Прогнозування повільних DDoS атак на основі кореляційного аналізу індивідуальних траєкторій трафіку

Віталій Савченко[1,*,†], Галина Гайдур[1,†], Світлана Легомінова[1,†]

[1] Державний університет інформаційно-комунікаційних технологій, вул. Солом'янська, 7, 03110, Київ, Україна

Анотація

У статті досліджується проблема виявлення низькоінтенсивних та повільних розподілених атак типу "відмова в обслуговуванні" (DDoS), які становлять суттєву загрозу для сучасних інформаційних систем. На відміну від класичних об'ємних атак, що характеризуються різким зростанням інтенсивності мережевого трафіку, повільні атаки відзначаються прихованим характером дії та ускладненістю їх ідентифікації за стандартними методами моніторингу. У роботі висунуто припущення про залежність ефективності виявлення повільних атак від індивідуальних особливостей поведінки легітимних користувачів. Запропоновано метод, що ґрунтується на аналізі та прогнозуванні індивідуальної поведінкової траєкторії користувача у процесі його взаємодії з веб-сервісом. Практичні можливості цього підходу підтверджено шляхом моделювання атак типу RUDY на HTTP-сервіси, що дало змогу оцінити вплив обсягу накопиченого трафіку та статистичних характеристик атак на точність прогнозування. Отримані результати свідчать про перспективність запропонованого методу для виявлення широкого спектра повільних DDoS-атак та підвищення загального рівня захисту інформаційних ресурсів.

Ключові слова

повільна DDoS-атака, індивідуальна траєкторія, індивідуальне прогнозування, кореляційний аналіз, випадковий процес

1. Вступ

Доступність інструментів для пошуку мережевих вразливостей зумовила широке розповсюдження DDoS-атак. Ефективна протидія таким загрозам передбачає реалізацію двох ключових завдань: 1) своєчасне діагностування атаки на ранніх етапах її розвитку; 2) відокремлення шкідливого трафіку від легітимного. Ідентифікація запитів, що є результатом DDoS-атаки, створює можливість для налаштування параметрів брандмауерів, маршрутизаторів або застосування інших механізмів захисту. Особливістю повільних DDoS-атак є їх залежність від поведінкових характеристик окремого користувача, що ускладнює їх своєчасне виявлення. Тому, для підвищення ефективності заходів із нейтралізації таких атак, доцільним є детальне прогнозування індивідуальної поведінкової моделі користувача.

2. Визначення проблеми

Характерною особливістю повільних DDoS-атак є експлуатація вразливостей протоколу TCP, коли перебої у функціонуванні можуть бути зумовлені як навмисними діями зловмисників, так і ненавмисними затримками у каналі зв'язку. На відміну від об'ємних атак, повільні DDoS-атаки не спричиняють різкого зростання трафіку, що миттєво призводить до відмови в обслуговуванні сервера. Це ускладнює своєчасне виявлення

[1]Security of Modern Information & Communication Systems (SMI&CS-2025), October 16-18, 2025, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

savitan@ukr.net (V. Savchenko); gaydurg@gmail.com (H. Haidur); chiarasvitlana77@gmail.com (S. Lehominova)

0000-0002-3014-131X (V. Savchenko); 0000-0003-0591-3290 (H. Haidur); 0000-0002-4433-5123 (S. Lehominova)

моменту початку атаки та створює значні труднощі у відокремленні шкідливого трафіку від легітимного. Для ефективного виявлення та класифікації повільних атак необхідна розробка спеціалізованих підходів і методів. Ключовою проблемою ідентифікації повільних DDoS-атак є обмеженість традиційних механізмів запобігання, оскільки вони ґрунтуються на аналізі вже наявного трафіку без урахування можливості його прогнозування відповідно до поведінкової активності користувачів. У цьому контексті моделювання та прогнозування користувацької поведінки розглядається як перспективний напрям, що дає змогу виявляти аномальні дії та своєчасно реагувати на загрозу повільних DDoS-атак.

3. Аналіз дотичних робіт

В наукових публікаціях розглядаються різні підходи до виявлення повільних DDoS-атак. Зокрема, у [1, 2] запропоновано методи ідентифікації та класифікації повільних HTTP-атак у хмарних середовищах, однак вони не забезпечують своєчасного виявлення на ранніх стадіях. У роботах [3, 4] розроблено моделі, що ґрунтуються на швидкості передавання та інтервалах між пакетами, проте ці параметри не дозволяють випередити дії зловмисників. Дослідження [5] акцентує увагу на балансуванні вибірок даних для побудови класифікаторів, але передбачає використання нереалістично великих наборів атак. Метриковий підхід [6] демонструє ефективність за умов наявності великих обсягів однотипних даних, однак його результативність знижується при високій різноманітності атак. У [7] параметри TCP-з'єднань застосовуються для оцінки ймовірності перевантаження серверів, проте метод базується лише на статистичних спостереженнях. Алгоритм, представлений у [8], використовує шаблони трафіку залежно від завантаження сервера, але не враховує процедуру прийняття рішень.

У роботі [9] запропоновано метод виявлення атак типу RUDY, що ґрунтується на аналізі самоподібності мережевого трафіку, однак у дослідженні не враховано різноманітність навчальних вибірок та особливості формування навчальних даних. У [10] описано систему виявлення HTTP DTP-атак у хмарних середовищах із використанням індикаторів інформаційної ентропії та випадкових дерев; попри високу ефективність, такий підхід не забезпечує можливості прогнозування розвитку атаки. Узагальнення результатів попередніх досліджень свідчить, що більшість наявних рішень, спрямованих на протидію повільним DDoS-атакам, не враховують поведінкові аспекти користувачів, що обмежує їх придатність для раннього виявлення.

Метою даної роботи є розробка системи виявлення повільних DDoS-атак на основі кореляційного аналізу мережевого трафіку з урахуванням прогнозування індивідуальної поведінки користувачів. Для досягнення поставленої мети передбачається побудова моделі та технології прогнозування на основі історії взаємодії користувачів із сервером, а також визначення відповідної топології для розпізнавання атак.

4. Математичні основи кореляційного аналізу трафіку

Поведінкова активність користувача в мережі визначає індивідуальну траєкторію зміни параметрів його мережевого трафіку. Такі траєкторії є характерними як для легітимної взаємодії, так і для сценаріїв повільних DDoS-атак. Для своєчасного визначення моменту початку нейтралізації подібних атак необхідним є розв'язання задачі прогнозування індивідуальної часової траєкторії трафіку. У роботах [11 – 13] вже розглядалися підходи до прогнозування параметрів трафіку на основі індивідуальних траєкторій, однак ці підходи орієнтовані на великі часові інтервали (тиждень, місяць). Для завдань виявлення та класифікації повільних DDoS-атак необхідна значно вища точність, що зумовлює потребу у вдосконаленні наявних методів. Таким чином, постає задача прогнозування індивідуальної траєкторії параметрів мережевого трафіку з метою підвищення ефективності системи виявлення. Для її вирішення досліджуваний процес доцільно формалізувати у вигляді математичної моделі

$$X(t) = m(t) + \sum_{v} V_v \varphi_v(t), \tag{1}$$

де $m(t)$ – математичне очікування процесу; $\varphi_v(t)$ – невипадкові (координатні) функції часу; V_v – випадкові, некорельовані коефіцієнти ($M[V_v] = 0$, $M[V_v, V_\mu] = 0$, $v \neq \mu$).

Цей підхід можна застосувати до будь-якого параметра трафіку, який можна подати у вигляді часового ряду. Тоді процес $X(t)$ можна записати як послідовність $X(t_i) = X(i), i = \overline{1, I}$ у дискретній серії t_i:

$$X(i) = m(i) + \sum_{v=1}^{i} V_v \varphi_v(i), i = \overline{1, I} \tag{2}$$

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, $\varphi_v(v) = 1$, $\varphi_v(i) = 0$ поки $v > i$.

Формули для дисперсії та кореляційної функцій можна подати як

$$D(i) = \sum_{v=1}^{i} D_v \varphi_v^2(i), i = \overline{1, I}, \tag{3}$$

$$D(i, j) = \sum_{v=1}^{inf(i,j)} D_v \varphi_v(i) \varphi_v(j), i, j = \overline{1, I}. \tag{4}$$

Таким чином, подання випадкових процесів параметрів трафіку у вигляді (1) – (2) дозволяє виявити повільну DDoS-атаку на основі прогнозування індивідуальної поведінки користувача.

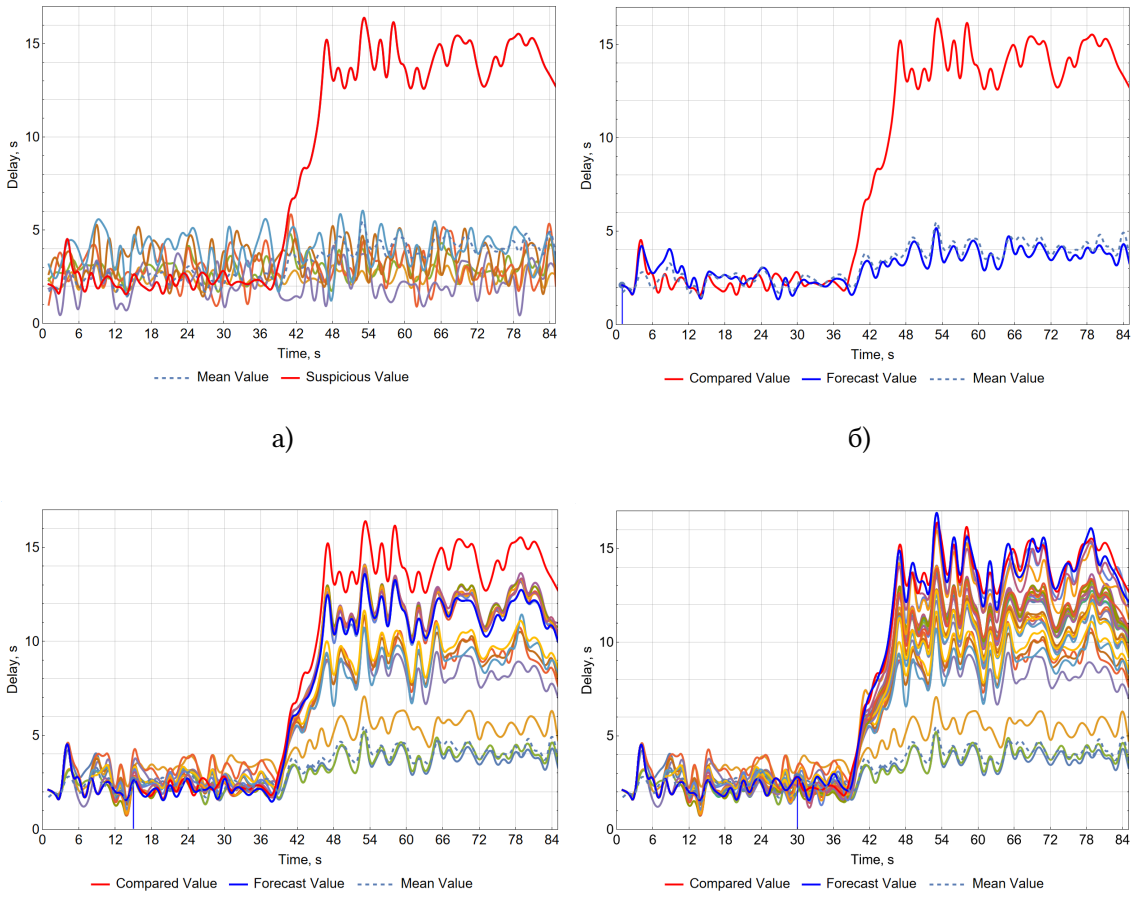
5. Моделювання та обговорення результатів

Моделювання процесу виявлення повільних DDoS-атак на основі прогнозування параметрів трафіку здійснювалося на прикладі атаки типу RUDY, яка спрямована на мережевий сервер і викликає відмову у його роботі шляхом надсилання надзвичайно довгих запитів. Реалізація атаки передбачає попереднє сканування цільового веб-ресурсу з метою виявлення вбудованих форм, після чого здійснюється надсилання легітимних HTTP POST-запитів із аномально великим значенням поля заголовка content-length. Передавання даних відбувається по одному байту в пакеті, що ускладнює ідентифікацію атаки через мінімальні коливання у вхідному трафіку.

Для спрощення було розглянуто окремий сценарій атаки на фоні легітимного трафіку (рис. 1,а). У якості контрольного параметра використовувалася середня затримка між переданими пакетами. До наведеного процесу (рис. 1) було застосовано методику прогнозування (1) – (4), використавши як початкові дані окремі точки часового ряду, що відповідають частковій траєкторії № 1 (рис. 2, червона крива). У цьому випадку спостереження при t = 1, 15, 30 с було взято як вихідні дані.

Результати прогнозування для t = 1 с наведені на рис. 1,б. Обмежена кількість початкових даних дає змогу відтворити лише усереднений перебіг процесу, тоді як прогнозовані значення істотно відрізняються від контрольної траєкторії. Таким чином, використання лише середніх параметрів трафіку та точки входу у прогноз не забезпечує точного передбачення подальшої поведінки системи. Запропонований метод формує відповідну траєкторію на основі поєднання початкових спостережень із усередненою траєкторією.

Збільшення обсягу спостережень до моментів часу t = 15 с та t = 30 с (рис. 1,в,г) забезпечує підвищення достовірності подальшого прогнозування, причому для t = 30 с результати можна вважати достатньо точними. На рис. 1,в та 1,г криві різних кольорів ілюструють можливі сценарії прогнозування у випадку використання даних з альтернативних контрольних точок, що передують моменту t. Таким чином, ймовірність похибки у виборі коректної траєкторії безпосередньо залежить від кількості початкових спостережень. Водночас доцільно зазначити, що у даній ситуації точність прогнозування істотно визначається особливостями поведінки траєкторії, яка зумовлює виникнення аномальних відхилень, а також частотою появи таких аномалій.



а) б)

в) г)

Рисунок 1: Прогнозування повільних DDoS-атак на основі кореляційного аналізу трафіку

6. Висновки

Повільні DDoS-атаки набувають дедалі більшого поширення завдяки відносній простоті їх реалізації та складності своєчасного виявлення. Існуючі методи детектування характеризуються низькою ефективністю через затримку реакції, що виникає у разі використання лише спостереження та аналізу параметрів трафіку. Перспективнішим підходом у цьому контексті є прогнозування поведінки користувачів на основі статистичних даних попередніх атак.

Використання прогнозування індивідуальної поведінки користувачів дає змогу розв'язати проблему ідентифікації повільних DDoS-атак шляхом пошуку невідомих майбутніх значень часових рядів параметрів трафіку. Запропонований метод поєднує можливості штучного інтелекту та статистичного аналізу, що забезпечує самонавчання системи в умовах поповнення новими статистичними даними атак. Такий підхід дозволяє

точно визначати характеристики випадкового процесу у контрольних точках та мінімізувати середньоквадратичну похибку апроксимації в інтервалах між ними.

Подальші дослідження у сфері протидії повільним DDoS-атакам можуть бути спрямовані на вдосконалення запропонованого методу, зокрема на забезпечення прогнозування у часових інтервалах, що виходять за межі доступної статистики. Це включає умови підвищеного рівня шуму даних або їх часткової відсутності, що суттєво розширює практичні можливості застосування методу.

Декларація щодо застосування ШІ

Під час написання статті засоби Генеративного ШІ не застосовувались.

Посилання

[1] A. Dhanapal, P. Nithyanandam, The Slow Http Distributed Denial of Service Attack Detection in Cloud, Scalable Computing: Practice and Experience 20(2) (2019) 285–298. doi:10.12694/scpe.v20i2.1501

[2] A. Dhanapal, 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

[3] T. Lukaseder, L. Maile, B. Erb, F. Kargl, SDN-Assisted Network-Based Mitigation of Slow DDoS Attacks, [cs.CR] 18 Apr 2018 (2018). doi:10.48550/arXiv.1804.06750

[4] R. Giryes, L. Shafir, A. Wool, A Flow is a Stream of Packets: A Stream-Structured Data Approach for DDoS Detection, [cs.CR] 12 May 2024 (2024). doi:10.48550/arXiv.2405.07232

[5] C. L. Calvert, T. M. Khoshgoftaar, Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data, Journal of Big Data 6(67) (2019). doi:10.1186/s40537-019-0230-3

[6] B. Cusack, Z. Tian, Detecting and tracing slow attacks on mobile phone user service, in: Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia, 2016, 4–10. doi:10.4225/75/58a54b013185a

[7] Є. В. Дуравкін, А. Карлссон, А. С. Локтіонова, Метод виявлення повільної атаки, Системи обробки інформації 8(124) (2014) 102–106. URL: http://nbuv.gov.ua/UJRN/soi_2014_8_24

[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) (2013) 85–88. URL: https://openarchive.nure.ua/server/api/core/bitstreams/08ee6ddf-c868-4676-9b7a-5db073e6ac83/content

[9] С. М. Лисенко, В. А. Ткачук, Метод та програмні засоби виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку, Herald of Khmelnytskyi National University 3 (2019) 273, 180–187. doi:10.31891/2307-5732-2019-273-3-180-187

[10] L. Liu, H. Wang, Z. Wu, M. Yue, The detection method of low-rate DoS attack based on multi-feature fusion, Digital Communications and Networks 6 4 (2020) 504–513. doi:10.1016/j.dcan.2020.04.002

[11] V. Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, 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

[12] V. Savchenko, V. Savchenko, O. Laptiev, O. Matsko, I. Havryliuk, K. Yerhidzei, I. Novikova, Detection of Slow DDoS Attacks Based on Time Delay Forecasting, in: Proceedings of III International Scientific and Practical Conference “Information Security

and Information Technologies", September 13–19, 2021. URL: https://ceur-ws.org/Vol-3200/paper6.pdf

[13] О. А. Лаптєв, С. С. Бучик, В. А. Савченко, В. С. Наконечний, І. І. Михальчук, Я. В. Шестак, Виявлення та блокування повільних DDOS-атак за допомогою прогнозування поведінки користувача, Наукоємні технології 55(3) (2022) 184–192. doi:10.18372/2310-5461.55.16908