Афонцев Э.В., соискатель
Поршнев С.В. проф., д-р техн. наук

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ ИНТЕРНЕТ-ТРАФИКА НА ОСНОВЕ ВЫЧИСЛЕНИЯ КОЭФФИЦИЕНТА КОРРЕЛЯЦИИ

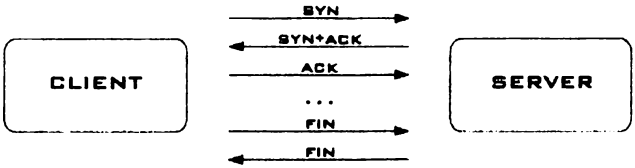
В настоящее время наблюдается стремительное развитие телекоммуникаций. Однако до сих пор задача выявления аномалий в сетях передачи данных (СПД) и Интернет остается актуальной. Авторами предлагается методика детектирования сетевых аномалий на основе вычисления коэффициента корреляции параметров трафика.

Классификация сетевых аномалий

Сетевые аномалии делятся на две основные группы: программно-аппаратные отклонения и проблемы безопасности. К программно-аппаратным отклонениям относятся: аппаратные неисправности, ошибки конфигурирования, ошибки программного обеспечения и проблемы производительности оборудования. Нарушения сетевой безопасности включают в себя следующие аномалии: сканирование, атаки с целью отказа от обслуживания, вирусная активность, распространение программных "червей", эксплуатация уязвимостей, анализаторы трафика (сниферы) и сетевые модификаторы. Наибольший экономический ущерб операторам связи наносят атаки с целью перегрузки сетей или сервисов и сетевая вирусная активность.

Интернет-трафик

Структура протоколов Интернет-трафика описывается эталонной моделью открытых систем Open Systems Interconnection (OSI). Межсетевому уровню взаимодействия (Layer 3) соответствует Internet Protocol (IP). Каждый пакет IP состоит из заголовка и блока данных. В заголовке содержатся параметры передачи, основными из которых являются адреса источника (Source IP) и назначения (Destination IP). В свою очередь, пакет IP инкапсулирует данные протоколов транспортного уровня (Layer 4), таких как TCP и UDP. Учитывая подавляющее преобладание трафика TCP, рассмотрим модель взаимодействия участников сетевого соединения в рамках протокола TCP более подробно (рисунок). Клиент посылает в сторону сервера пакет с установленным флагом синхронизации потока (Synchronize - SYN). В ответ на это сервер посылает пакет уведомления и установления встречной синхронизации (Acknowledge – ACK и Synchronize - SYN). Клиент подтверждает установление соединения пакетом уведомления (Acknowledge – ACK). Дальше идет обмен данными (только флаги ACK). Завершается процесс взаимной посылкой пакетов с флагом закрытия соединения (Finish) или разрыва (Reset).



Модель взаимодействия TCP

В итоге процесс передачи данных заключается в дуплексном обмене IP пакетами между участниками сетевого взаимодействия.

Коэффициент корреляции параметров Интернет-трафика

В общем случае коэффициент корреляции для сигналов x и y рассчитывается по формуле:

$$\rho = \frac{\sum_{i=1}^{N}(x_i - \bar{x}) \cdot (y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \cdot \sum_{i=1}^{N}(y_i - \bar{y})^2}}, \quad (1)$$

где $\bar{x}$ и $\bar{y}$ - средние значения сигналов, N - число отсчетов сигналов x и y.

Для расчета коэффициента корреляции TCP/IP трафика по формуле (1) авторами выбраны следующие параметры:

x_i - число пакетов с уникальным адресом IP_i, присутствующим в позиции адреса источника (Source IP),

y_i - число пакетов с тем же самым уникальным адресом IP_i, присутствующим в позиции адреса назначения (Destination IP),

$\bar{x} = \frac{\sum_{i=1}^{N} x_i}{N}$ - среднее число пакетов с уникальным адресом IP_i, присутствующим в позиции адреса источника (Source IP),

$\bar{y} = \frac{\sum_{i=1}^{N} y_i}{N}$ - среднее число пакетов с тем же самым уникальным адресом IP_i, присутствующим в позиции адреса назначения (Destination IP),

N - общее число уникальных IP_i адресов.

Методика проведения измерений

Для детектирования аномальной сетевой активности авторами применяется следующая методика:

1. Производится перехват сетевого трафика Интернет-магистрали (утилитой Tcpdump) с записью заголовков пакетов вплоть до транспортного уровня инкапсуляции.

2. С помощью обработки сигнатурным детектором (Snort IDS) выявляется наличие аномалий.
3. Вычисляется значение коэффициента корреляции по формуле (1) для IP адресов.

Результаты расчетов

Для экспериментальной проверки предлагаемого метода использовались дампы нормального и аномального трафика (по 100 дампов объемом 100000 пакетов), созданные случайным образом в течение одного месяца работы Интернет-магистрали. Аномальный трафик составляла вирусная сетевая активность и сканирование. В результате получено значение коэффициента корреляции для нормального IP трафика, равное 0.9 ± 0.1. Коэффициент корреляции для аномального трафика не превышает 0.6.

Заключение

Экспериментальная проверка предлагаемой методики позволяет сделать вывод о надежном детектировании сетевых аномалий при помощи вычисления коэффициента корреляции заголовков пакетов IP трафика.