АЛГОРИТМ КОМПЬЮТЕРНОЙ ПРОГРАММЫ ДЛЯ МОНИТОРИНГА ТРАФИКА IP-ТЕЛЕФОНИИ

Белорусский государственный университет информатики и радиоэлектроники
г.Минск, Республика Беларусь

Гончаров П.А.

Утин Л.Л.

Основу современных сетей телекоммуникаций составляют узлы цифровой коммутации каналов и пакетов. В широкополосных сетях с интеграцией служб и мобильных сетях связи третьего и четвертого поколения базовым протоколом передачи информации является IP. Интерес различных субъектов рынка телекоммуникационных услуг к данному виду связи необычайно возрос в связи с разработкой новых стандартов и протоколов когда IP-телефонный разговор вплотную приблизился по качеству к телефонному разговору по телефонным сетям. Этот интерес объясняется тем, что IP-телефония существенно экономит требуемую полосу пропускания каналов.

В качестве наиболее популярных областей практического применения можно выделить анализ трафика с целью выявления проблем в работе сети, в том числе, несанкционированной активности; восстановление потоков данных, предотвращение различного рода сетевых атак, сбор статистики.

Телефонный разговор – это интерактивный процесс, не допускающий больших задержек. В соответствии с рекомендацией ITU–T G. 114 для большинства абонентов задержка речевого сигнала на 150 мс приемлема, а на 400 мс – недопустима. Общая задержка речевой информации делится на две основные части - задержка при кодировании и декодировании речи в шлюзах или терминальном оборудовании пользователей и задержка, вносимая самой сетью.

Основными открытыми протоколами IP- телефонии являются:

- SIP (Session Initiation Protocol) –протокол устанавления сеанса, используемый для определения местоположения пользователей сети и создание канала для передачи данных.
- RTP/SRTP (Real-time Transport Protocol) – протокол транспортного уровня и используется для передачи трафика в реальном времени.
- IAX (Inter-Asterisk eXchange Protocol) – протокол обмена VoIP данными между оконечными устройствами.

Анализ компьютерной сети является необходимым процессом и в первую очередь ориентирован на поиск дефектов в процессах передачи сетевого трафика, как при начальном формировании сети, так и для поддержания в дальнейшем ее работоспособности.

Основным преимуществом программы анализа трафика является:

- Учет трафика индивидуального хоста по любому IP протоколу.
- Одновременный сбор трафика с нескольких сетевых адаптеров.
-Фильтрация пакетов с функцией анализа состояния соединения.

Мониторинга трафика упрощает работу системного администратора в выполнении поставленной задачи в кратчайшие сроки, а также выполнят свою основную функцию как решение сетевых проблем. Также облегчает понимание и знание функционала данного программного обеспечения, последовательность ее действий.

Система мониторинга должна обеспечивать захват 100% трафика и предоставлять эффективные методы анализа с навигацией по результатам. Если говорить о комплексном решении задачи анализа сетевого трафика, то в первую очередь следует разделить ее на три в достаточной степени независимые подзадачи: перехват трафика, его хранение и анализ

Изучение современных методик анализа сетевого трафика показало, что статистическое исследование трафика, исходящего из сети пользования во внешнюю сеть на текущий момент активно не используется в системах защиты. Основное направление подобных систем – это мониторинг работоспособности оборудования, нагрузки на каналы; а для локальных сетей – это защита от угроз приходящих из внешней сети.

Список использованных источников:

1. Гольдштейн Б.С, Пинчук А.В, Суховицкий А.П. IP-телефония М.: Радио и связь, 2006. – 336 с.
2. Кайлачакова Д.И. Система анализа сетевого трафика // Магистерская диссертация : тез. докл. Институт космических и информационных технологий ,Красноярск, 2016. - Красноярск: Сибирский Федеральный Университет,, 2016. – 56с.
3. Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика [Электронный ресурс] // сборники трудов Института системного программирования Российской академии наук. – 2014. http://www.ispras.ru/preprints/docs/prep_27_2014.