

ВІЯВЛЕННЯ DDoS-АТАК ПРИКЛАДНОГО РІВНЯ

Зінченко В. В.; Зінченко М. В., к.т.н.

Національний технічний університет України

«Київський політехнічний інститут», м. Київ, Україна

Однією з загроз у сфері захисту інформації є технологія DDoS-атак на сервери інформаційних ресурсів. Умовно DDoS-атаки можна поділити на два підвиди: мережевого та прикладного рівня. Атаки мережевого рівня сьогодні не створюють серйозної небезпеки, завдяки розробленим успішним методам боротьби з ними. При цьому, DDoS-атаки прикладного рівня продовжують бути ефективним інструментом для перевантаження інформаційних ресурсів, що призводить до подальших збоїв у функціонуванні останніх. Ці атаки використовують легальні HTTP-запити, а тому їх виявлення у реальному часі є досить складною задачею. У цій роботі пропонується реалізація ефективного методу, що дозволяє в режимі online з високою ймовірністю виявити ознаки дії DDoS-атак прикладного рівня.

Під DDoS-атаками прикладного рівня розуміють атаки, робота яких відбувається за участю верхнього рівня OSI-моделі – рівня додатків. Зазвичай, їхня дія проявляється у вивантаженні великої кількості об'ємних файлів або переповненні зовнішніми запитами пошукової системи, баз даних тощо. Таким чином, відбувається примусове переведення сервера у «невизначений» стан. Щоб не бути завчасно виявленою, атака передбачає замасковане під флешмоб (одночасне звернення користувачів до вебсайту) насичення інформаційного каналу. Аналіз надходження запитів за часовими та адресними параметрами дозволяє з високою точністю виявити напад на комп'ютерну систему (див. рис. 1).

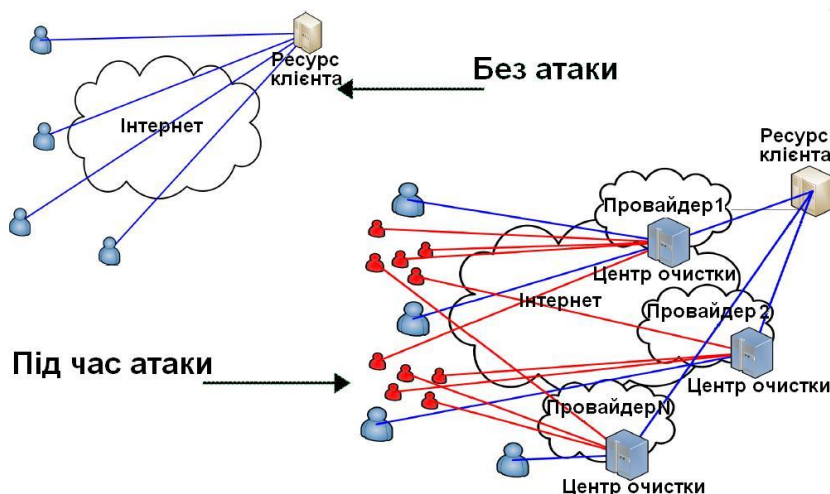


Рисунок 1. DDoS-атака прикладного рівня

Трафік, що надходить до веб-сайтів, складається переважно з потоку HTTP Get-запитів. За деякий проміжок часу Δt з IP-адреси x_i надходить s_i таких запитів. Отже, кожному проміжку Δt можна співставити пари (x_i, s_i) ,

$(x_2, s_2), \dots, (x_n, s_n)$, де x_1, \dots, x_n — усі IP-адреси, з яких за час Δt надходили *HTTP Get*-запити, s_1, \dots, s_n — кількість таких запитів з відповідної адреси.

Введемо поняття ентропії *HTTP Get*-запитів відносно IP-адрес, з яких вони надійшли:

$$H = - \sum_i p(x_i) \log_2(p(x_i)),$$

де $p(x_i)$ — ймовірність *HTTP Get*-запиту з адреси x_i , $p(x_i) = \frac{s_i}{\sum_i s_i}$.

Очевидно, що таким чином визначене значення ентропії, при *DDoS*-атаці прикладного рівня, буде меншим, ніж значення ентропії, при роботі сервера за звичайної кількості запитів, яке, у свою чергу, буде меншим за значення ентропії при ситуації флешмобу.

Значення ентропії H_1, H_2, \dots, H_t , знайдені у послідовні проміжки часу, утворюють часовий ряд [1]. Такий часовий ряд можна описати рівнянням авторегресії p -го порядку:

$$y_t = a_1^t y_{t-1} + a_2^t y_{t-2} + \dots + a_p^t y_{t-p} + e_t,$$

тобто поточне значення ентропії дорівнює зваженій сумі попередніх значень і помилки e_t . Помилка e_t вводиться для врахування можливої невідповідності обчисленого значення ентропії з реальним (наприклад, коли не всі *HTTP Get*-запити надійшли до серверу).

Оцінки коефіцієнтів такої моделі можна знайти за допомогою фільтра Калмана [2, 3]. Для цього доцільно перейти у простір стану.

Нехай $X_t = (a_1^t, a_2^t, \dots, a_p^t)$ — вектор стану; $F_t = (H_{t-1}, H_{t-2}, \dots, H_{t-p})$ — матриця переходу. Тоді рівняння авторегресії можна записати у вигляді:

$$H_t = F_t X_t + e_t.$$

Припустимо, що X_t є вінеровським процесом:

$$X_t = X_{t-1} + w_{t-1}, \quad w_t \text{ і } e_t \text{ — некорельовані,}$$

$$D(w_t) = \sigma_w^2, \quad D(e_t) = \sigma_e^2.$$

Оцінка \hat{X}_t реального стану X_t буде обчислюватися наступним чином:

$$\hat{X}_{t|t-1} = X_{t-1}, \quad P_{t|t-1} = P_{t-1} + C_{w_{t-1}},$$

$$K_t = P_{t|t-1} F_t^T (F_t P_{t|t-1} F_t^T + C_{e_t})^{-1}, \quad \hat{X}_t = \hat{X}_{t|t-1} + K_t (H_t - F_t \hat{X}_{t|t-1}),$$

$$P_t = (I - K_t F_t) P_{t|t-1},$$

де $P_{t|t-1}$ — апіорна коваріаційна матриця, а P_t — апостеріорна коваріаційна матриця.

За допомогою отриманих оцінок \hat{X}_t можна охарактеризувати поточний рівень небезпеки трафіку, направлено на сервер. Тобто, виявлення факту *DDoS*-атаки зводиться до віднесення значень оцінок стану до однієї з двох груп значень: перша, при якій досить висока ймовірність перебігу *DDoS*-атаки прикладного рівня на сервер «жертви», та друга, для якої невластиві подібні атаки. Для розв'язання цієї задачі класифікації використовується метод опорних векторів.

Випробування запропонованого методу виявлення *DDoS*-атак прикладного рівня були проведені за умов як звичайного перебігу подій для сервера, так і в умовах, подібних до флешмобу. В обох випадках атаки фіксувалися з досить високою точністю (близько 90 %), що вказує на придатність даного методу для боротьби з такого роду загрозами.

Отже, у роботі розглянуто ефективний підхід для протистояння одній з найактуальніших проблем захисту інформації сучасності – проблемі *DDoS*-атак прикладного рівня. Закладений в основу методу фільтр Калмана для обчислення оцінки стану потребує лише значення оцінки стану з попереднього кроку та значення вимірювань з поточного кроку. Така властивість дає змогу ефективно відстежувати трафік на можливість проведення *DDoS*-атак прикладного рівня у режимі реального часу. Висока точність вияву загроз в умовах нормального потоку запитів і в умовах флешмобу є незаперечною перевагою запропонованого методу.

Перелік посилань

1. Бідюк П. І. Аналіз часових рядів: навчальний посібник / П.І.Бідюк, В.Д.Романенко, О.Л.Тимошук. – К. : Політехніка, 2010. – 317 с.
2. Grewal M. Kalman Filtering: Theory and Practice using Matlab / M.Grewal, A.Andrews. – Wiley & Sons Interscience, 2008. – 575 с.
3. Anderson B. Optimal Filtering / B.Anderson, J.Moore. – Prentice-hall, 1979. – 357 с.

Анотація

Представлено метод для виявлення *DDoS*-атак прикладного рівня, який дозволяє відстежувати трафік у режимі реального часу. Розглянуто застосування запропонованого методу в умовах нормального потоку запитів і подібних до флешмобу.

Ключові слова: *DDoS*-атаки, фільтр Калмана, безпека мережі.

Аннотация

Представлен метод для выявления *DDoS*-атак уровня приложений, который позволяет исследовать трафик в режиме реального времени. Рассмотрено применение предложенного метода в условиях нормального потока запросов и подобных флешмобу.

Ключевые слова: *DDoS*-атаки, фильтр Калмана, безопасность сети.

Abstract

An approach for detection of application-layer *DDoS*-attacks which allows to monitor network traffic in real time is provided. Applying of this method in different conditions: with a normal stream of requests and in flash crowd is considered.

Keywords: *DDoS*-attacks, Kalman filter, network security.