УДК 612.087 DOI: 10.34824/VKNIIRAN.2021.6.2.014

ИССЛЕДОВАНИЕ ВЛИЯНИЯ РАЗЛИЧНЫХ ТИПОВ УСЛУГ НА ПРОИЗВОДИТЕЛЬНОСТЬ DPI СИСТЕМ

© Лорсанов Усман Шамильевич (a), Закриева Петимат Ахмедовна (b), Хасамбиев Ибрагим Вахаевич (c), Юнусова Зулихан Умаровна (d)

(a) Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова, Российская Федерация, г. Грозный
(b) Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова, Российская Федерация, г. Грозный
(c) Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова, Российская Федерация, г. Грозный
(d) Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова, Российская Федерация, г. Грозный

Аннотация. Система DPI выполняет глубокий анализ пакетов – анализ на верхних уровнях модели OSI, а не только по стандартным номерам сетевых портов. Помимо изучения пакетов по неким стандартным шаблонам, по которым можно однозначно определить принадлежность пакета определённому приложению: по формату заголовков, номерам портов и прочему, система DPI осуществляет и так называемый поведенческий анализ трафика, который позволяет распознать приложения, не использующие для обмена данными заранее известные заголовки и структуры данных, к примеру, BitTorrent.

Основная проблема всех существующих решений DPI заключается в том, что для того, чтобы однозначно определить принадлежность того или иного потока данных к одному из сетевых приложений, устройство, осуществляющее анализ трафика, должно обрабатывать оба направления сессии: входящий и исходящий трафик в пределах одного потока должны пройти через одно и то же устройство.

Ключевые слова: DPI система, производительность DPI, различные типы услуг, контроль пакетов.

RESEARCH OF THE INFLUENCE OF DIFFERENT TYPES OF SERVICES ON THE PERFORMANCE OF DPI SYSTEMS

© Lorsanov Usman Shamilevich (a), Zakrieva Petimat Akhmedovna (b), Khasambiev Ibragim Vakhaevich (c), Yunusova Zulikhan Umarovna (d)

(a) Grozny State Oil Technical University by Acad. M.D. Millionshikov, Russian Federation, Grozny
(b) Grozny State Oil Technical University by Acad. M.D. Millionshikov, Russian Federation, Grozny

(c) Grozny State Oil Technical University by Acad. M.D. Millionshikov, Russian Federation, Grozny
(d) Grozny State Oil Technical University by Acad. M.D. Millionshikov, Russian Federation, Grozny

Abstract. DPI system performs deep packet inspection - analysis at the upper layers of the OSI model, not just the standard network port numbers. In addition to studying packets according to certain standard templates, by which you can unambiguously determine whether a packet belongs to a particular application: by the format of the headers, port numbers, and so on, the DPI system also performs the so-called behavioral traffic analysis, which allows you to recognize applications that do not use previously known headers for data exchange. and data structures, for example, BitTorrent.

The main problem of all existing DPI solutions is that in order to unambiguously determine whether a particular data stream belongs to one of the network applications, a device performing traffic analysis must handle both directions of the session: incoming and outgoing traffic within the same stream must go through the same device.

Key words: DPI система, производительность DPI, различные типы услуг, контроль пакетов.

Глубокий контроль пакетов, который также известен как DPI, извлечение информации, IX или полный контроль пакетов, является одним из видов фильтрации сетевых пакетов. Глубокая проверка пакета оценивает часть данных и заголовок пакета, который передается через точку проверки, отсеивая любые несоответствия протоколу, спаму, вирусам, вторжениям и любым другим определенным критериям, чтобы заблокировать пакет от прохождения через точку проверки.

DPI также используется для принятия решения о том, будет ли конкретный пакет перенаправлен в другое место назначения. Короче говоря, DPI способна находить, обнаруживать, классифицировать, блокировать или перенаправлять пакеты, имеющие определенный код или полезную нагрузку данных, которые не обнаруживаются, не обнаруживаются, не классифицируются, не блокируются и не перенаправляются обычной фильтрацией пакетов. В отличие от простой фильтрации пакетов, DPI выходит за рамки изучения заголовков пакетов. [10]

Как работает DPI

DPI - это форма фильтрации пакетов, обычно выполняемая как функция вашего брандмауэра. Он применяется на прикладном уровне Межсоединения открытых систем.

DPI оценивает содержимое пакета, проходящего через контрольную точку. Используя правила, назначенные вами, вашим интернет-провайдером, сетевым или системным администратором, deep packet inspection определяет, что делать с этими пакетами в режиме реального времени.

DPI способна проверить содержимое этих пакетов, а затем выяснить, откуда они пришли, например, от службы или приложения, которое их отправило. Кроме того, он может работать с фильтрами для поиска и перенаправления сетевого трафика с онлайн-сервиса, такого как Twitter или Facebook, или с определенного IP-адреса.

Обычная фильтрация пакетов считывает только информацию заголовка каждого пакета. Это был базовый подход, который был менее сложным, чем современный подход к фильтрации пакетов, во многом из-за технологических ограничений того времени. У брандмауэров было очень мало вычислительной мощности, и этого было недостаточно для обработки больших объемов пакетов. Другими словами, обычная пакетная фильтрация была похожа на чтение названия книги, без осознания или оценки содержания внутри обложки.

С появлением новых технологий стала возможной DPI. По мере того как она становилась все более основательной и полной, она становилась все более сравнимой с тем, как взять книгу, открыть ее и прочитать от корки до корки.

Deep Packet Inspection (DPI) вызывается для работы с этой глубиной. Он проверяет как адреса, так и основной текст и даже может назвать службу или приложение, которое сгенерировало этот самый пакет. Самое главное: пользователь DPI вводит параметры проверки самостоятельно, критерии анализа полностью настраиваемы. Так же просто, как применить фильтр к вашему почтовому ящику, не так ли? Но DPI может пойти еще дальше – например, сверить порты с их привычным использованием или специально созданным списком. Есть подтвержденные случаи, когда владельцы сетей обнаруживали с помощью DPI некоторые серьезные злоупотребления своими собственными сетями – например, создание пирингового обмена пиратскими фильмами, например.

Увы, методы DPI также могут быть использованы в качестве препятствия для свободного потока информации. Об этом позже [9].

Еще одна задача, в которой DPI не менее хорош, - это организация дорожного движения. В соответствии с критериями, установленными, опять же, конкретным пользователем, любой пакет может быть обнаружен, а затем не только заблокирован, но и классифицирован и/или перенаправлен в режиме реального времени. Это очень важно для организаций, которые заботятся как о безопасности, так и о качестве своего трафика, операторов связи и интернет-провайдеров, которые должны быть названы в первую очередь.

Примеры включают (но слишком далеки от того, чтобы ограничиваться):

– Бизнес, ориентированный на продажи – скажем, через собственный интернет – магазин, - тем не менее демонстрирует определенный уровень активности в социальных сетях и видеопотоках. DPI этикетки, связанные с магазином трафика на переднем плане один в то время как YouTube, Facebook и т.д. являются 2-й уровень отныне;

– Телекоммуникационный провайдер – получение наиболее четкой картины “каковы мои абоненты”, включая модели использования трафика, уровень спроса на любую доступную услугу и масштабируемые срывы пиковых нагрузок сети. Это относится и к упомянутому “качеству трафика”, или, что более разумно, к наилучшему возможному использованию выделенных полос пропускания (QoS); [1]

– Практически любой крупный (читай – городской или районный) поставщик коммунальных услуг или аварийная служба. Информация, которую DPI распознает как срочную,

может обойти любые очереди обычных данных и быть отправлена немедленно. Эта же система может предотвратить атаки, связанные с 5G, блокируя вредоносные запросы от устройств в рамках IoT framework;

– Любая организация, работающая преимущественно с конфиденциальной или защищенной авторским правом информацией: например, правоохранительные органы, лейбл звукозаписи или издательство. Пакеты, не совместимые с настройками DPI, не будут пропускаться, что предотвращает утечку несанкционированных данных. В то время как полностью совместимые сообщения могут идти без специального разрешения для каждой отправки: правила устанавливаются в/системой DPI.

Не так давно это было немыслимо из-за простых вещей. Все было сравнительно ограничено. Скромные вычислительные ресурсы делали брандмауэры окончательными решениями: они потребляли очень мало вычислительной мощности. Тонкие полосы пропускания не были предназначены для обильного потока данных, но еще менее способны к глубокому анализу пакетов.

Подход DPI, как мы уже узнали, появился как инструмент безопасности, но может сделать гораздо больше и продолжает развиваться. И словосочетание “должно быть” тоже цитировалось. Итак, Глубокая проверка пакетов действительно является силой, находящейся с вами против темной стороны?

Зависит. Не в системе как таковой: человеческий фактор вступает в игру, как обычно. Определенно, на темной стороне находится возможность использовать DPI для цензуры и шпионажа. Правительство Китая сумело создать свою собственную Великую (Огненную)стену, используя функции DPI. Результаты, с одной стороны, вполне осуществимы: у Китая есть свой собственный Facebook (WeChat) и десятки других местных сервисов, которые заменяют глобальные. С другой стороны, это просто пугает: DPI может отрезать такую большую страну, как Китай, от Всемирной паутины.

Самый последний случай-интернет-блэкауты в Беларуси. Власти, часто именуемые “последней диктатурой Европы”, неоднократно сворачивали внешние ворота страны (принадлежащие государству), чтобы лишить протестное движение связи. По мнению официального Минска, в этом виноват Запад, как бы “блокирующий доступ”. Довольно быстро выяснилось, что некая, ранее канадская, компания поставляла в Беларусь соответствующую посуду. Так что на самом деле ни весь трафик не был остановлен, ни шлюз не был закрыт. Запросы – все они – были просто перенаправлены в DPI. Вызвав колоссальное замедление движения, практически общегосударственный коллапс [3].

Последние новости: ранее канадская компания name-starts-with-an-S отказалась от дальнейшей поддержки своих белорусских клиентов.

Вышеизложенное приводит еще один не столь яркий вопрос. Если вы, случайно или намеренно, перенаправили весь свой трафик на DPI – испытайте Медленное. Еще одним бременем является отдельная необходимость обновления и пересмотра политики DPI, поскольку этот метод делает вашу защиту более эффективной, но несколько сложной. Так что, по крайней мере, первоначальный запуск требует высококвалифицированных кадров.

Истории успеха, когда внедрение DPI сдвинулось с мертвой точки, а иногда и значительно обновило бизнес, многочисленны.

Стратегически мыслящие методы DPI представляются ценным решением для решения вопросов безопасности, защиты/конфиденциальности данных, управления производительностью (с применением сетевого анализа) и некоторых других.

Чисто технический подход показывает универсальность метода, а также его легкость в сочетании с широким спектром аппаратных средств и несравненным потенциалом обнаружения, как несомненные преимущества DPI.

Просто “думающие клиенты” означают лучшее управление трафиком и его распределение, что, в свою очередь, позволяет оператору предоставлять своим клиентам услуги более высокого качества.

Существует несколько способов глубокой проверки пакетов. Он может действовать как система обнаружения вторжений, так и комбинация предотвращения вторжений и обнаружения вторжений. Он может идентифицировать конкретные атаки, которые ваш брандмауэр, системы предотвращения вторжений и обнаружения вторжений не могут адекватно обнаружить [8].

Если в вашей организации есть пользователи, которые используют свои ноутбуки для работы, то DPI жизненно важна для предотвращения проникновения червей, шпионских программ и вирусов в вашу корпоративную сеть. Кроме того, использование глубокой проверки пакетов основано на правилах и политиках, определенных вами, что позволяет вашей сети определять, есть ли запрещенное использование одобренных приложений.

DPI также используется сетевыми менеджерами для облегчения потока сетевого трафика. Например, если у вас есть сообщение с высоким приоритетом, вы можете использовать глубокую проверку пакетов, чтобы позволить высокоприоритетной информации проходить сразу же, опережая другие сообщения с более низким приоритетом. Вы также можете установить приоритет пакетов, которые являются критически важными, перед обычными пакетами просмотра. Если у вас возникли проблемы с одноранговыми загрузками, вы можете использовать глубокую проверку пакетов для дросселирования или замедления скорости передачи данных. DPI также может быть использован для расширения возможностей интернет-провайдеров по предотвращению использования IoT-устройств при DDOS-атаках путем блокировки вредоносных запросов от устройств.

Операторы мобильной связи и другие подобные поставщики услуг также используют глубокую проверку пакетов, чтобы адаптировать свои предложения к отдельным абонентам, позволяя им дифференцировать использование данных как “все, что вы можете съесть”, "настенный сад" или "добавленная стоимость". Звукозаписывающие компании и другие правообладатели также могут попросить интернет – провайдеров заблокировать незаконную загрузку их контента-процесс, достигаемый путем глубокой проверки пакетов.

В других случаях DPI используется для предоставления целевой рекламы пользователям, законного перехвата и обеспечения соблюдения политики. DPI также может предотвратить некоторые типы атак переполнения буфера [2].

Наконец, DPI может помочь вам предотвратить утечку информации, например, при отправке конфиденциального файла по электронной почте. Вместо того, чтобы успешно отправить файл, пользователь вместо этого получит информацию о том, как получить необходимое разрешение и разрешение на его отправку.

Как и в других технологиях, DPI может также использоваться для менее чем достойных восхищения целей, таких как подслушивание и цензура. На самом деле китайское правительство, как известно, использует глубокую проверку пакетов для мониторинга сетевого трафика страны и цензуры некоторых материалов и сайтов, которые вредны для их интересов. Именно так Китай смог блокировать порнографию, религиозную информацию, материалы, касающиеся политического инакомыслия, и даже популярные веб-сайты, такие как Википедия, Google и Facebook.

Хотя DPI имеет много потенциальных вариантов использования, он может легко обнаружить получателя или отправителя контента, который он отслеживает, поэтому существуют некоторые проблемы с конфиденциальностью. Это в первую очередь касается тех случаев, когда DPI используется в контексте маркетинга и рекламы, посредством мониторинга поведения пользователей и продажи просмотра и других данных маркетинговым или рекламным компаниям [4].

Методы

Два основных типа продуктов используют глубокую проверку пакетов: брандмауэры, которые реализовали функции IDS, такие как проверка содержимого, и системы IDS, которые направлены на защиту сети, а не фокусируются только на обнаружении атак. Некоторые из основных методов, используемых для глубокой проверки пакетов, включают:

1. Сопоставление шаблонов или сигнатур – Один из подходов к использованию брандмауэров, использующих функции IDS, сопоставление шаблонов или сигнатур, анализирует каждый пакет по базе данных известных сетевых атак. Недостатком такого подхода является то, что он эффективен только для известных атак, а не для атак, которые еще предстоит обнаружить.
2. Аномалия протокола – Еще один подход к использованию брандмауэров с функциями IDS, protocol anomaly использует подход “default deny”, который является ключевым принципом безопасности. Используя этот метод, определения протоколов используются для определения того, какой контент должен быть разрешен. Это отличается от подхода, заключающегося в простом разрешении всего контента, который не соответствует базе данных сигнатур, как это происходит в случае сопоставления шаблонов или сигнатур. Основное преимущество аномалии протокола заключается в том, что она обеспечивает защиту от неизвестных атак.
3. IPS-решения – Некоторые IPS-решения реализуют технологии DPI. Эти решения имеют аналогичную функциональность встроенным идентификаторам, хотя и имеют возможность блокировать обнаруженные атаки в режиме реального времени. Одной из самых больших проблем при использовании этого метода является риск ложных срабатываний, который может быть в некоторой степени смягчен путем создания консервативной политики.

Некоторые ограничения существуют с этими и другими методами DPI, хотя поставщики предлагают решения, направленные на устранение практических и архитектурных проблем с помощью различных средств. Кроме того, решения DPI теперь предлагают ряд других бесплатных технологий, таких как VPN, анализ вредоносных программ, фильтрация антиспама, фильтрация URL-адресов и другие технологии, обеспечивающие более полную защиту сети [5].

Проблемы

Ни одна технология не совершенна, и глубокий контроль пакетов не является исключением. У него есть три явных слабости:

1. DPI очень эффективна для предотвращения таких атак, как отказ в обслуживании, переполнение буфера и даже некоторые формы вредоносных программ. Но он также может быть использован для создания подобных атак.

2. DPI может сделать ваш текущий брандмауэр и другое программное обеспечение безопасности, которое вы используете, более сложным и трудным в управлении. Вы должны быть уверены, что постоянно обновляете и пересматриваете политику глубокой проверки пакетов, чтобы обеспечить постоянную эффективность.

3. DPI может замедлить работу вашей сети, выделив ресурсы для того, чтобы ваш брандмауэр мог справиться с нагрузкой обработки.

Помимо проблем конфиденциальности и присущих ограничений глубокой проверки пакетов, некоторые проблемы возникли из-за использования сертификатов HTTPS и даже VPN с туннелированием конфиденциальности. Некоторые брандмауэры теперь предлагают проверки HTTPS, которые будут расшифровывать HTTPS-защищенный трафик и определять, разрешено ли пропускать содержимое. Тем не менее, DPI продолжает оставаться ценной практикой для целей, начиная от управления производительностью и заканчивая сетевой аналитикой, криминалистикой и безопасностью предприятия [7].

Сложно определить, какие именно услуги будут требовать пользователи в будущем, но основываясь на поведении потребителей сегодня, завтрашние предпочтения, скорее всего, составят эклектическую смесь существующего набора сервисов, сервисов на основе приложений и избирательности их использования (например, услуга родительский контроль – запрещение конкретных сервисов по требованиям отдельного пользователя). Если провайдеры будут готовы предоставлять сервисы нового уровня, тогда и они и их пользователи будут иметь преимущество, от имеющего источника генерации кастомизированных сервисов.

Конкретный набор услуг, потребляемых клиентами должен будет варьироваться с таким же стремлением, с которым будет возникать желание индивидуализации сервисов пользователями широкополосного доступа, согласно своим уникальным требованиям.

Выбор DPI систем операторского класса

(На что необходимо обратить внимание при выборе DPI системы?)

1. DPI система должна удовлетворять требования сегодняшней производительности передачи данных (10+ Gbps) и быть масштабируемой, при необходимости использования системы с большей производительностью. Вдобавок, DPI система должна поддерживать сотни тысяч подписчиков и миллионы сессий (IP flows) параллельно, без потерь пользовательского QoE.

2. Важным в выборе является мощность DPI engine, обеспечивающего анализ сетевых приложений, сетевой интеллект и видимость всех предоставляемых сервисов. DPI система, также должна иметь мощный анализатор сессий в режиме реального времени с заданной производительностью, внося минимальные или не внося вовсе задержки при анализе приложений проходящих по сети.

3. Открытость и соответствие стандартам – важный фактор при выборе DPI системы. Открытая, стандартизированная платформа обеспечивает независимость от запатентированного (proprietary) оборудования и протоколов [6].

Операторы и поставщики услуг сталкиваются с бесконечными проблемами соответствия требованиям абонента и появления новых трендов в условиях жесткой конкуренции. При этом, теперь недостаточно просто увеличивать производительность каналов и основывать тарифные планы на большей пропускной способности на абонента. Необходимо кардинально менять подход к ценообразованию, переходя на тарифные планы на основе предоставляемого контента. Выполнять дифференциацию сервисов и тем самым создавать добавочную стоимость услуг, пользуясь этой возможностью как источником увеличения доходов. Понимание и контроль, предоставляемый DPI-системой, дает возможность провайдерам связи персонализировать сервисы, в результате чего повышать степень удовлетворенности клиентов (QoE), уменьшать отток абонентов и повышать ARPU (Average revenue per user — средняя выручка на одного пользователя). Выбор DPI-систем должен быть основан на их открытости и соответствии отраслевым стандартам, проверенных возможностях и реальной производительности.

ЛИТЕРАТУРА

1. Бриткин А. NFV и пример ее применения для оператора связи // Журнал сетевых решений LAN. 2014. № 10. С. 42-44.
2. Гольдштейн Б.С., Маршак М.А., Мишин Е.Д., Соколов Н.А., Тум А.В. Показатели функционирования муль-тисервисной сети связи общего пользования // Техника связи. 2009. № 3-4. С. 26-31.
3. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. СПб: БХВ-Петербург, 2010. 400 с.
4. Елагин В.С., Онуфриенко А. В. Как оператору заработать на OTT-сервисах и при чем тут SDN? // T-comm: Телекоммуникации и транспорт. 2017. № 1. С. 17-21.
5. Елагин В.С., Онуфриенко А.В. Технология глубокой инспекции пакетов в программно-конфигурируемой сети // Труды учебных заведений связи. 2016. № 2. С. 59-63.
6. Зарубин А.А., Кызьюров О.Е., Савельева А.А. Цифровое качество программно-определяемых приложений инфокоммуникационных сетей. Формирование подходов к разработке моделей и методов его оценки // Информационные технологии и телекоммуникации. 2017. Т. 5. № 2. С. 56-61.
7. Щербакова Е.Н. Актуальные вопросы построения сети связи общего пользования в России // T-comm: Телекоммуникации и транспорт. 2017. № 11. 2017. С. 17-21.
8. Makolkina M., Koucheryavy A., Paramonov A. Investigation of traffic pattern for the augmented reality applications // Lecture notes in computer science. 2017. Pp. 233-246.
9. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical evaluation of D2D connectivity potential in 5G wireless systems // Lecture notes in computer science. 2016. Pp. 395-403.
10. Slattery T. QoS in an SDN. URL: http://www.nojit-ter.com/post/240168323/qos-in-an-sdn (дата обращения: 16.11.2017).

REFERENCES

1. Britkin A. NFV and an example of its application for a telecom operator // Journal of network solutions LAN. 2014. № 10. Pp. 42-44.

2. Goldstein B.S., Marshak M.A., Mishin E.D., Sokolov N.A., Tum A.V. Indicators of the functioning of a multiservice public communication network // Communication technology. 2009. № 3-4. Pp. 26-31.
3. Goldstein B.S., Sokolov N.A., Yanovskiy G.G. Communication networks. SPb: BHV-Petersburg, 2010. 400 p.
4. Elagin V.S., Onufrienko A.V. How can an operator make money on OTT services and what does SDN have to do with it? // T-comm: Telecommunications and Transport. 2017. № 1. Pp. 17-21.
5. Elagin V.S., Onufrienko A.V. Technology of deep packet inspection in a software-defined network // Proceedings of educational institutions of communication. 2016. № 2. Pp. 59-63.
6. Zarubin A.A., Kyzyurov O.E., Savelyeva A. A. Digital quality of software-defined applications of infocommunication networks. Formation of approaches to the development of models and methods of its assessment // Information technologies and telecommunications. 2017. Vol. 5. № 2. Pp. 56-61.
7. Shcherbakova E. N. Topical issues of building a public communication network in Russia // T-comm: Telecommunications and transport. 2017. № 11. 2017. Pp. 17-21.
8. Makolkina M., Koucheryavy A., Paramonov A. Investigation of traffic pattern for the augmented reality applications // Lecture notes in computer science. 2017. Pp. 233-246.
9. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical evaluation of D2D connectivity potential in 5G wireless systems // Lecture notes in computer science. 2016. Pp. 395-403.
10. Slattery T. QoS in an SDN. URL: http://www.nojit-ter.com/post/240168323/qos-in-an-sdn (accessed: 11.16.2017).