УДК 004.942
А.М. Луцків, канд. техн. наук, доцент, В.Ю. Бутинець
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ АНАЛІЗУ ТРАФІКУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

UDC 004.942
A.M. Lutskiv PhD, Assoc. Prof., V.Yu. Butynets

METHODS OF COMPUTER NETWORK TRAFFIC ANALYSIS

Більшість програмних продуктів, які функціонують у комп'ютерній мережі передають дані через вже відомі порти апаратного забезпечення. У такому випадку, суть задачі класифікації пакетів полягає у знаходженні TCP SYN-пакету для встановлення серверної частини клієнт-серверного з'єднання на основі TCP. Після цього, необхідно одержати результат щодо доступності цільового номера порту для конкретного додатку, який надіслав пакет. По такому ж принципу працює класифікація пакетів на основі UDP, однак з'єднання при цьому не встановлюється.

Найбільш вагомою перевагою даного методу є простота реалізації та швидкість виконання операцій щодо класифікації. Однак даний метод має і ряд недоліків. До них належать:

– відсутність у деяких програмних продуктів власних портів, які зареєстровані в IANA (функція управління IP адресним простором);

– здатність програмних додатків використовувати відмінні від визначених в операційній системі портів для виконання певних функцій, наприклад, використання відмінного від порта «80» в Unix-подібних системах для HTTP-сервера;

– виникнення помилок при шифруванні на IP рівні, що може спровокувати плутанину TCP і UDP заголовків.

Інший підхід базується на тому, що для зменшення залежності від портів і одержання достовірних даних про використовуваний протокол, застосовуються методи відновлення стану сеансу та аналізуються дані щодо вмісту кожного окремого пакету.

Класифікація на основі корисного навантаження для peer-to-peer трафіку передбачає аналіз його сигнатур на прикладному рівні. Застосування такої класифікації пакетів дає змогу зменшити кількість помилок першого і другого роду до 5%.

Класифікацію, базовану на корисному навантаженні, можна організувати шляхом застосування наступних методів перевірки та опрацювання:

– PBNS (Packet Based No State);
– PBFS (Packet Based Per Flow State);
– MBFS (Message Based Per Flow State);
– MBPS (Message Based Per Protocol State).

Статистичні методи дають змогу аналізувати трафік у комп'ютерних мережах за двома підходами: на основі алгоритмів аналізу поведінки трафіку; статистичні методи аналізу трафіку на мережевому і транспортному рівнях.

Основна ціль алгоритмів аналізу поведінки трафіку ґрунтується на визначенні додатків, які генерують найбільшу частину трафіку у комп'ютерній мережі. У результаті такого аналізу можна виявити, яким чином вузли комунікують між собою і яке програмне забезпечення функціонує на них.