Статистический анализ сетевого трафика и выявление DDoS-атак

Соседова Надежда Ивановна

Аспирант

Тихоокеанский государственный университет, Хабаровск, Россия

E-mail: elena_chal@mail.ru

Научный руководитель *— Карачанская Елена Викторовна*

Проблема защиты от сетевых атак и информировании о них стоит особенно остро последние несколько лет. Активная цифровизация привычной деятельности в эпоху повышенной заболеваемости по всему миру привела к стремительному росту числа всевозможных онлайн сервисов и повышения их критичности для людей в 2019-2021 годах, а обостряющаяся ситуация в мире в 2022 году вызвала беспрецедентную волну сетевых атак на них, в том числе и DDoS-атак.

Для выявления сетевых атак различного характера, в том числе и DDoS, автором разработан статистический метод, построенный на принятии решений о нормальности или аномальности сетевого трафика исходя из удаленности параметров, рассчитываемых в режиме времени близком к реальному, от эталонных [1]. Основополагающим предположением данного метода является предположение о самоподобии сетевого трафика, поэтому сравниваемыми величинами являются параметры Хёрста. За основную единицу наблюдения приняты флаги транспортного уровня SYN и ACK в единицу времени, для них и производится расчет параметров Херста.

Анализ и выявление аномалий в сетевом трафике выполняется по следующему алгоритму:

1. выбор оптимальных окон наблюдений для расчета эталонных значений;

2. расчет эталонных значений, с которыми будет производится сравнение сетевого трафика при выявлении аномалий (расчет параметров Хёрста для всех выбранных окон наблюдения, формирование доверительного интервала);

3. обнаружение аномалий сетевого трафика в режиме времени близком к реальному (оценка попадания рассчитываемых параметров Хёрста в доверительных интервал).

Для расчета параметра Хёрста выбран метод RS-анализа.

Для тестирования метода разработано программное обеспечение и проведен ряд экспериментов. Целевым устройством (устройством, подвергаемым атакам) являлся персональных компьютер под управлением операционной системы Windows 10 с размещенным на нем программным обеспечением для выявления аномалий. Атаки осуществлялись по беспроводному каналу связи с ноутбука под управлением операционной системой Arch Linux. Для имитации DoS-атак были использованы программные продукты для операционной системы семейства Linux: hping3, BoNeSi и проведено сканирование портов при помощи nmap.

Для проведения тестирования программного обеспечения были следующие окна наблюдения: 5, 20, 30 и 60 секунд. Затем был проведен расчет эталонных значений для каждого окна наблюдения и получены доверительные интервалы.

По результатам трех экспериментов были сделаны следующие выводы:

1. программное обеспечение по выявлению аномалий сетевого трафика, а следовательно, и метод, являются состоятельными в части выявления DoS-атак;

2. при симуляции атак происходит их установление на всех окнах наблюдений, выбранных в данном эксперименте;

3. окна наблюдений менее 10 секунд не могут быть использованы, так как дают ложные срабатывания и на нормальном трафике;

4. если интенсивность атаки равномерна на промежутке времени, равном времени обучения сетевого трафика, то аномальный трафик становится самоподобным, а программное обеспечение перестает выдавать сообщение об аномалиях.

Литература

1. Карачанская Е. В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре. Безопасность информационных технологий. 2019. Т. 26, № 1. С.98–110.