – відмова в обслуговуванні значної кількості законних користувачів мережі.

Проблемі протидії повільним DDoS-атакам присвячено значну кількість робіт.

У [3] авторами запропоновано архітектуру контролера SDN для розпізнавання повільних HTTP-атак. Їх підхід базується на тому, що під час ідентифікації система розраховує швидкість передачі пакетів і рівномірність відстані між пакетами. У разі перевищення зазначених показників деяких встановлених середніх значень робиться висновок про наявність нападу. У роботі [4] розглядається загальний механізм захисту від повільних DDoS-HTTP атак. Тут вперше вводиться параметр кількості підключень і тривалості підключення. В публікації [5] показано підхід до відбору даних, на основі якого можна створити ефективні механізми класифікації повільних HTTP DoS-атак. При цьому автори зазначають, що для досягнення високої ефективності розпізнавання необхідно використовувати майже 2 мільйони шаблонів атак, реалізувати які в реальному житті досить складно. Найбільш прийнятним є метод, запропонований у [6], який базується на параметрах TCP-з'єднань. Для цього вони використовували статистику спостережень і результати прогнозів. При цьому прогнозування в такій моделі базується на лінійних трендах, що дозволяє реалізувати його лише на короткі проміжки часу. В публікації [7] представлені можливості хмарної платформи OpenStack для аналізу та оцінки DDoS-атак. Цей підхід є одним з найпростіших і доступних, однак існують певні труднощі з впровадженням заходів протидії повільним DDoS-атакам у хмарі.

Патерни трафіку досліджуються в [8], де запропоновано алгоритм виявлення повільних DDoS-атак залежно від стану завантаження сервера. Такий підхід достатньо ефективний для постфактологічного аналізу, але не дозволяє прийняти рішення про наявність чи відсутність атаки. У [9] була запропонована хмарна тестова модель OpenStack для оцінки DDoS-атак у хмарному середовищі. У цій роботі досліджено різні можливості атак для програм, що працюють у хмарному середовищі. Результати, запропоновані в [9], були продовжені в [10] для виявлення, пом'якшення та запобігання повільним HTTP-атакам DDoS у хмарі. Найбільш перспективним є підхід, запропонований тими ж авторами в [11], де вони досліджують новий метод і модель класифікації для захисту від повільних HTTP-атак у хмарі. У статті

запропоновано чотиризонну архітектуру виявлення атак на основі аналізу двох параметрів: кількості підключень до сервера та середнього часу затримки відповіді клієнта.

Таким чином, більшість робіт із протидії повільним DDoS-атакам базуються на статистичних моделях, не стосуються прогнозування поведінки хоста, а отже, недостатньо ефективні для виявлення атак на ранніх стадіях.

Питання прогнозування трафіку для виявлення DDoS-атаки вже розглядалися в [12–15], де запропоновано модель прогнозу на основі декомпозиції випадкового процесу. В якості аргументу у цих роботах використовується загальний мережевий трафік і затримки відповіді користувача, які визначають індивідуальну поведінку користувача. У цих роботах реалізовано однопараметричний підхід, заснований лише на одному факторі, який визначає сутність повільної DDoS-атаки.

3. Мета і задачі дослідження

Метою дослідження є розробка моделі для діагностування повільної DDoS-атаки при спільному використанні двох параметрів: кількості відкритих з'єднань і середньої затримки між переданими пакетами.

Для досягнення поставленої мети вирішено такі завдання:

– розроблено архітектуру класифікатора повільних HTTP DDoS атак;

– запропоновано методику виявлення повільних DDOS атак на основі кореляційного аналізу та прогнозу параметрів;

– розроблено алгоритм виявлення повільної DDoS-атаки на основі прогнозування двох параметрів;

– здійснено моделювання двопараметричного алгоритму виявлення повільних DDOS атак на основі прогнозування та оцінено його ефективність.

4. Архітектура класифікатора повільних HTTP DDoS атак

У [13] запропоновано рішення на основі чотириступеневої зональної архітектури класифікації споживачів. Запит від будь-якого клієнта до веб-сервера класифікується за будь-яким станом зони в будь-який момент часу за допомогою багатоетапної зональної моделі. Модель багатоступеневої архітектури зональної класифікації показана на рисунку 1. Спочатку всі вхідні запити відстежуються на їх активність у блоці моніторингу. У разі правомірної поведінки клієнтів запит направляється в зелену зону. Із зеленої зони всі клієнтські запити пересилаються на веб-сервер.

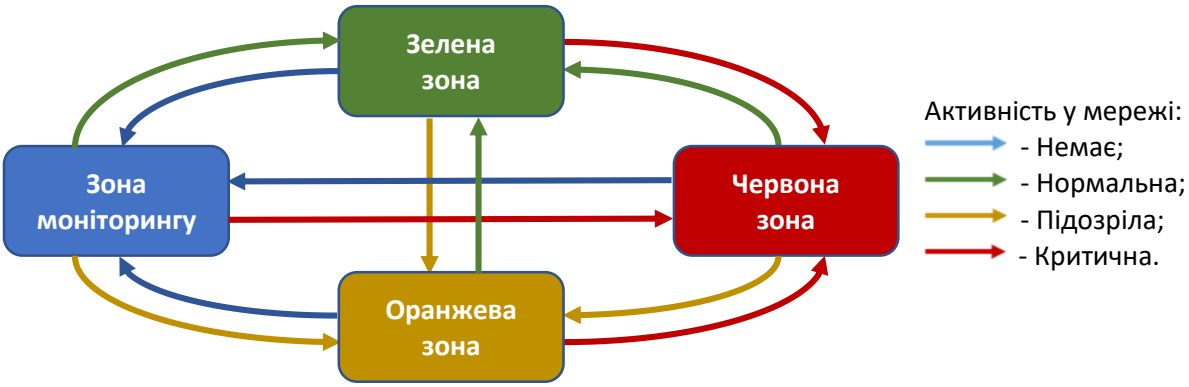


Рис. 1. Багатоступенева архітектура класифікатора HTTP DDoS атак

У разі підозрілої активності клієнта (відкриття більшої кількості з'єднань, надсилання частих GET-запитів із неповним заголовком, POST-запитів із меншою кількістю байтів із довшим інтервалом перед часом переходу), такі запити переміщуються в помаранчеву зону блоку та продовжують підлягати моніторингу. Клієнти, які виглядають підозріло в блоці моніторингу, зеленій або помаранчевій зоні (наприклад, під час відкриття великої кількості запитів на з'єднання, яке у 8 разів перевищує деяке середнє значення, запити на з'єднання з

неповним заголовком, запити на публікацію з кількома байтами або запит до Сервера з інтервалом, наприклад понад 80% від максимального інтервалу), вважаються DDoS-атаками, і такі клієнти потрапляють у червону зону. Будь-які звернення клієнтів із червоної зони блокуються. Клієнти із зеленої, помаранчевої чи червоної зон без активності або без активного запиту на підключення повертаються назад до блоку моніторингу. Клієнт із зеленої зони, який постійно виявляє підозрілу активність, переходить в помаранчеву зону, і навпаки - якщо клієнт після входу в помаранчеву зону проявляє нормальну активність, він переходить в зелений блок.

Щоб розпізнати повільну DDoS-атаку HTTP на веб-сервер, зональна модель використовує:

• Кількість підключень (NC), дозволена для кожного клієнта.

• Середня реальна мережева затримка (ARNL) доступності клієнта.

Клієнти, які намагаються відкрити в 6 разів більше дозволених з'єднань, підлягають ретельному моніторингу. Тут модель надсилає клієнту 5 запитів ping. Відповідь ping використовується для обчислення середньої затримки мережі. Значення ARNL порівнюється із середнім часом інтервалу запиту клієнта. Клієнти з повільними запитами, що перевищують 0,8 максимально допустимого ARNL, вважаються атакою та переходять до червоного блоку. Клієнти, які намагаються відкрити в 6–8 разів більше дозволених з'єднань і мають середню затримку запиту в 0,6–0,8 разів від максимально допустимого ARNL, переходять на помаранчевий блок. Клієнти в цьому стані залишаються під наглядом і відповідно класифікуються на основі постійного аналізу поведінки. Клієнти з менш ніж 6-кратним середнім підключенням і затримкою підключення до 0,6 відносно максимально допустимого ARNL знаходяться в зеленій зоні.

Система зберігає щойно підключений клієнт у блоці моніторингу для ідентифікації моделі активності та переходить у будь-який із станів на основі своєї поведінки, визначеної вище. Коли клієнт намагається відкрити в 6 разів більше підключень, ніж середня кількість, або час відповіді такому клієнту перевищує 0,6 максимально допустимого часу очікування, така активність клієнта виявляється підозрілою. Небезпечною вважається діяльність, коли кількість відкритих з'єднань перевищує середнє значення у 8 разів, а час відгуку перевищує 0,8 від максимального значення.

Протидія таким нападам має включати два першочергових заходи: 1) діагностувати напад на самих ранніх стадіях; 2) відокремити шкідливу поведінку користувача від нормальної поведінки. Розуміючи, які запити користувачів є результатом DDoS-атаки, ви можете налаштувати параметри брандмауерів, маршрутизаторів або інші заходи безпеки.

Проблема раннього виявлення низьких або повільних DDoS-атак залишається актуальною. Чим швидше ми виявимо, що параметри трафіку несумісні з нормальними значеннями, тим швидше можна буде вжити заходів для нейтралізації атаки. Тут необхідно додати модулі прогнозування параметрів до існуючих систем виявлення. Слід зазначити, що параметри NC і ARNL є незалежними і під час атаки можуть відбуватися як окремо, так і разом. Крім того, такі атаки, як Slow HTTP Headers, досить важко виявити через ARNL, оскільки в цьому випадку час відповіді сервера буде максимальним, а зловмисник впливає на сервер переважно через значну кількість з'єднань. Для організації успішної відповіді на такі атаки необхідно організувати систему, яка б дозволяла паралельно аналізувати обидва фактори. Найбільш цікавими є випадки сумісного використання зловмисником обох факторів, використовуючи різні стратегії їх поєднання.

5. Методика виявлення повільних DDOS атак на основі кореляційного аналізу та прогнозу параметрів

5.1. Налаштування трафіку для виявлення повільної DDoS-атаки

Більшість робіт із протидії повільним DDoS-атакам базуються на статистичних моделях і не стосуються прогнозування поведінки хоста, а отже, недостатньо ефективні для виявлення атак на ранніх стадіях.

Ця робота формує систему виявлення повільних DDoS-атак на основі прогнозування елементів трафіку в мережі. Як уже зазначалося, особливий інтерес становлять випадки, коли обидва фактори (NC і ARNL) використовуються разом. Цей варіант являє собою комбіновану атаку, яка є більш складною, ніж у разі одноразового застосування окремих факторів. Для успішного вирішення виявленої проблеми необхідно побудувати модель і технологію прогнозування поведінки параметрів трафіку з урахуванням історії взаємодії хостів у мережі, а також запропонувати технологію розпізнавання комбінованих повільних DDoS-атак.

Архітектура, запропонована в [14], є найбільш прийнятною для виявлення повільних DDoS-атак. Така IDS повинна складатися з чотирьох модулів: 1) Модуль збору трафіку; 2) Розрахунковий модуль; 3) Модуль прогнозування; 4) Модуль виявлення атак.

Система працює наступним чином:

1. Модуль збору трафіку протягом деякого часу записує основні параметри, необхідні для подальших розрахунків: IP-адреси відправника та одержувача; розмір вікна TCP; кількість відкритих з'єднань; час прибуття посилки.

2. Для кожної IP-адреси обчислювальний модуль підраховує: кількість відкритих з'єднань і середню затримку між переданими пакетами

$$\bar{T} = \frac{1}{k-1}\sum_{i=1}^{k}(t_{i+1} - t_i), \quad (1)$$

де:

t_i – час прибуття i-го пакету;

t_{i+1} – час прибуття $i+1$-го пакету;

k – кількість пакетів, отримана за аналізований період.

Початок і кінець сесії фіксуються вбудованим таймером, після чого розраховується тривалість затримки між пакетами.

3. Модуль виявлення атак приймає рішення про можливу повільну HTTP-атаку на основі порівняння отриманих показників із середньостатистичними значеннями. Зокрема, якщо клієнти намагаються відкрити в 6–8 разів більше, ніж середня кількість з'єднань, і/або середня затримка часу запиту в 0,6–0,8 разів перевищує максимально допустимий ARNL, то такий клієнт належить до помаранчевої зони. Клієнти в цьому стані залишаються під наглядом і відповідно класифікуються за результатами постійного аналізу поведінки. Якщо кількість підключень перевищує допустиму кількість у 8 разів і/або середня затримка часу запиту становить від 0,8 до 1,0 від максимально допустимого ARNL, клієнт належить до червоної зони.

Однак, як показано в [14], рішення про повільну DDoS-атаку доцільніше приймати на основі прогнозу параметрів трафіку, що дозволить очікувати такі атаки протягом деякого часу та вживати відповідних заходів. Такий підхід реалізовано в модулі прогнозування IDS.

5.2. Методика прогнозування параметрів повільної DDoS-атаки

Взаємодія комп'ютерних систем у мережі формує індивідуальну траєкторію поведінки користувача для кожної пари взаємодій. Такі траєкторії мають свої особливості як у звичайному режимі, так і під час повільної DDoS-атаки. Для своєчасного вжиття заходів щодо нейтралізації повільної DDoS-атаки необхідно передбачити часову траєкторію поведінки користувача, яка залежить від дій взаємодіючої системи. Прогнозування окремої траєкторії часового ряду ми вже вивчали в [15], де перевіряли параметри руху через великі інтервали (тиждень або місяць). Той самий підхід був використаний для прогнозування повільних DDoS-атак у [14]. В обох випадках розглядалися лише окремі показники: у [15] – кількість інформації в одиницю часу, у [14] – середня затримка між переданими пакетами. В обох випадках була запущена модель прогнозу з одним параметром, і ми досліджували лише один параметр трафіку. Повільні DDoS-атаки характеризуються невеликими відхиленнями в трафіку, тому для їх виявлення необхідно використовувати NC і ARNL як прогностичні

фактори. Тут ми можемо виконати оцінку NC відносно деякого середнього значення, і ми можемо виміряти ARNL відносно максимального часу підключення, дозволеного системою. Крім прямих значень (кількість з'єднань і середній час затримки), необхідно також розрахувати значення кореляційної функції для кожного з вимірювань за допомогою методу канонічної декомпозиції випадкового процесу, що робить метод більш ефективним для прогнозування слабких збурень.

Для моніторингу параметрів атаки, як і в [14], будемо використовувати NC та ARNL, які можуть сформувати вектор параметрів $X = (X_1, X_2, \dots, X_H)$ де $X_i = \{X_{NC_i}, X_{ARNL_i}\}$. Виконання умови $X \in S_0$, де S_0 – область допуску вектора X. Випадковий процес $X(t)$ відображає зміну параметрів у часі. процес $X(t)$ статистично визначається в діапазоні $t \geq t_1$, де t_1 є початком спостережень і $t_k \geq t_1$.

Поставимо задачу прогнозування так: для параметра $x_\omega(t) \in S_0$, який спостерігається в інтервалі $t_1 \leq t \leq t_k$, нам потрібно визначити час випуску конкретної реалізації $x_\omega(t)$ поза межами S_0 на основі розрахунку апостериорного процесу $X(t)$. Імовірність того, що певна траєкторія параметра ω гарантовано потрапляє в допустимий діапазон $s \leq t_k$, якщо до того часу t_k в тому числі було описано його стан as $x_\omega(t), t_1 \leq t \leq t_k$, буде

$$P^{ps}(s) = P\{X(s) \in S_0 / x_\omega(t)\}, t_1 \leq t \leq t_k, s \leq t_k. \quad (2)$$

Для вирішення задачі прогнозування досліджуваного процесу необхідно представити формулу

$$X(t) = m(t) + \sum_v V_v \varphi_v(t), \quad (3)$$

де $m(t)$ – середня функція процесу;

$\varphi_v(t)$ – невипадкові (координатні) функції часу;

V_v – випадкові, некорельовані коефіцієнти $M[V_v] = 0$, $M[V_v, V_\mu] = 0$, $v \neq \mu$.

Це уявлення, запропоноване в [14, 15], дозволяє застосовувати його до будь-якого параметра трафіку, який можна визначити як часовий ряд. Процес $X(t)$ можна розглядати як випадкову послідовність $X(t_i) = X(i), i = \overline{1, I}$ в дискретній серії спостережень t_i:

$$X(i) = m(i) + \sum_{v=1}^{i} V_v \varphi_v(i), i = \overline{1, I}, \quad (4)$$

де V_v – випадковий коефіцієнт з параметрами $M[V_v] = 0$, $M[V_v, V_\mu] = 0$, $v \neq \mu$; $M[V_v^2] = D_v$;

$\varphi_v(i)$ – невипадкова координатна функція, $\varphi_v(v) = 1$, $\varphi_v(i) = 0$ на $v > i$.

Формули дисперсії та кореляційної функції можна записати як

$$D(i) = \sum_{v=1}^{i} D_v \varphi_v^2(i), i = \overline{1, I}, \quad (5)$$

$$D(i, j) = \sum_{v=1}^{\inf(i,j)} D_v \varphi_v(i) \varphi_v(j), i, j = \overline{1, I}. \quad (6)$$

Таким чином, подання випадкових параметрів (2) дозволяє вирішити задачу виявлення повільної DDoS-атаки на основі прогнозування поведінки самих параметрів. Якщо використовується більше ніж один незалежний параметр, операція виконується відповідно до вектора параметрів.

5.3. Алгоритм виявлення повільної DDoS-атаки на основі передбачення двох параметрів

Для виявлення повільних DDoS-атак за підходом (1) – (6) ми пропонуємо наступний алгоритм для комбінованого прогнозування кількості з'єднань і затримок між переданими пакетами.

0. **Start**

1. $X(t) \leftarrow X(t), t = \overline{1,T}$ – формування масиву спостережень процесу $X(t)$, $X_i = \{X_{NC_i}, X_{ARNL_i}\}$.

2. $x(\mu) \leftarrow x(\mu), \mu = \overline{1,k}$ – формування масиву результатів контролю.

3. $L \leftarrow Length[X(t)], X_i = \{X_{NC_i}, X_{ARNL_i}\}$ – визначення кількості спостережуваних траєкторій.

4. $m(t) \leftarrow Mean[X(t)],\ X_i = \{X_{NC_i}, X_{ARNL_i}\}$ – обчислення середнього значення функції $X(t)$.

5. $c \leftarrow Covariance[X(t)], X_i = \{X_{NC_i}, X_{ARNL_i}\}$ – обчислення коваріаційної матриці для $X(t)$.

6. $d \leftarrow Variance[X(t)],\ X_i = \{X_{NC_i}, X_{ARNL_i}\}$ – обчислення масиву дисперсій процесу $X(t)$.

7. $\varphi \leftarrow Table[0, \{T\}, \{T\}]$ – собчислення початкового значення координатних функцій.

8. $\hat{X}(t) = X(t) - m(t), t = \overline{1,T}$ – центрування вихідних даних.

9. $V(t) = X_l(t) - m(t), t = \overline{1,T}, l = \overline{1,L}$ – обчислення початкових значень випадкових коефіцієнтів.

10. $\varphi_1 = \frac{c_{1,j}}{d_1}, j = \overline{1,T}$ – визначення першої координатної функції.

11. **For** $i = 1$ to $i = T$

12. $d_i = c_{i,i} - \sum_{j=1}^{i-1} \varphi_{i,j}^2\, d_j$ – перевизначення дисперсії.

13. **For** $j = 1$ to $j = T$

14. $\varphi_i = \frac{1}{d_1}\left(c_{i,j} - \sum_{l=1}^{i-1} d_l \varphi_{i,l} \varphi_{j,l}\right)$ – перевизначення координатних функцій.

15. **end for** j

16. **end for** i

17. **For** $i = 2$ to $i \le T$

18. **For** $k = 1$ to $k < i$

19. $\varphi_{i,k} = 0$ – перевизначення координатних функцій випадкового процесу.

20. **end for** k

21. **end for** i

22. **For** $i = 2$ to $i \le T$

23. **For** $l = 1$ to $l = L$

24. $V_{l,i} = \hat{X}_{l,i} - \sum_{k=1}^{i-1} V_{l,k} \varphi_{k,i}$ – обчислення випадкових коефіцієнтів.

25. **end for** l

26. **end for** i

27. $p_s \leftarrow Length[x(\mu)]$ – визначення розміру масиву результатів контролю.

28. $M_1 = Table[m_i + (x_1 - m_1)\varphi_{1,i}, \{i = \overline{1,T}\}]$ – обчислення початкової прогнозованої траєкторії.

29. **For** $h = 2$ to $h = p_s$

30. $M_h = Table[M_{h-1,i} + (x_h - M_{h-1,h})\varphi_{h,i}, \{i = \overline{1,T}\}]$ – розрахунок контрольних точок прогнозу.

31. **end for** h

32. $X_{forecast} = Table[M_{k,i} + \sum_{j=k+1}^{i} V_{k,j}\varphi_{k,j}, \{k = \overline{1,p_s}, i = \overline{1,T}\}]$ – обчислення прогнозованої траєкторії.

33. **Stop**

Алгоритм здійснює двовимірне передбачення параметрів поведінки користувача. Враховуючи незалежність параметрів NC і ARNL один від одного (оскільки атака може розвиватися як за одним параметром, так і комбіновано), це дає можливість побудувати двопараметричний класифікатор за вищевказаними критеріями. Розроблений алгоритм

методу дозволяє точно виконати випадковий процес у контрольних точках і забезпечити мінімальний середньоквадратичний похибки апроксимації в інтервалах між цими точками.

У результаті застосування алгоритму можна побудувати прогноз розвитку одного або обох параметрів одночасно і застосувати момент, коли окремий параметр виходить за межі критичних значень. Якщо параметр показує перехід у помаранчеву або червону зону, що говорить про можливість вільної DDoS-атаки, необхідно вжити заходи безпеки. Рішення про початок повільної DDoS-атаки має прийматися для IP-адрес кожного відправника на основі порівняння прогнозованого NC та/або ARNL з критичними значеннями, щоб завантажити, коли параметр потрапляє в критичну зону. Наявність у моделях середньої кількості запитів і максимального часу поведінки відповіді на запит дозволяє розглядати індивідуальну взаємодіючих хостів у порівнянні з поведінкою інших хостів в аналогічних ситуаціях з повними DDoS-атаками.

6. Моделювання двопараметричного алгоритму виявлення повільних DDOS атак на основі прогнозування

Було проведено моделювання виявлення DDoS-атаки за допомогою архітектури хмарного середовища OpenStack із фіксацією параметрів за допомогою Wireshark. Атаки Slow HTTP Headers аналізувалися за допомогою параметра NC, а також атаки Slow HTTP Body і Slow HTTP Read одночасно NC і ARNL. Як і в [13], були взяті параметри, які використовуються для цих атак: загальна кількість підключень (NCtotal = 10000); інтервал між контрольними даними (ARNLmax = 10 seconds). Оцінювали можливості методу за співвідношенням NC та ARNL, які розраховували за формулами $NC_{Rate} = NC_{Current}/NC_{Total}$ та $ARNL_{Rate} = ARNL_{Current}/ARNL_{Max}$.

На рис. 2 показані початкові шаблони атак. Тут початкові значення спостережень є окремими точками часового ряду. Напади можуть розвиватися як по одному з параметрів, так і в комбінації, по двох параметрах одночасно. Багатоступеневий зональний класифікатор визначає підозрілу або зловмисну поведінку користувача, розміщуючи траєкторії в помаранчевій або червоній зонах за частотою NC або ARNL.

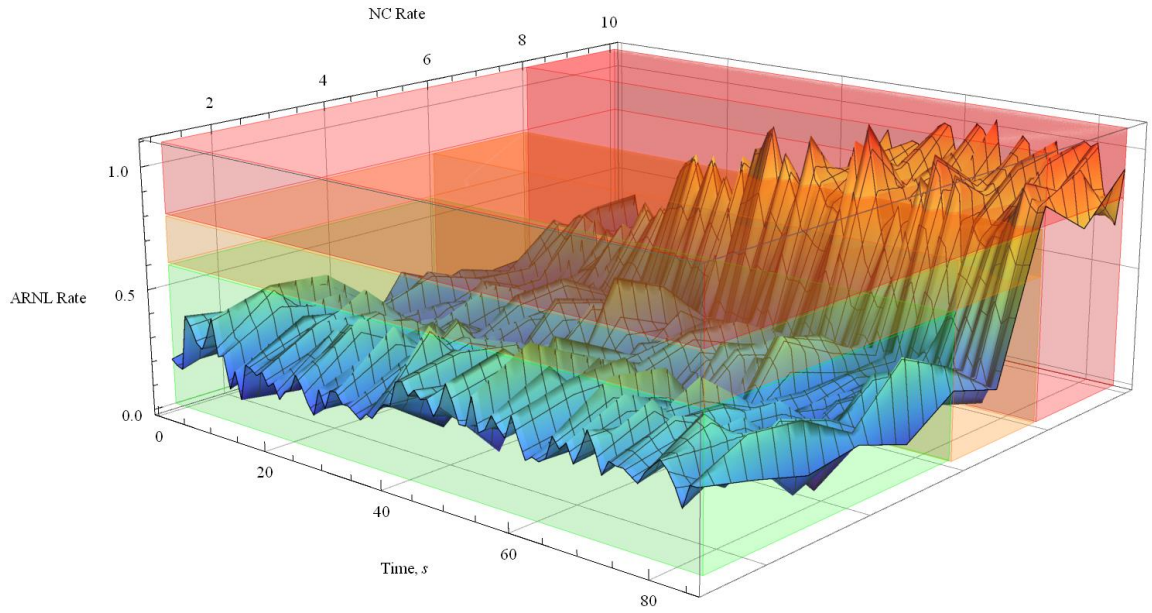


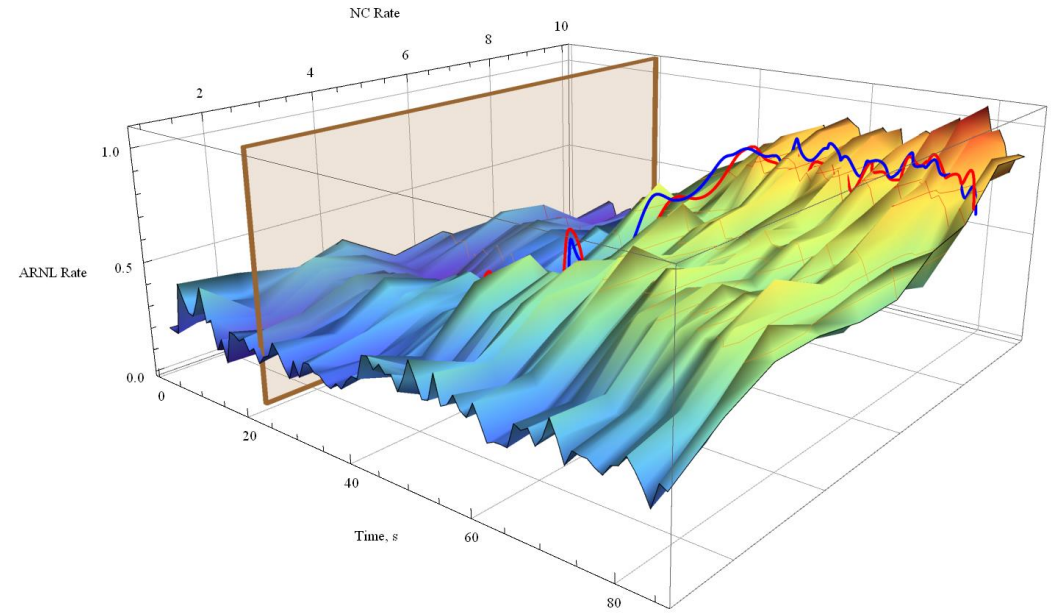
Рис. 2. Статистика спостереження повільної HTTP DDoS-атаки

Модуль прогнозування IDS, використовуючи алгоритм прогнозування, застосований до апріорного процесу, приймає рішення про підозрілу або зловмисну поведінку на основі результатів прогнозу. Оскільки на фоні досліджуваного процесу розвиток процесу може

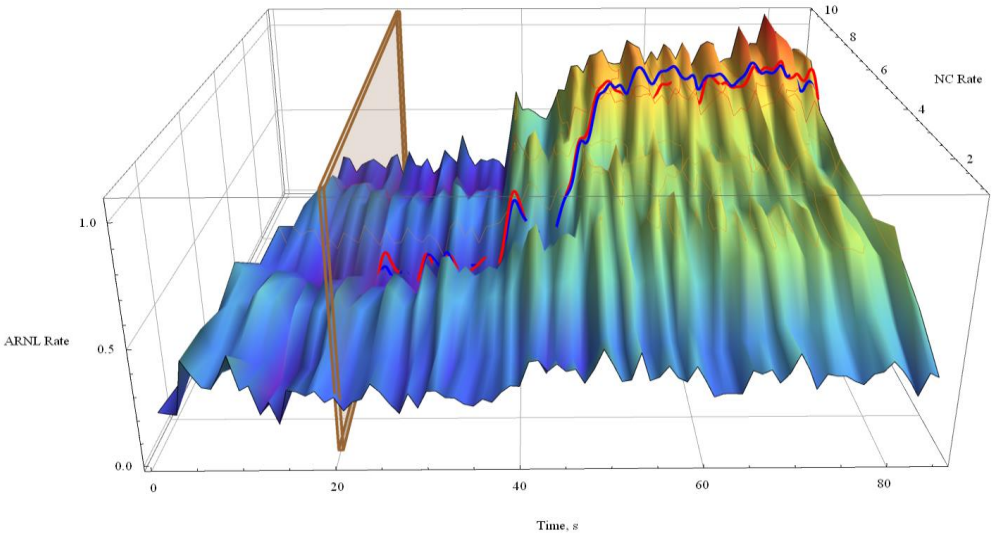
призводити далі до кількох траєкторій. Прогнозувати атаку означає визначити момент часу, коли крива потрапляє в одну з критичних зон.

Заслуговує на увагу дослідження окремої траєкторії прогнозу. Отже, якщо взяти за основу одну конкретну траєкторію (червона лінія на рис. 3) і побудувати прогноз (синя лінія), то можна побачити, що метод дає досить точний результат, який залежить від часу апріорного спостереження.

Як ми зазначали в [14–15] кількість початкових спостережень впливає на точність прогнозу. На рис. 3а і 3б поле кривих показує, як будуть працювати прогнози при отриманні даних з інших контрольних точок перед прогнозним моментом (20 с). Імовірність помилки у виборі правильної траєкторії залежить від кількості спостережуваних необроблених даних. Логічно припустити, що в цьому випадку точність прогнозу буде занадто сильно залежати від особливостей поведінки траєкторії, що призводить до аномального руху, а також від спостережуваної частоти аномалій. Таким чином, метод «вибирає» потрібну траєкторію залежно від точки входу та середньої траєкторії.



а)



б)

Рис. 3. Дослідження окремої траєкторії прогнозу:
а) двопараметричний вигляд; б) вигляд ARNL

Важливе питання полягає в тому, як залежить точність прогнозування від кількості апріорних спостережень. Це питання розглядалося в [14], де було показано, що через 60 ... 90 с відхилення прогнозованої траєкторії від контрольної зменшується до 5 ... 0 %. Це підтверджує адекватність моделі прогнозування для виявлення повільних DDoS-атак на основі двопараметричних прогнозів.

7. Висновки

Повільні HTTP DDoS-атаки залишаються досить складними для виявлення через незначні зміни в параметрах трафіку. Поведінка зловмисників, які імітують поведінку законних користувачів, спричиняє розвиток складних технологій виявлення атак. Існуючі методи виявлення повільних DDoS-атак, засновані на штучному інтелекті, вимагають значних статистичних даних для навчання. Однак, як було доведено в цій публікації, більш перспективними є методи, засновані на прогнозуванні поведінки користувача за кількістю підключень і часом середньої реальної затримки мережі.

Прогнозування параметрів поведінки користувача дозволяє заздалегідь виявляти повільні DDoS-атаки на основі алгоритму пошуку невідомих майбутніх значень для часового ряду параметрів. Використання відносних значень NC і ARNL як параметрів прогнозу дає можливість побудувати гнучку систему розпізнавання, адаптовану до специфіки конкретної системи. Запропонований метод є поєднанням штучного інтелекту та статистичного аналізу та використовує алгоритм самонавчання з достатньою статистикою атак.

Подальші дослідження щодо протидії повільним HTTP DDoS-атакам можуть бути присвячені питанням багатовимірного прогнозування на інтервалах, що не охоплюються статистикою, шуму даних і для випадку довільної кількості параметрів.

Список використаної літератури

1. Mohammad Fakrul Alam, "Application Layer DDoS, A Practical Approach & Mitigation Techniques, “South Asian network Operators Group (SANOG) -23 Conference, Thimpu, Bhutan, 2014.

2. G. Agosta, S. Chiocchio, E. Cinque, P. Fezzardi, M. Mongelli, A. Persia, M. Pratesi, and F. Valentini. Toward a v2i-based solution for traffic lights optimization. In 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pages 1--6, 2019.

3. Hong, Kiwon & Kim, Younjun & Choi, Hyungoo & Park, Jinwoo. (2017). SDN-Assisted Slow HTTP DDoS Attack Defense Method. IEEE Communications Letters. PP. 1-1. 10.1109/LCOMM.2017.2766636.

4. Y. -C. Wang and R. -X. Ye, "Credibility-Based Countermeasure Against Slow HTTP DoS Attacks by Using SDN," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 0890-0895, doi: 10.1109/CCWC51732.2021.9375911.

5. L. Calvert, and T. M. Khoshgoftaar. Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data. Journal of Big Data, 6 (2019). doi:10.1186/s40537-019-0230-3.

6. Є. В. Дуравкін, А. Карлссон, А. С. Локтіонова. Метод виявлення повільної атаки. Системи обробки інформації, випуск 8 (124), с. 102-106, 2014.

7. A. Bhardwaj, A. Sharma, V. Mangat, K. Kumar and R. Vig. Experimental Analysis of DDoS Attacks on OpenStack Cloud Platform, in: Proceedings of 2nd International Conference on Communication, Computing and Networking, Lecture Notes in Networks and Systems, 46 (2019). doi:10.1007/978-981-13-1217-5_1.

8. І.В. Рубан, Д.В. Прибильнов, Е.С. Лошаков. Метод виявлення низькошвидкісної атаки типу «відмова в обслуговуванні». Наука і техніка Повітряних Сил ЗС України, № 4(13). 85-88, 2013.

9. A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience, 20/4 (2019) 669–685. doi:10.12694/scpe.v20i4.1569.

10. A. Dhanapal, and P. Nithyanandam. The slow HTTP Distributed Denial of Service Attack Detection in Cloud, Scalable Computing, 20/2 (2019) 285–297. doi:10.12694/scpe.v20i2.1501.

11. A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience, 20/4 (2019) 669–685. doi:10.12694/scpe.v20i4.1569.

12. V. Savchenko. Detection of Slow DDoS Attacks based on Time Delay Forecasting / Vitalii Savchenko, Valeriia Savchenko, Oleksandr Laptiev, Oleksander Matsko, Ivan Havryliuk, Kseniia Yerhidzei and Iryna Novikova // Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum "DIGITAL REALITY", September 13 − 19, 2021, Odesa, Ukraine.

13. V. Savchenko. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network / Oleksandr Laptiev, Nataliia Lukova-Chuiko, Serhii Laptiev, Vitaliy Savchenko, Tetiana Laptieva and Serhii Yevseiev // Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum "DIGITAL REALITY", September 13 − 19, 2021, Odesa, Ukraine.

14. V. Savchenko, O. Ilin, N. Hnidenko, O. Tkachenko, O. Laptiev, S. Lehominova. Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER), 8/5 (2020) 2019–2025. doi:10.30534/ijeter/2020/90852020.

15. V. Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, and A. Kotenko. Network traffic forecasting based on the canonical expansion of a random process. Eastern European Journal of Enterprise Technologies, 3/2(93) (2018) 33–41. doi:10.15587/1729-4061.2018.131471.

References

1. Mohammad Fakrul Alam, "Application Layer DDoS, A Practical Approach & Mitigation Techniques, "South Asian network Operators Group (SANOG) -23 Conference, Thimpu, Bhutan, 2014.

2. G. Agosta, S. Chiocchio, E. Cinque, P. Fezzardi, M. Mongelli, A. Persia, M. Pratesi, and F. Valentini. Toward a v2i-based solution for traffic lights optimization. In 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pages 1--6, 2019.

3. Hong, Kiwon & Kim, Younjun & Choi, Hyungoo & Park, Jinwoo. (2017). SDN-Assisted Slow HTTP DDoS Attack Defense Method. IEEE Communications Letters. PP. 1-1. 10.1109/LCOMM.2017.2766636.

4. Y. -C. Wang and R. -X. Ye, "Credibility-Based Countermeasure Against Slow HTTP DoS Attacks by Using SDN," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 0890-0895, doi: 10.1109/CCWC51732.2021.9375911.

5. L. Calvert, and T. M. Khoshgoftaar. Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data. Journal of Big Data, 6 (2019). doi:10.1186/s40537-019-0230-3.

6. Ie. V. Duravkin, A. Carlsson, and A. S. Loktionova. Method of Slow-Attack Detection. Information processing systems, 8 (2014), pp. 102-106. URL: http://nbuv.gov.ua/UJRN/soi_2014_8_24

7. A. Bhardwaj, A. Sharma, V. Mangat, K. Kumar and R. Vig. Experimental Analysis of DDoS Attacks on OpenStack Cloud Platform, in: Proceedings of 2nd International Conference on Communication, Computing and Networking, Lecture Notes in Networks and Systems, 46 (2019). doi:10.1007/978-981-13-1217-5_1.

8. I.V. Ruban, D.W. Pribylnov, and E.C. Loshakov. A method of detecting a low-speed denial-of-service attack. Science and technology of the Air Force of the Armed Forces of Ukraine, 4 (2013) 85–88. URL: http://www.hups.mil.gov.ua/periodic-app/article/549/nitps_2013_4_21.pdf

9. A. Dhanapal, and P. Nithyanandam. An OpenStack based cloud testbed framework for evaluating HTTP flooding attacks, Wireless Networks, (2019) 570–575. doi:10.1007/s11276-019-01937-4.

10. A. Dhanapal, and P. Nithyanandam. The slow HTTP Distributed Denial of Service Attack Detection in Cloud, Scalable Computing, 20/2 (2019) 285–297. doi:10.12694/scpe.v20i2.1501.

11. A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience, 20/4 (2019) 669–685. doi:10.12694/scpe.v20i4.1569.

12. Detection of Slow DDoS Attacks based on Time Delay Forecasting / Vitalii Savchenko, Valeriia Savchenko, Oleksandr Laptiev, Oleksander Matsko, Ivan Havryliuk, Kseniia Yerhidzei and Iryna Novikova // Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum “DIGITAL REALITY”, September 13 − 19, 2021, Odesa, Ukraine.

13. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network / Oleksandr Laptiev, Nataliia Lukova-Chuiko, Serhii Laptiev, Vitaliy Savchenko, Tetiana Laptieva and Serhii Yevseiev // Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum “DIGITAL REALITY”, September 13 − 19, 2021, Odesa, Ukraine.

14. V. Savchenko, O. Ilin, N. Hnidenko, O. Tkachenko, O. Laptiev, S. Lehominova. Detection of Slow DDoS Attacks based on User’s Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER), 8/5 (2020) 2019–2025. doi:10.30534/ijeter/2020/90852020.

15. V. Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, and A. Kotenko. Network traffic forecasting based on the canonical expansion of a random process. Eastern European Journal of Enterprise Technologies, 3/2(93) (2018) 33–41. doi:10.15587/1729-4061.2018.131471.