УДК 004.056.5:004.032.26

Н.Х. САІТГАРЕЄВ, канд. тех. наук, доцент, Н.Н. ШАПОВАЛОВА, ст. викладач,
С.В. БІЛАШЕНКО, асистент, Криворізький національний університет

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ DDOS-АТАК

У час інформаційних технологій безліч компаній зберігають, обчислюють, аналізують чи поширюють інформацію в мережі Інтернет, що зменшує обсяг додаткових витрат. Однак з появою нових можливостей, виникають і нові загрози. В одну мить безвідмовно працююча система може бути піддана хакерській атаці. Дослівно з англійської термін DDoS (Distributed Denial of Service) перекладається як «відмова в обслуговуванні», тобто метою такої атаки є створення умов, при яких рядовим користувачам буде утруднений або повністю обмежений доступ до системи. В результаті атаки такого типу мережевий ресурс, який атакується, отримує лавиноподібну кількість запитів, які не встигає обробити. Компанія, що була піддана DDoS-атаці може зазнати величезних збитків [1]. У зв'язку з цим постає проблема виявлення DDoS-атак, тобто аналіз становища та виявлення аномальної активності мережевого трафіку.

За своєю суттю аналіз аномалій дозволяє виявляти суттєві відхилення трафіку мережевих пристроїв від «нормального» профілю трафіку для даного пристрою або групи пристроїв. Шаблон «нормального» трафіку мережі складається протягом часу на основі статистичних даних. Прикладами аномалій, є раптове збільшення інтенсивності трафіку від робочої станції або зміна структури трафіку в порівнянні зі звичайними щоденними показниками для даної мережі або пристрою.

При виявленні мережевої аномалії, з метою прийняття рішення про подальші дії, необхідно ретельно вивчити її природу, потенційну небезпеку та можливі наслідки, тобто вирішити задачу класифікації, використовуючи нейронні мережи. Задача класифікації полягає в визначенні приналежності об'єкта з певною ознакою до одного з відомих класів. В нашому випадку ознаками виступають дані телеметрії (кількість з'єднань, обсяг трафіку, вільна пам'ять, завантаження ЦПУ, інші вичерпні ресурси), а класами – тип аномалії. Пропонується використовувати нейронну мережу для класифікації трафіку та прийняття рішення для блокування ip-адреси.

Спочатку необхідно підготувати дані та утворити вибірку, яка використовується для навчання нейронної мережі. Дані надходитимуть з log-файлу, який містить системну інформацію про роботу сервера і інформацію про дії користувачів. З log-файлу виділимо важливі ознаки: ip (адреса, звідки надійшов запит); тип запиту (HEAD / GET / POST /); Url (адреса ресурсу); HTTP version (версія протоколу передачі даних); Referer (попередня веб-сторінка); User-Agent (браузер, пошуковий робот, мобільний телефон та інші пристрої); статус відповіді від серверу (200, 404, 502, 503 тощо).

Спроектуємо нейронну мережу з одного прихованого шару, який складається з 14 нейронів. Активаційна функція нейронів прихованого шару – сигмоїдна. Вхідний шар складається за кількістю ознак з семи нейронів. Вихідний шар активується функцією softmax і повертає ймовірності належності ip-адреси до того чи іншого класу. Адреси, які потрапили до кластеру «поганих» відсилаються в фаєрвол [2].

Вибірку даних, яка складається з біль ніж 3000 об'єктів було поділено на дві частини у пропорції 70:30 для уникнення перенавчання. Для навчання нейронної мережі був використаний метод зворотного поширення помилки, навчання виконувалось впродовж 1000 епох. Якість визначення класу відіграє вирішальну роль у блокуванні шкідливого трафіку та пропущення легітимних адрес, і складає 87%.

Робота розробленого програмного модуля була апробована в лабораторних умовах з використанням даних, що відповідають реальним DDOS-атакам.

Список літератури

1. **Щелухин О.И., Сакалема Д.Ж., Филинова А.С.** Обнаружение вторжений и компьютерные сети., / О.И. Шелухин - М.: Горячая линия- Телеком, 2013. - 220 с.

2. **Тарасов Я. В.** Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети [Електронний ресурс] / Я. В. Тарасов // Известия ЮФУ. Технические науки. – 2015. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/metod-obnaruzheniya-nizkointensivnyh-ddos-atak-na-osnove-gibridnoy-neyronnoy-seti.