DOI: 10.18372/2310-5461.55.16908
УДК 004.056

О. А. Лаптєв, д-р техн. наук, ст. наук. сп.,
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-4194-402X
e-mail: olaptiev@knu.ua;

С. С. Бучик, д-р техн. наук, професор,
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0003-0892-3494
e-mail: buchyk@knu.ua;

В. А. Савченко, д-р техн. наук, професор,
Київський національний університет
імені Тараса Шевченка
orcid.org: http://orcid.org/0000-0002-3014-131X
e-mail: savitan@ukr.net;

В. С. Наконечний, д-р техн. наук, професор,
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-0247-5400
e-mail: nvc2006@i.ua;

І. І. Михальчук, канд. техн. наук,
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-1802-7653
e-mail: inna.mykhalchuk@knu.ua;

Я. В. Шестак, канд. техн. наук,
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-1703-0316
e-mail: yaninashestak@gmail.com

ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ПОВІЛЬНИХ DDOS-АТАК ЗА ДОПОМОГОЮ ПРОГНОЗУВАННЯ ПОВЕДІНКИ КОРИСТУВАЧА

Вступ

Може здатися, що повільні малопотужні атаки (так звані атаки Low and Slow) залишилися в минулому, але практика показує, що вони досі активно використовуються зловмисниками. У 2021 році від таких атак постраждали 65 % організацій, при цьому 30 % стикалися з ними щомісяця. Середня інтенсивність, тривалість та складність DDoS-атак зростають рік у рік (у світі вже були прецеденти DDoS-атак з інтенсивністю 60 Gbps та тривалістю до декількох місяців). Очікується, що найближчими роками ситуація з цим видом атак погіршиться, адже активно розвиваються нові складні та повільні DDoS-атаки, вкрай важкі для виявлення. Легкість пошуку мережевих вразливостей зумовила надзвичайну розповсюдженість DDoS-атак.

Для ефективної протидії таким загрозам необхідно передбачити наступні два основні заходи:

1) діагностувати атаку на найбільш ранній стадії;

2) відокремити шкідливий трафік від звичайного одразу після виявлення.

Розуміючи запити користувачів, які використовуються для проведення DDoS-атаки, адміністратори інформаційних систем мають змогу зробити відповідні налаштування для брандмауерів, ма-

ршрутизаторів або застосувати інші заходи безпеки в межах мережі. Переважно параметри повільних DDoS-атак залежать від поведінки конкретного користувача, тож для ефективного пом'якшення такої поведінки користувача слід зважати на деталі запиту. Отже, прогнозування поведінки користувача на основі параметрів трафіку стає головним кроком у боротьбі з повільними DDoS-атаками.

Постановка проблеми

Повільні DDoS-атаки не викликають різке збільшення трафіку, яке приводить до миттєвої відмови сервера в обслуговуванні. Тобто визначити момент початку атаки майже неможливо. Відповідно, значно ускладнюється відокремлення шкідливого трафіку від нормального. Основна проблема в виявленні повільних DDoS-атак – це нездатність запобігти їм, оскільки процес визначення базується на вивченні існуючого трафіку без можливості його прогнозування в залежності від активності користувачів. Без сумніву, прогнозована поведінка користувачів дасть змогу виявити аномальну поведінку і запобігати появі повільних DDoS-атак.

Аналіз останніх досліджень і публікацій

Питанням виявлення розподілених атак типу «відмова в обслуговуванні» або DDoS присвячено значну кількість публікацій. Якщо зловмисник хоче паралізувати роботу програми, найпростіший спосіб – передача надлишкового обсягу трафіку з метою відключення сервера програми. Однак сьогодні існує чимало технологій, здатних виявляти та блокувати такі атаки на основі IP-адрес або сигнатур, управління квотами, а також за допомогою спеціалізованих рішень для запобігання DDoS-атакам. Існує величезна кількість публікацій, які досліджують способи виявлення DDoS-атак.

Так у роботі [1] запропоновано новий метод виявлення повільних HTTP-атак у хмарі. Рішення дозволяє виявити атаки Slow HTTP Header (Slowloris), Slow HTTP Body (RUDY) або Slow Read HTTP DDoS. Інша робота [2] пропонує нову модель класифікації атак, для пом'якшення атак у хмарі. Водночас такі підходи не гарантують ефективного виявлення атак на ранніх стадіях їх розвитку.

У роботі [3] представлено систему, яка може виявити і пом'якшувати атаки в межах мережевої інфраструктури. Ця робота продовжується роботою [4] у який досліджено модель захисту бічного каналу. Головними ідентифікаційними параметрами в обох моделях є швидкість передачі пакету та рівномірна відстань між пакетами, що не дозволяє упередити дії зловмисників. Тому у роботі [5] розглядається вибірка для створення різних розподілів класів для протидії впливу незбалансованих повільних наборів даних HTTP DoS.

У роботах [6,7] наводяться дослідження які розвивають систему захисту на основі метрики для виявлення традиційних повільних атак, які можуть бути ефективним з обмеженими ресурсами на основі подібності дослідження та впровадження евклідової метрики. Цей підхід досить ефективний лише за наявності великої кількості зразків таких повільних атак, і з великою ймовірністю такий підхід навряд чи буде ефективним.

У роботі [8] визначається якість параметрів TCP-з'єднань, які характерні для повільного HTTP нападу. Отримані формули оцінюють ймовірність і час переходу веб-сервера в режим перевантаження. Незважаючи на детальне вивчення, таке виявлення атак базується на спостереженні статистики та не стосується прогнозування.

У роботах [9, 10] запропоновано алгоритм виявлення повільних DDoS-атак на основі моделей трафіку залежно від стану завантаження сервера. Водночас процес пошуку рішення для запобігання не розглядаються. У роботі [11] розглянуто різні сценарії та запропоновано гібридні нейронні мережі для виявлення DDoS-атак, але метод і методика виявлення DDoS-атак низької інтенсивності не розглядається.

У роботі [12] розглянуто інтервал прогнозу на основі імовірнісної нейронної мережі з динамічним оновленням параметра згладжування. Але проблема динаміки такої моделі залишається невирішеною.

Робота [13] представляє новий метод для виявлення DDoS-атаки RUDY на основі самоподібності мережевого трафіку. Проте в роботі не враховано різноманітність навчальних зразків і процес отримання навчальної множини для навчання.

У роботі [14] представлена система для виявлення атак HTP DTP у хмарі на основі інформації індикатори ентропії та випадкові дерева. Такий підхід цілком ефективний, хоча він не вирішує питань прогнозування розвиток нападу.

Таким чином, більшість робіт, які присвячено протидії повільним DDoS-атаки не вирішують проблеми прогнозування поведінки користувача і тому є недостатньо ефективні для виявлення нападів на ранніх стадіях.

Метою даної роботи є формування системи виявлення повільних DDoS-атак на основі прогнозування поведінки користувачів мережі. Для успішного вирішення виявленої проблеми, необхідно побудувати модель і технологію прогнозування поведінки користувачів з урахуванням історії їх взаємодії з сервером, а також запропонувати топологію для розпізнавання повільних DDoS-атак.

Виклад основного матеріалу

Розрахунок параметрів трафіку для виявлення повільної DDoS-атаки

Основні компоненти виявлення повільної DDoS-атаки системи були запропоновані в [15]. Архітектура такої системи повинна складатися з чотирьох модулів:

1) збір трафіку;

2) розрахунок параметрів руху;

3) розрахунок мережевої статистики;

4) класифікатор атак.

Робочий процес такої системи повинен складатися з наступних кроків:

1. Модуль збору трафіку за певний період часу реєструє параметри руху, необхідні для подальшого обчислення: IP-адреси відправника та одержувача; TCP розмір вікна; час прибуття посилки.

2. У модулі розрахунку параметрів трафіку для кожної IP адреси розраховуються такі характеристики трафіку, напр. середня затримка між переданими пакетами (1).

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

де: t_i – час прибуття i-го пакету; t_{i+1} – час надходження i+1-го пакету; k – кількість пакетів, отриманих під час аналізу.

Вбудований таймер дозволяє записати початок і кінець сесії, що дає можливість відстежувати тривалість відкритих з'єднань. Інші параметри також можна використовувати для прогнозування в залежності від налаштувань системи.

3. У модулі класифікації атак рішення про наявність можливої повільної HTTP-атаки можна зробити після порівняння отриманих показників з пороговими значеннями. При такому підході рішення про наявність або відсутність повільної DDoS-атаки можливо здійснити лише після збору достатньої кількості статистичної інформації. Водночас у такій ситуації адміністратори системи часто не мають часу на активні дії. Тому рішення про наявність повільної DDoS-атаки, повинно базуватися на прогнозі поведінки користувача, який можливо сформувати на основі вивчення статистики подібних дій інших користувачів. Таким чином, доцільно додати блок прогнозування до розглянутого алгоритму дій.

Прогнозування поведінки користувача

Поведінка користувача в мережі формує особистісну траєкторію зміни параметрів трафіку конкретного користувача. Такі траєкторії будуть характерні як для звичайного руху, так і у випадку повільної DDoS-атаки. Для визначення відповідного часу, щоб почати нейтралізувати повільну DDoS-атаку, необхідно вирішити задачу індивідуального передбачення. Прогнозування параметрів руху по індивідууму вже було досліджено і продемонстровано в [13], де були показані параметри руху, які визначаються через великі проміжки часу (тиждень, місяць). Цей підхід також частково використовувався для захисту інформації в соціальних мережах [14] і для прогнозування в а мультиагентному середовищі [15]. Проте водночас точність системи розпізнавання повільної DDos-атаки повинна бути набагато вище і тому цей підхід потребує вдосконалення.

У цьому випадку вхідні дані можна використовувати для спостереження за рухом параметрів, наприклад, середнім інтервалом часу між переданими пакетами, затримкою між пакетами в сеансі тощо, які утворюють вектор параметрів $X = (X_1, X_2, .., X_H)$.

Виконання умови $X \in S_0$, де S_0 – область допуску вектора X. Випадковий процес $X(t)$ формується з часовими інтервалами між пакетами або затримками між ними у часі та описує еволюцію мережі параметри в часі. Припустимо також, що процес $X(t)$ статистично визначається при $t \geq t_1$, де t_1 – момент початку спостережень.

На рис. 1 показано конкретної траєкторії контрольного моменту спостереження $t_k \geq t_1$.

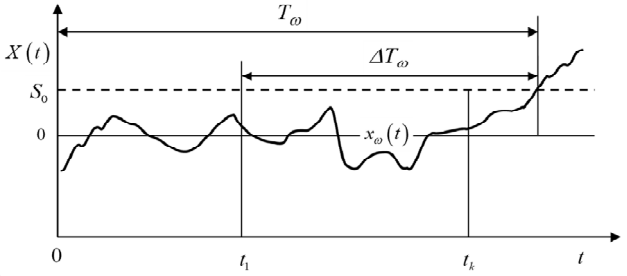


Рис. 1. Прогноз трафіку

Інформація про початок траєкторії руху параметра ω можна задати як $x_\omega(t) \in S_0, t_1 \leq t \leq t_k$ і отримані зі спостережень за параметром руху $X(t)$.

У цьому випадку проблема індивідуального прогнозування трафіку, параметр поведінки формулюється як проблема визначення апостеріорного розподілу результату процесу часу $T_\omega(t)$.

$X(t)$ поза зоною допуску S_0 відносно реалізації $x_\omega(t)$ можливо представити як задачу:

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

Формула (2) дає ймовірність того, що конкретна траєкторія, параметр ω гарантовано потрапляє в межі допустимого діапазону $s > t_k$, до моменту t_k включно. При цьому умова описується як $x_\omega(t)$, $t_1 < t < t_k$. Тобто, проблему індивідуального прогнозування траєкторії мережевого трафіку вирішено.

Для вирішення задачі прогнозування, досліджуваний процес повинен бути представлений формулою (3):

$$X(t) = m(t) + \sum_{\nu} V_{\nu} \cdot \varphi_{\nu}(t), \qquad (3)$$

де $m(t)$ – середня функція процесу; $\varphi_v(t)$ – невипадкові (координатні) функції часу; V_v – випадкові, некорельовані коефіцієнти

$$(M[V_{\nu}] = 0, M[V_{\nu}, V_{\mu}] = 0, \nu \neq \mu).$$

Це представлення, запропоноване в [13], дозволяє застосовувати його до будь-якого параметра трафіку, який можна представити як часовий ряд.

Цей процес X(t) можливо записати у вигляді випадкової послідовності $X(t_i) = X(i)$, $i = [1, i]$ у дискретній серії спостережень t_i:

$$X(t) = m(t) + \sum_{\nu=1}^{i} V_{\nu} \cdot \varphi_{\nu}(i), i \in [1, I], \qquad (4)$$

де V_v – випадковий коефіцієнт з параметрами;

$$M[V_{\nu}] = 0, M[V_{\nu}, V_{\mu}] = 0, \nu \neq \mu; [V_{\nu}^2] = D_{\nu};$$

$\varphi_v(i)$ – невипадкова функція координат, $\varphi_v(t) = 1$, $\varphi_v(i) = 0$ тоді як $v > i$.

Тоді формули для дисперсії та кореляційної функції будуть мати наступний вигляд (5–6):

$$D(i) = \sum_{\nu=1}^{i} D_v \cdot \varphi_v^2(i), i \in [1, I], \qquad (5)$$

$$D(i, j) = \sum_{\nu=1}^{\inf(i,j)} D_v \cdot \varphi_v(j), \; i, j \in [1, I]. \qquad (6)$$

Отже, представлення випадкових процесів руху параметрів (2) дозволяє вирішити задачу виявлення повільної DDoS-атаки на основі прогнозування поведінки користувача.

Алгоритм виявлення повільної DDoS-атаки на основі прогнозування поведінки користувача

Алгоритм складається з наступних кроків:

1. Визначити характеристики апріорного випадкового процесу $X(t)$ у вигляді рівняння (4) на дискретний ряд точки t_i. Для цього необхідно згенерувати результати контролю параметрів $x(\mu)$, у вигляді часового ряду, де будуть результати спостережень співвіднесені з моментами часу $t_\mu, \mu \in [1, k]$, $k < I$.

2. Встановити значення процесу реалізації $x(1)$, які отримані в результаті контролю, в момент часу $\mu = 1$, і представленні як:

$$x(1) = m(1) + v_1. \qquad (7)$$

3. Конкретизувати значення v_1 випадкового коефіцієнта V_1 за допомогою формули (7), що відповідає результату першого спостереження. Конкретизація значення V_1 призводить до зміни в щільності розподілу решти коефіцієнтів $V_i, i \in [2, I]$.

4. Встановити тип апостеріорного випадкового процесу, який в момент $i = 1$ проходить через точку $x(1)$ шляхом підстановки значення V_1 з (7) у формулу (4):

$$X^1(i) = m(i) - (x(1) - m(1)) \cdot \varphi_1(i) + \sum_{\nu=1}^{i} V_{\nu} \cdot \varphi_{\nu}(i), \; i \in [1, I] \qquad (8)$$

5. Визначити середнє значення для процесу (8), що знаходиться в момент проходження $i = 1$ через точку $x(1)$:

$$m^1(i) = m(i) + (x(1) - m(1) \cdot \varphi_1(i), \quad i \in [1, I]. \qquad (9)$$

6. Встановити загальну залежність для процесу, який проходить через точку x (1) :

$$X^1(i) = m^1(i) + \sum_{\nu=1}^{i} V_{\nu} \cdot \varphi_{\nu}(i), \; i \in [1, I]. \qquad (10)$$

7. Якщо $\mu = k$, то перейти до кроку 9; інакше – до наступного кроку.

8. Встановити значення процесу реалізації $x(2)$, результати отримані в результаті контролю в момент часу $\mu = 2$, при врахуванні (10) представимо у вигляді:

$$x(2) = m^2(2) + v_2. \qquad (11)$$

Повернення до кроку 3. Повторення операції, як для випадку $\mu = 1$, дасть результат

$$m^2(i) = m^1(i) + (x(2) - m(2)) \cdot \varphi_2(i), \quad i \in [1, I], \qquad (12)$$

$$X^2(i) = m^2(i) + \sum_{\nu=1}^{i} V_{\nu} \cdot \varphi_{\nu}(i), i \in [1, I]. \qquad (13)$$

9. Визначити оператор екстраполяції для функції середнього апостеріорного випадкового процесу та довільного числа $k < I$ у момент контролю $m^0(i) = m(i), \quad i \in [1, I]$:

$$m^k(i) = m^{k-1}(i) + (x(k) - m(k-1)) \cdot \varphi_k(i), \; i \in [1, I], \qquad (14)$$

$$X^k(i) = m^k(i) + \sum_{\nu=k+1}^{i} V_{\nu} \cdot \varphi_{\nu}(i), i \in [1, I]. \qquad (15)$$

Таким чином, формули (13)–(15) повністю описують процес, в якому вираз (14) є середньою функцією цього процесу для точки t_i.

10. Побудувати прогноз параметра трафіку та визначити момент, коли параметр перевищує критичні значення.

11. Класифікувати трафік як повільну DDoS-атаку та запровадити заходи безпеки.

12. Кінець алгоритму.

Таким чином, формула (14) дозволяє оптимально вирішити задачу екстраполяції процесу, а формула (15) – відтворює апостеріорний випадковий процес на основі моделювання.

Задана лінійна аналітична модель апостеріорного випадкового процесу на основі такого уявлення дозволяє вирішувати проблеми прогнозування параметрів мережевого трафіку.

В такому випадку рішення про повільну DDoS-атаку необхідно прийняти для кожної IP-адреси відправника на основі порівняння прогнозованих параметрів з критичними значеннями для визначення часу входження параметра в зону критичних значень. Такий підхід враховує статистику конкретної поведінки користувача, а також подібні поведінки інших користувачів у разі повільної DDoS-атаки.

Моделювання алгоритму детектування повільної DDOS-атаки на основі прогнозу-вання поведінки користувачів

Симуляцію виявлення повільної атаки DDoS на основі поведінки користувача було виконано для атаки RUDY та розроблено прогноз поведінки. Для простоти, було розглянуто лише один випадок нападу на тлі нормального трафіку, як показано на рис. 2.

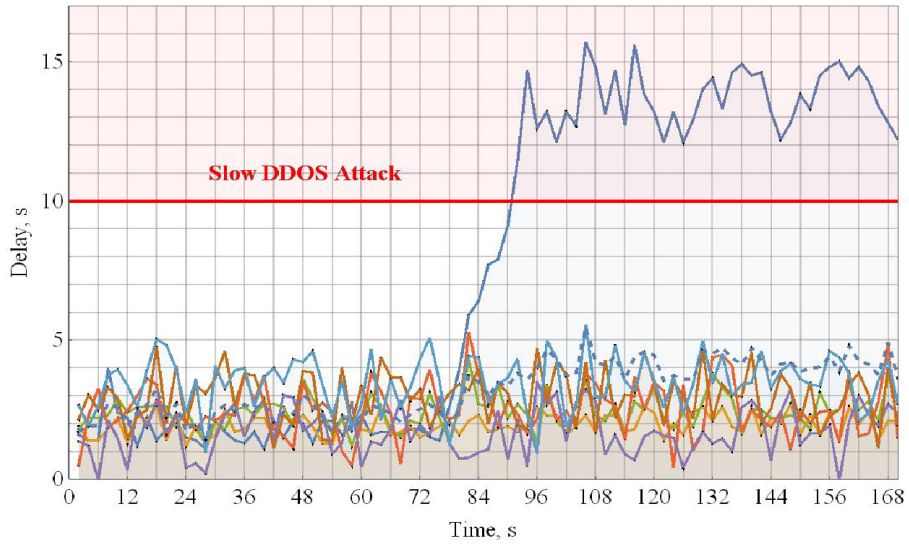


Рис. 2. Графік повільної DDoS атаки

Середня затримка між переданими пакетами розглядається як досліджуваний параметр.

RUDY – це атака на мережевий сервер, призначена для виклику збою веб-сервера через надсилання довгих запитів. Напад виконується за допомогою інструменту, який сканує цільовий веб-сайт і виявляє вбудовані веб-форми. Після того, як форми були виявлені, RUDY надсилає законні HTTP POST-запити з аномальною довжиною поля заголовка content-length, після чого починається введення інформації по одному байту на пакет. Цей вид атаки важко виявити через мізерні коливання вхідного трафіку.

Для процесу, показаного на рис. 2, застосовували вирази (4)–(15), взявши за вихідні значення спостережень окремі точки динамічного ряду, які відповідають частковій траєкторії № 1 (рис. 2, темна крива). Взявши цю криву як контрольну, за вихідні дані спостережень беруться перші значення динамічного ряду, які відповідають t= 1, 40, 90 с спостереження.

За наведеними результатами прогнозування при $t = 1$ с. Невелика кількість початкових контрольних даних дозволяє лише відтворити процес в цілому (середня крива процесу), але конкретні значення в прогнозований трафік будуть сильно відрізнятися від реальних (траєкторія керування). Відповідно, знаючи середні параметри в мережевому трафіку і точку входу в прогноз, ви не можете точно передбачити майбутню поведінку системи. Отже запропонований метод «вибирає» необхідну траєкторію залежно від точки входу і середньою траєкторію.

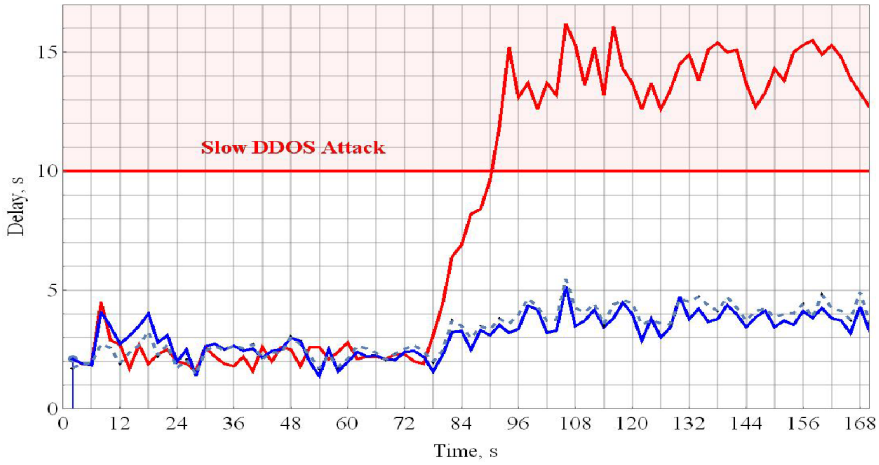
Збільшення кількості спостережень до $t = 40$, 90 с (рис. 3) підвищує достовірність прогнозування, тож при $t = 90$ с можна говорити про досить точний прогноз

$$P^{ps} = P\{X(s) \in S_o / \chi_\omega(t)\} \geq 0{,}99 .$$

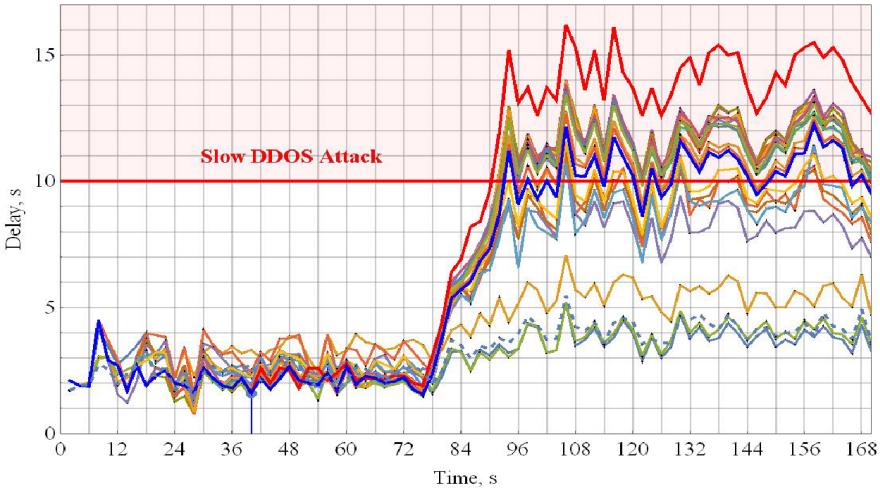
На малюнках 3*b* і 3*c* криві інших кольорів показують, як буде здійснюватися прогнозування при отриманні даних з інших контрольних точок $t_\mu, \mu = [1, k], k < I$, що передує моменту t_k.

Тобто ймовірність помилки при виборі правильної траєкторії залежить від кількості вихідних

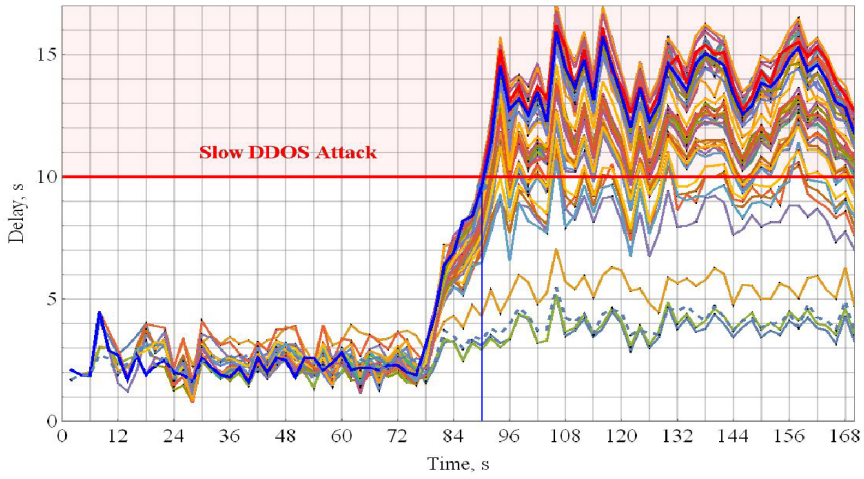
даних, що спостерігаються. В цьому випадку помилка і точність прогнозу буде залежати від особливості поведінки траєкторії, які призводять до аномального трафіку.



а) $t = 1$ с



б) $t = 40$ с



в) $t = 90$ с

Рис. 3: Прогнозування поведінки користувача з часом спостереження $t = 1, 40, 90$ с: — прогнозне значення; --- середнє значення

Для даного прикладу моделі постає питання про необхідну кількість спостережень і точність прогнозування траєкторії руху атаки. Результати розрахунків які наведені в табл. 1 показують збільшення точності передбачення з більшістю кількості контролю поведінки користувача, що досягає < 1 % за 90 с.

Таблиця 1

Середнє відхилення прогнозу від здійснення контролю поведінки користувача

Час спостереження, с	1	10	20	30	40	50	60	70	80	90
Відхилення, %	86	64	44	28	19	12	6	3	2	≤1

Отже, результати моделювання підтверджують адекватність моделі прогнозування для визначення повільних DDoS-атак на індивідуальній основі передбачення поведінки користувача. У даному випадку випадковий процес точно визначається в контрольних точках і забезпечує мінімум середньої квадратичної помилки в інтервалах між цими точками.

Висновки

Повільні DDoS-атаки стають все більш поширеними через простоту виконання і складність їх виявлення. Виявлення атаки існуючими методами наразі є неефективним через запізнілий характер відповіді на атаки у разі спостереження та аналізу параметрів трафіку. Більш перспективним підходом є прогнозування користувача поведінка на основі статистики попередніх атак. Прогнозування індивідуальної поведінки користувача забезпечує рішення проблеми виявлення повільних DDoS-атак на основі алгоритму знаходження невідомих майбутніх значень для часового ряду параметрів руху. Запропонований спосіб поєднує в собі переваги штучного інтелекту та статистичного аналізу і здатний до самонавчання у випадку наявності статистики атак. Такий підхід дає можливість точно визначити випадковий процес в контрольних точках і забезпечити мінімум середнього квадрата апроксимації помилки в інтервалах між цими точками. Подальші дослідження у галузі протидії повільним DDoS-атакам можуть бути широко розвинуті розглядом питання вдосконалення запропонованого методу, щоб надати можливість прогнозування з інтервалами, що виходять за межі доступної статистики, в тому числі в умовах високого шуму даних або їх часткової відсутності.

ЛІТЕРАТУРА

[1] A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. *Scalable Computing: Practice and Experience*. 2019. Volume 20, Number 4, pp. 669–685. https://doi.org/ 10.12694/ scpe.v20i4.1569

[2] H. Abusaimeh, H. Atta, H. Shihadeh. Survey on Cache-Based Side-Channel Attacks in Cloud Computing. *International Journal of Emerging Trends in Engineering Research*. 2020. Volume 8, No. 4, p. 1019–1026.

[3] Лаптев О. А., Собчук В. В., Саланди И. П., Сачук Ю. В. Математична модель структури інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2019. Вип. 64. С. 124–132.

[4] 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*. 2019. Volume 6, No. 67 https://doi.org/10.1186/s40537-019-0230-3.

[5] Karaboga D. An idea based on honey bee swarm for numerical optimization Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.

[6] Ya. V. Tarasov. Investigation of the application of neural networks for the detection of low-intensity DDoS-attacks of the application level. *Cybersecurity.* 2017. Issues №5(24). PP. 23–29. https://doi.org/ 10.21681/2311-3456-2017-5-23-29.

[7] Kureichik V. V., Zaruba D. V., Zaporozhets D. Y. Algoritm parametricheskoy optimizatsii na osnove modeli povedeniya roya svetlyachkov. Parametric optimization algorithm based on the model of glowworm swarm behavior. *Izvestiya SFedU. Engineering Sciences*. 2015, no. 6 (167), pp. 6–15.

[8] Лаптєв О. А., Собчук В. В., Савченко В. А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2019. Вип. 66. С. 124–132.

[9] M. Idhammad, K. Afdel, and M. Belouch. Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest. *Security and Communication Networks*. 2018, Volume Article ID 1263123, 13 p. https://doi.org/10.1155/2018/1263123.

[10] Лаптєв О. А. Експериментально-статистичний метод обчислення кореляційної взаємозалежності параметрів розпізнавання засобів негласного отримання інформації. *Сучасний захист інформації*. 2019. № 3(39). С. 23–29.

[11] S. Lysenko, V. Tkachuk. Method and software for detecting r.u.d.y. attack based on the usage of the algorithm of determining traffic self-similarity. *Herald of Khmelnytskyi national university*. 2019. Issue 3, p. 273.

[12] Sobchuk A. V., Sobchuk V. V., Barabash O. V., Lyashenko I. O. Functionally sustainable wireless sensor network technologies aspects analysis. Science and Education a New Dimension. *Natural and Technical Sciences.* 2019. VII (23), Issue 193, Budapest, Hungary, pp. 46–48.

[13] B. Cusack, and Z. Tian. Detecting and tracing slow attacks on mobile phone user service. In Valli, C. (Ed.). The Proceedings of 14th Australian Digital Forensics Conference, 5–6 December 2016, Edith Cowan University, Perth, Australia. pp. 4–10, 2016

[14] 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*. 2018. VOL 3, NO 2 (93). p. 33–41. https://doi.org/10.15587/1729-4061.2018.131471.

[15] В. В. Козловський, О. Л. Туровський, В. Д. Кулінський. Формализация требований к системе управления телекоммуникационными сетями. *Проблеми інформатизації та управління*. 2020. Том 2 № 64. С. 41–47

[16] V. V. Kozlovskii, M. V. Kuklinskyi, Yu. V. Balanyuk, O. V. Ivanov. End-to-end control and optimization in information and calculating networks. *Інформаційні технології, кібербезпека*. 2018. Vol. 40 No. 4. C.393-397. DOI: 10.18372/2310-5461.40.13263.

[17] Наконечний В. С., Барабаш О. В., Лаптєва Т. О., Міщенко А. В. Удосконалення методу виявлення та кластерізації джерел неправдивої інформації. Наукоємні технології. 2022. Том 54, № 4. С. 105–111. DOI 10.18372/2310-5461.54.16747.

[18] Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. 2022. Vol. 1, № 9(115), pp. 93–101.1729–4061. DOI: 10.15587/1729-4061.2022.253530.

Лаптєв О. А., Бучик С. С., Савченко В. А., Наконечний В. С., Михальчук І. І., Шестак Я. В.

ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ПОВІЛЬНИХ DDOS АТАК ЗА ДОПОМОГОЮ ПРОГНОЗУВАННЯ ПОВЕДІНКИ КОРИСТУВАЧА

Особливістю повільної DDoS-атаки є використання вразливості в протоколі TCP/IP, де навмисно чи ненавмисно можуть бути викликані переривання в результаті затримки в каналах зв'язку. У статті розглядається проблема виявлення повільної розподіленої атаки відмови в обслуговуванні. Відомо, що виявлення повільних DDoS-атак відрізняється від атак на основі обсягу трафіку, оскільки вони не збільшують інтенсивність трафіку в мережі. Замість створення раптового надлишку трафіку, повільні малопотужні атаки проводяться з мінімальною активністю і не реєструються системами. Вони спрямовані на те, щоб вивести об'єкт з ладу непомітно, створюючи мінімальну кількість підключень та залишаючи їх незавершеними якомога довше. Як правило, зловмисники відправляють часткові запити HTTP і невеликі пакети даних або повідомлення для перевірки активності, щоб підключення залишалося активним. Подібні атаки важко заблокувати, і складно виявити. У зв'язку з малим обсягом трафіку, а також з тим, що атаки можуть виглядати як стандартні підключення, потрібна інша технологія запобігання. Джерела атак необхідно блокувати, виходячи з особливостей виконання запитів, а не на основі їх репутації. Тому було зроблено припущення про залежність успішної повільної DDoS-атаки залежить та поведінки користувача. На основі моделювання методу виявлення повільних атак було проведено дослідження та прогнозування поведінки особистості, запропоновано траєкторію поведінки конкретного користувача. Можливості застосування такого методу підтверджено моделюванням атак RUDY на HTTP-сервіси. Отримані характеристики точності прогнозування залежно від відображуваного накопиченого трафіку і статистики атак. Дослідження доводить, такий метод можна використовувати для виявлення різних типів повільних DDoS-атак.

Ключові слова: мережевий протокол; блокування; індивідуальне передбачення; випадковий процес; повільна DDoS-атака; поведінка користувача.

Laptiev O., Buchyk S., Savchenko V., Nakonechnyy V., Mikhalchuk I., Shestak Y.

DETECTION AND BLOCKING SLOW DDOS ATTACKS BASED ON PREDICTING USER BEHAVIOR

Security researchers have identified 14 vulnerabilities affecting the TCP/IP protocol library. A feature of a slow DDoS attack is the use of a vulnerability in the TCP/IP protocol, where interruptions can be caused intentionally or unintentionally as a result of delays in communication channels. The article deals with the problem of detecting a slow distributed denial of service attack. Detecting slow-moving DDoS attacks is known to differ from traffic-based attacks because they do not increase network traffic. Instead of creating a sudden surge of traffic, slow, low-power attacks are conducted with minimal activity and are not registered

by systems. They aim to fail the object inconspicuously by creating the minimum number of connections and leaving them unfinished for as long as possible. Typically, attackers send partial HTTP requests and small data packets or activity check messages to keep the connection active. Such attacks are difficult to block and difficult to detect. Due to the low volume of traffic and the fact that attacks can look like standard connections, a different prevention technology is required. Attack sources should be blocked based on the characteristics of the request execution, not on the basis of their reputation. Therefore, it was assumed that the success of a slow DDoS attack depends on the user's behavior. Based on the modeling of the method of detecting slow attacks, research and prediction of the behavior of the individual was carried out, and the trajectory of the behavior of a specific user was proposed. The possibilities of using this method were confirmed by modeling RUDY attacks on HTTP services. The obtained prediction accuracy characteristics depend on the displayed accumulated traffic and attack statistics. The study proves that such a method can be used to detect different types of slow DDoS attacks.

Keywords: network protocol; locking; individual prediction; random process; slow DDoS attack; user behavior.

Стаття надійшла до редакції 01.09.2022 р.
Прийнято до друку 14.09.2022 р.