УДК 004.716

ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ КАК СРЕДСТВО АНАЛИЗА И КОНТРОЛЯ ТРАФИКА

О.А. РОМАНЕНКО

Белорусский государственный университет информатики и радиоэлектроники, РеспубликаБеларусь

Поступила в редакцию 31 октября 2018

Аннотация. В статье рассмотрены вопросы анализа, контроля и фильтрации трафика при помощи глубокой инспекции пакетов в сетях операторов связи. Содержится общее описание технологии, а также кратко освещены этапы ее развития. Описываются способы внедрения технологии глубокой инспекции пакетов в сетях связи.

Ключевые слова: глубокая инспекция пакетов, контроль трафика, фильтрация трафика, сетевая безопасность.

Введение

DPI (Deep Packet Inspection) – это совокупное название технологии, позволяющей проводить в режиме реального времени накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого.

Технологии инспекции трафика развивались последовательно, каждая последующая наследовала часть предыдущих механизмов и добавляла новые. На рис. 1 представлены уровни развития технологии.

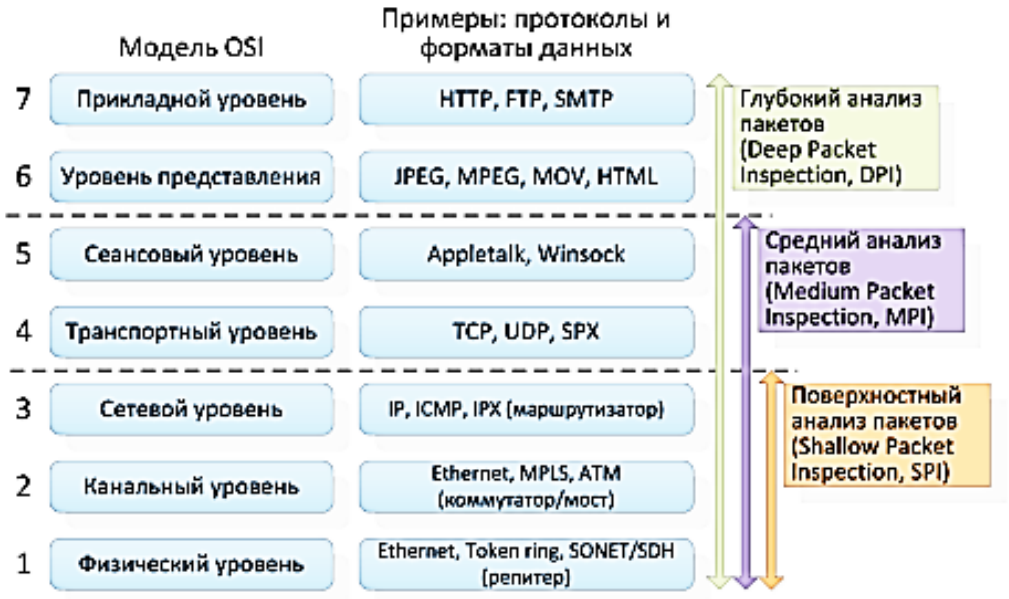

Рис. 1. Уровни развития технологии инспекции трафика

Поверхностный анализ пакетов

SPI (Shallow Packet Inspection) – технология анализа трафика, основывающаяся исключительно на анализе заголовков пакетов уровней L2–L3 модели OSI. SPI осуществляет

проверку только заголовков пакетов для оптимизации маршрутизации, обнаружения попыток злоупотребления сетью и статистического анализа. Если информация пакета находится в «черном списке», пакет отбрасывается. Средства поверхностного анализа пакетов эффективны для межсетевых экранов, которые могут отделять сети друг от друга, разрешать или запрещать трафик в зависимости от выбранного протокола передачи. В связи с тем, что технология работает на канальном и сетевом уровнях модели OSI, к вычислительным ресурсам SPI предъявляются низкие требования, что позволяет обрабатывать большие объемы трафика с высокой скоростью. Технология получила широкое распространение: на ее основе работает большинство межсетевых экранов операционных систем (в частности, в ОС Windows XP/Vista и OS X), маршрутизаторов и других сетевых устройств. На ее основе реализованы сетевые списки контроля доступа на уровне IP-адресов и портов (ACL, Access Control List)). Таким образом, технология SPI хорошо подходит для разграничения доступа извне к отдельным компьютерам и сервисам внутренней сети.

Средний анализ пакетов

MPI (Medium Packet Inspection) – технология анализа трафика, основанная на инспектировании сессий и сеансов связи, инициированных приложением, но устанавливаемых шлюзом-посредником. Также применяется термин «прокси приложений» (application proxy). В рамках этой технологии содержимое пакетов анализируется частично и по предопределенным правилам. Не используются сложные методы анализа типа сигнатурного. Устройства, реализующие функциональность, размещаются между Интернет-провайдером и конечным пользователем. Данные устройства разбирают заголовки вплоть до транспортного уровня и небольшую часть данных пакета для сопоставления разобранной части с некоторым списком разбора (parse list). Списки разбора по сравнению со списками ACL являются более короткими и предоставляют более широкий диапазон действий. Набор протоколов, как правило, очень ограничен. Например, в первых версиях CheckPoint FireWall-1 (CheckPoint FW-1) поддерживались протоколы Telnet, FTP, HTTP, а в Cisco Private Internet Exchange (Cisco PI X) – FTP, HTTP, H.323, RSH, SMTP и SQLNET. В дальнейшем данные наборы незначительно расширялись.

Технология MPI более гибкая по сравнению с SPI и, помимо разграничения доступа, подходит для большего числа задач: кэширование содержимого, анализ сжатого/шифрованного трафика, ограничение функциональности отдельных протоколов путем запрета отдельных команд.

Основной недостаток технологии среднего анализа пакетов – плохая масштабируемость. Это заключается в том, что каждая команда и протокол требуют отдельного шлюза (входного и выходного портов). Кроме того, работа в режиме прокси сильно снижает скорость обработки [1]. Эти факторы ограничивают применение этой технологии на уровне Интернет-провайдеров вследствие необходимости анализа большого числа протоколов и команд.

Глубокий анализ пакетов

DPI (Deep Packet Inspection) – технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэров, DPI анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше.

Одной из важнейших функций DPI является поддержка управления эффективной загрузкой сети путем ограничения тяжелого трафика, например, файлообменных сетей P2P (Peer-to-Peer), потокового видео, а также других ресурсоемких услуг. Средства DPI позволяют выявлять принадлежность потока пакетов к конкретному приложению, а затем при необходимости блокировать или ограничивать его скорость передачи, прогнозировать уровень загрузки каналов тем или иным трафиком, распределять сетевые ресурсы между разными приложениями, не допускать перегрузок и повышать качество обслуживания. Такая возможность появляется за счет того, что технология DPI обеспечивает полный разбор первых пакетов потока трафика. В дополнение применяются статистические методы слежения за характеристиками потока.

Например, из HTTP-трафика легко извлекаются URL запрашиваемых страниц. Далее они могут использоваться для сравнения с «черными» или «белыми» списками или для ведения статистики обращения пользователей к различным ресурсам [2].

Основной метод DPI – проверка сигнатур протоколов и приложений. Под сигнатурой понимается шаблон описания данных, который однозначно соответствует приложению или протоколу. Например, это может быть поиск таких ключевых слов в данных пакета, как BitTorrent, или запросов GET/POST протокола HTTP. Простейшие сигнатуры основаны на URL-адресах в заголовке HTTP, а сам файл сигнатур вендора периодически обновляется. Часть методов DPI основана на статистических и поведенческих критериях анализа потока данных. Именно поведенческий анализ позволяет обнаружить сканирование портов, выполняемое одним источником. В более сложных случаях сигнатура основана на анализе параметров связанных потоков одного приложения. Все эти сигнатуры используются для выявления используемых потоком приложения IP-адресов и транспортных портов, а также для дальнейшего контроля над потоком данных [3].

Среди задач, которые позволяет решить технология DPI, можно выделить следующие: контроль приложений; назначение политик для трафика приложений; оптимизация полосы пропускания; предоставление новых услуг; родительский контроль; защита от DDoS-атак; антиспам; веб-фильтрация; антивирусная защита; управление абонентами; управление квотами; уменьшение P2P; оптимизация видео потоков и HTTP-трафика; визуализация сети; динамический просмотр загрузки сетевых ресурсов и построение отчетов по приложениям, абонентам, базовым станциям.

DPI-технология может быть реализована двумя путями: распределенное и локальное подключение. Распределенная система состоит из пробников (probes) для сбора данных о сетевом трафике и набора его анализаторов (collectors), которые получают данные от пробников. Локальные системы подключаются к конкретному каналу передачи данных. Они могут находиться как на стороне конечного пользователя, так и на стороне шлюза. Локальные системы на стороне конечного пользователя подключаются на уровне сетевой карты пользователя. В то время как локальные системы на стороне шлюза подключаются в точке, которая является единственным выходом в глобальную сеть для некоторой локальной подсети.

Как правило, DPI-система устанавливается на границе сети оператора таким образом, чтобы весь трафик, который покидает сеть или входит в нее, мог анализироваться этой системой. На рис. 2 представлено одно из типовых решений подключения DPI-системы на границе сети оператора.

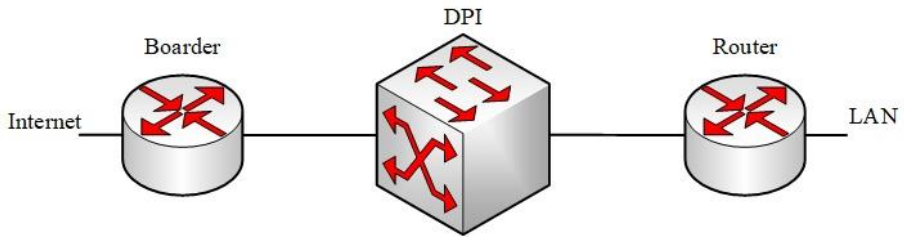

Рис. 2. Типовое решение подключения DPI системы в сеть

Для решения специфических задач систему глубокого анализа пакетов устанавливают не на границе сети, а ближе к конечным пользователям, например, на уровень BRAS/CMTS/GGSN/. Это может быть полезно тем операторам, которые по ряду причин помимо контроля внешних каналов хотят решать задачу контроля внутренних [4].

DPI-системы часто используется провайдерами для контроля трафика, а иногда и для блокировки некоторых протоколов или сайтов (целиком или отдельно взятые страницы). С помощью глубокой инспекции пакетов можно определить, какое приложение сгенерировало или получает данные, и на основании этого предпринять какое-либо действие. Кроме того, DPI-система может обнаруживать среди общего потока трафика фрагменты, соответствующие компьютерным вирусам и блокировать их, повышая тем самым безопасность сети. Технология также позволяет демонстрировать пользователю рекламу в зависимости от содержимого его пакетов.

Заключение

Системы глубокого анализа пакетов позволяют операторам в режиме реального времени проводить анализ пакетов на всех уровнях модели OSI. Помимо изучения пакетов по неким стандартным параметрам, по которым можно однозначно распознать принадлежность пакета к определенному приложению, например, по формату заголовка или номера порта, технология DPI осуществляет анализ того, как ведет себя трафик. Все это открывает большие перспективы коммерческого использования технологии оперативного перехвата и анализа трафика. Также обеспечивается корпоративная сетевая безопасность и защищенность инфокоммуникаций оператора связи.

DEEP PACKET INSPECTION AS A MEANS OF ANALYSIS AND TRAFFIC FILTRATION

O.A. ROMANENKO

Abstract. This article deals with analysis, control and filtration of traffic using deep packet inspection in the networks of telecom operators. It contains general explanation of technology as well as brief description of stages of development. The ways of implementing of deep packet inspection technology are listed in this paper.

Keywords: deep packet inspection, traffic control, traffic filtration, network security.

Список литературы

1. Гетьман А. И., Евстропов Е.Ф., Маркин Ю. В. // Препринт ИСП РАН. 2015. № 28. С. 7–8
2. Фицов В.В. //. Вестник связи. 2016. № 11. С. 25
3. Фицов В.В. // Первая миля. 2015. № 8. С. 57
4. Гольдштейн Б.С., Фицов В.В. // Вестник связи. 2018. № 09. С. 8