

МЕТОД ФІЛЬТРАЦІЇ ЗА КІЛЬКІСТЮ ПРОЙДЕНИХ ВУЗЛІВ В БОРОТЬБИ З DDoS-АТАКАМИ

Студенников В. Д.;¹ Рудник Д. М.²

^{1,2} Національний авіаційний університет

^{1,2} Україна, Київ

¹ vladstudennikovwork@gmail.com; ² 5739122@stud.nau.edu.ua

Анотація. У статті розглянуто метод фільтрації за кількістю пройдених вузлів як ефективний спосіб боротьби з DDoS-атаками. Описано принцип роботи фільтрації за кількістю переходів між маршрутизаторами, який дозволяє виявляти та блокувати зловмисні пакети, що використовуються в атаках. Метод допомагає виявляти аномальні пакети, характерні для DDoS-атак. Також наведено приклади його застосування та аналіз ефективності в реальних умовах.

Ключові слова: кібербезпека; DDoS-атака; інформаційна безпека; фільтрація трафіку.

Вступна частина. DDoS-атаки – зростаюча проблема, яка впливає на всіх користувачів мережі. Це навмисна дія, мета якої – перешкодити нормальному використанню інтернет-ресурсів. Основна ідея DDoS-атаки – вичерпати ресурси цілі і змусити її відповідати на величезну кількість помилкових запитів, при цьому запити звичайних користувачів залишаються без відповіді або будуть оброблятися дуже довго. [1]

Головною проблемою у боротьбі з DDoS-атаками є відсутність надійного способу визначення джерела пакетів, що дозволяє зловмисникам уникати відповідальності. [1]

Методи протидії DDoS-атакам можна розділити на пасивні і активні, а також на превентивні і реакційні. Нижче наведений короткий список основних методів [2]:

- Запобігання – профілактика причин, що змушують тих або інших осіб організовувати та здійснювати DDoS-атаки.

- Зустрічні міри – вводячи технічні або правові міри, потрібно якомога активніше діяти на джерело та організатора DDoS-атаки.

- Програмне забезпечення – на ринку сучасного програмного і апаратного забезпечення існує і таке, що може захистити сервіси від слабких DDoS-атак.

- Фільтрація і блекхолинг (з англ. Blackholing – методи проти спаму) – блокування вихідного трафіку від атакуючих машин. Ефективність цих методів знижується по мірі наближення до об'єкта атаки і підвищується по мірі наближення до атакуючої машини.

- Зворотній DDoS – перенаправлення трафіку, використаного для атаки, на атакуючого.

- Усунення вразливостей – не працює проти флуд-атак, для яких «вразливістю» є обмеженість тих чи інших системних ресурсів. Сама міра націлена на усунення помилок в системах і службах.

- Збільшення обсягу ресурсів – як окремих метод демонструє певну обмеженість, але може стати хорошою базою для використання інших видів захисту від DDoS-атак.

- Розподіл – побудова розподілених і дубльованих систем, які не припиняють обслуговувати користувачів, навіть якщо деякі їх елементи стануть недоступними через DDoS-атаки.

- Ухилення – відхилення безпосередньої цілі атаки подалі від інших ресурсів, які часто також є вразливими разом з самою ціллю атаки.

- Активні зворотні дії – вплив на джерело, організатора або центр управління атакою, як технічними так і організаційно-правовими методами.

- Використання обладнання для захисту від DDoS-атак.

- Купівля сервісу по захисту від DDoS-атак.

Одним з сучасних методів боротьби з DDoS-атаками є фільтрація запитів за кількістю пройдених вузлів у мережі. Запит звичайного клієнта йде напряду від клієнтського пристрою до цілі, проте в разі DDoS-атаки запит проходить довший шлях – від комп'ютера зловмисника до зараженого комп'ютера, який здійснюватиме запит, і лише після чого направляється до цілі. Таким чином, з однієї і тієї ж локації звичайні запити проходять менший шлях по мережі, ніж запити, що є частиною DDoS-атаки.

Метою роботи є дослідження методу фільтрації запитів за кількістю пройдених вузлів для боротьби з DDoS-атаками і дослідженні потенційних проблем даного методу.

Основна частина. Кількість пройдених маршрутизаторів запитом можна поррахувати на основі поля TTL в IP-пакеті – це 8-бітове поле, в яке записується максимальна кількість переходів пакету у мережі перед тим, як його буде знищено. При проходженні пакету через маршрутизатор значення в даному полі зменшується на 1. [3]

Таким чином, поррахувати кількість пройдених маршрутизаторів можна, віднявши від початкового значення TTL те значення, що залишилося після досягнення цілі. Наприклад, якщо під час відправки пакету поле TTL дорівнювало 32, а після досягнення цілі TTL став рівним 20, то запит пройшов через $32 - 20 = 12$ маршрутизаторів (12 маршрутизатор є цільовим).

Даний метод боротьби з DDoS-атаками ускладнюється тим, що кожен пристрій при відправці пакету може задати будь-яке значення TTL, таким чином, відправивши запит з одного пристрою, поле TTL на цільовому пристрої може приймати різні значення в залежності від початкового значення TTL. Проте всі операційні системи, як правило, задають значення TTL за списку: 30, 32, 60, 64, 128 або 255, що значно спрощує обрахунки можливих кінцевих значень TTL. [3]

Також шлях різних пакетів по мережі може бути різним: один і той самий пакет може проходити через різну кількість маршрутизаторів, щоб дістатися цілі. Проте у [3] було визначено, що ймовірність, з якою кількість пройдених маршрутизаторів приймає конкретне значення, добре апроксимується функцією нормального розподілу.

У [3] було обрано декілька веб-ресурсів та визначено кількість пристроїв, через які проходить запит від клієнтського пристрою до заданого веб-ресурсу, з допомогою утиліти traceroute. На рисунку 1, зокрема, зазначено залежність між кількістю пройдених запитом маршрутизаторів до веб-ресурсу Стенфордського університету і кількістю дослідів, у яких запит пройшов задану кількість пристроїв, а також графік функції нормального розподілу. З рисунку 1 видно, що отримані експериментальні дані дійсно добре апроксимуються функцією нормального розподілу.

З допомогою нормального розподілу можна визначити ймовірність того, що деякий запит є нормальним або є частиною DDoS-атаки, а запити, в яких вказано достатньо мало ймовірний TTL, вважатимуться аномальними і не будуть розглядатися системою.

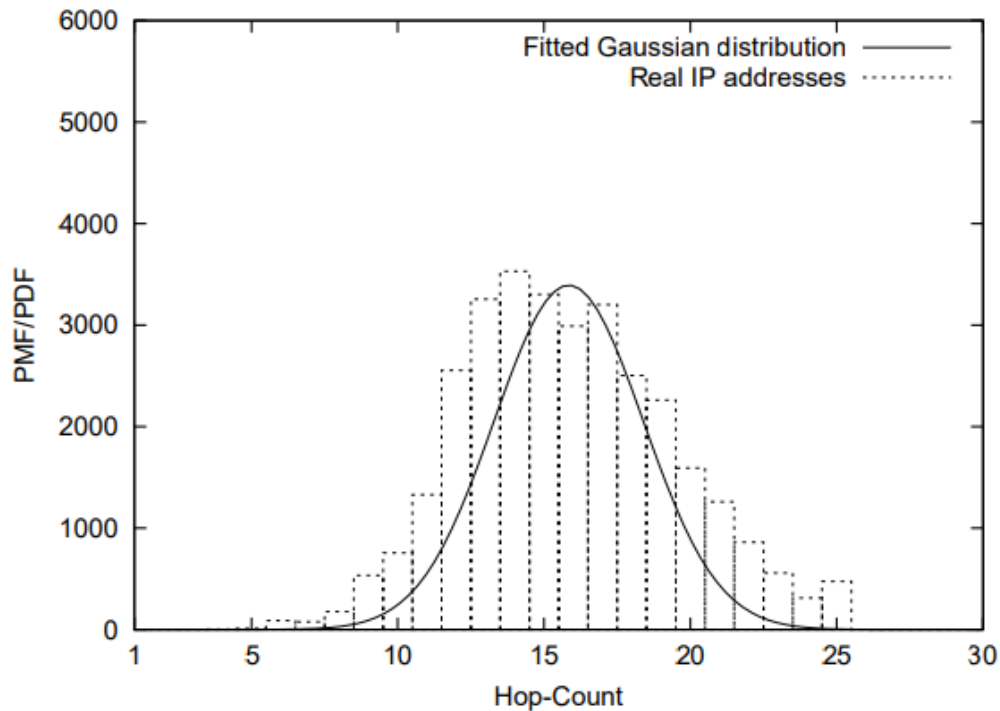


Рис. 1 – залежність між кількістю маршрутизаторів, що проходив кожен пакет від клієнтського пристрою до веб-ресурсу Stanford University, і кількістю експериментів, в яких пакет проходив задану кількість маршрутизаторів

Висновки. Метод фільтрації за кількістю пройдених вузлів є дієвим методом для боротьби з DDoS-атаками. На основі ідеї про те, що можна класифікувати пакети як злоякісні або нормальні на основі кількості пройдених маршрутизаторів в мережі, а також використовуючи статистичні та алгоритмічні методи, сьогодні створюються нові, ефективні апаратні та програмні інструменти для боротьби за DDoS-атаками, що здатні допомогти веб-ресурсами убезпечити себе від цього небезпечного типу атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Гвозденко, М., & Чобу, Я. (2014). Технічні та програмні засоби виявлення джерела DDoS-атаки. *Global Scientific Unity* 2014, 1.
- [2] Ковальов, В.А. (2019). Методи виявлення DDoS-атак [Магістерська робота, Вінницький національний технічний університет]. <https://iq.vntu.edu.ua/repository/getfile.php/1123.pdf>
- [3] Wang, H., Jin, C., & Shin, K. G. (2007). Defense Against Spoofed IP Traffic Using Hop-Count Filtering. *IEEE/ACM Transactions on Networking*, 15(1), 40–53. <https://doi.org/10.1109/tnet.2006.890133>

Studennykov V. D., Rudnyk D. M.

Hop count filtering for DDoS-attacks prevention

Abstract. The article discusses the hop count filtering method as an effective way to prevent DDoS attacks. The principle of operation of filtering by the number of transitions between routers is described, which allows detecting and blocking forged packets used in attacks. The method helps to detect anomalous packets typical of DDoS attacks. Examples of its application and analysis of effectiveness in real conditions are also given.

Keywords: cybersecurity; DDoS attack; information security; traffic filtering.