УДК 004.056

Охрімчук В. В. к.т.н., доцент, професор
Охрімчук І. А., викладач
Житомирський військовий інститут імені С. П. Корольова

МЕТОД ВИЯВЛЕННЯ ПОВІЛЬНИХ DDOS-АТАК

Стрімкий розвиток інформаційних технологій та глобальна цифровізація суспільства призвели до суттєвого зростання кількості кіберзагроз. Інформаційні системи державних установ, підприємств та об'єктів критичної інфраструктури постійно піддаються різноманітним типам кібератак. Сучасні тенденції розвитку кібератак свідчать не тільки про збільшення їх кількості, а й про зростання їх технологічної складності, що в свою чергу призводить до ускладнення їх виявлення.

Одним із найпоширеніших видів атак є атаки відмови в обслуговуванні (*Distributed Denial of Service, DDoS*), метою яких є порушення доступності інформаційних ресурсів шляхом перевантаження серверів або мережевої інфраструктури. Проте, особливу небезпеку становлять так звані повільні *DDoS*-атаки (*Slow DDoS attacks*), які відрізняються від класичних атак низькою інтенсивністю мережевого трафіку та використанням легітимних протокольних механізмів. На відміну від традиційних атак, що генерують значні обсяги трафіку, повільні атаки діють приховано, поступово виснажуючи доступні ресурси серверів за допомогою великої кількості частково відкритих або повільно оброблюваних з'єднань. Унаслідок цього сервер змушений підтримувати велику кількість активних сесій, що з часом призводить до закінчення його ресурсів і неможливості обслуговування легітимних користувачів.

Актуальність дослідження методів виявлення повільних *DDoS*-атак зумовлена саме складністю їх ідентифікації за допомогою традиційних систем виявлення вторгнень, в основу роботи яких покладено аналіз інтенсивності трафіку та виявлення аномалій в мережевих потоках. Однак повільні атаки генерують мінімальний обсяг даних і часто не перевищують порогових значень, встановлених системами моніторингу. У результаті такі атаки можуть залишатися непоміченими протягом тривалого часу, що призводить до поступового зниження продуктивності сервісів та втрати доступності інформаційних ресурсів.

Тому, одним із перспективних підходів до вирішення цієї проблеми є використання методів нечіткої логіки та теорії нечітких множин. Основна ідея такого підходу полягає у врахуванні невизначеності та нечітких характеристик мережевої поведінки. На відміну від класичних детермінованих методів, які використовують жорсткі порогові

значення, нечіткі моделі дозволяють оцінювати стан мережевого трафіку на основі ступеня належності параметрів до певних лінгвістичних змінних, таких як, наприклад, “низька швидкість передачі”, “тривалість з’єднання” або “кількість неповних запитів”.

Метод виявлення повільних *DDoS*-атак на основі нечітких множин передбачає аналіз кількох ключових параметрів мережевої взаємодії. До таких параметрів можуть належати тривалість *TCP*-з’єднань, швидкість передачі пакетів, кількість одночасних з’єднань від одного джерела, а також інтервали між пакетами. Кожен із цих параметрів описується нечіткими множинами з відповідними функціями належності. Після цього формується база нечітких правил, яка визначає можливі комбінації параметрів, характерні для повільних атак. Наприклад, якщо тривалість з’єднання значно перевищує звичні показники, швидкість передачі даних є низькою, а кількість активних з’єднань є значною, то ймовірність проведення повільної *DDoS*-атаки зростає.

Подальша обробка здійснюється за допомогою механізму нечіткого виведення Мамдані, який дозволяє агрегувати результати аналізу окремих параметрів і сформувати інтегральну оцінку рівня загрози. Отриманий результат може бути використаний для автоматичного прийняття рішень системами захисту, наприклад для обмеження підозрілих з’єднань, блокування джерел трафіку або активування додаткових механізмів перевірки.

Таким чином, застосування методу виявлення повільних *DDoS*-атак на основі теорії нечітких множин дозволить більш ефективно аналізувати складні та нечітко визначені характеристики мережевого трафіку. Використання такого підходу забезпечить підвищення точності виявлення прихованих атак, зменшення кількості хибних спрацювань та своєчасне реагування на загрози. Практична реалізація та впровадження запропонованого методу сприятиме підвищенню рівня захищеності інформаційних систем і забезпеченню стабільної роботи мережевих сервісів в умовах зростання кіберзагроз.

Список використаних джерел

1. Савченко В. А., Кожухівський А. Д., Ільїн О. Ю. Діагностування початку повільної HTTP DDoS атаки на основі двопараметричного кореляційного аналізу трафіку / Телекомунікаційні та інформаційні технології № 4, 2021. С. 28-40.

2. Tayama, S., Tanaka, H. Analysis of Slow Read DoS Attack and Communication Environment. Mobile and Wireless Technologies 2017. ICMWT 2017., vol 425. Springer, Singapore. pp 350–359.