ИДЕНТИФИКАЦИЯ ПРИНАДЛЕЖНОСТЕЙ СЕТЕВЫХ ПОТОКОВ ПРИ ПОМОЩИ ЭНТРОПИЙНОГО АНАЛИЗА

Булахов Н.Г., Кузнецов В.С.

Томский Государственный Университет,
Радиофизический ф-т, каф. Квантовой электроники и фотоники,
Россия, 634050, г. Томск, ул. Ленина 36,
Тел.: +7-923-402-72-32,
E-mail: nik@rff.tsu.ru

IT отделы современных предприятий, а также провайдеры Internet часто решают задачу идентификации сетевых информационных потоков для установления их принадлежности тому или иному классу программного обеспечения. В современных условиях задача усложняется за счет того, что программное обеспечение может маскировать свою сетевую активность и шифровать передаваемые данные.

Принципиально новые возможности идентификации сетевых потоков позволяет достичь метод энтропийного анализа заголовков информационных пакетов, из которых состоят данные потоки. Суть метода состоит в анализе информационной энтропии значений полей заголовков информационных пакетов, передаваемых по сети. Вычисление энтропийных характеристик осуществляется по формуле Шеннона $H = -\sum P_i log_2 P_i$, где H - информационная энтропия согласно определению Шеннона, P_i - вероятность некоторого события. Такой подход дает возможность проводить анализ заголовков пакетов без просмотра их содержимого. Используя эту особенность, можно решить проблемы, связанные с шифрованием передаваемых данных, а также увеличить скорость обработки данных благодаря малой ресурсоемкости рассматриваемого метода. Стоит отметить, что использование такого подхода дает нам высокую точность дифференциации сетевых потоков (более 95%), в частности определения типа используемого программного обеспечения, генерирующего сетевой трафик и выявление распространения в сети компьютерных червей. Дифференциацию сетевых потоков можно производить по измерениям информационной энтропии IP- и MAC-адресов, TCP- и UDP-портов источника и назначения в передаваемых по сети пакетов.

На основе предложенного авторами метода выполнена программная реализация дифференциации сетевых потоков, используемая для мониторинга состояния сети Радиофизического факультета Томского государственного университета. Программа успешно помогает выявлять аномалии состояния сети и ликвидировать большой класс проблем на ранней стадии их возникновения.

Литература.

1. *Булахов Н.Г., Медведев В.Д., Кузнецов В.С.* Практическое применение энтропийного метода анализа сетевых потоков *// Изв. Вузов. Физика, № 9/2, 2013, Стр. 244-246*.