РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **36557**
(51) ***H04L 12/40*** (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

(21) 2023/0607.1
(22) 14.09.2023
(45) 19.01.2024, бюл. №3
(72) Стейн Яаков (IL)
(73) АЛЛОТ ЛТД. (IL)
(74) Мадиярова Алия Сериковна
(56) US2012263071 A1, 18.10.2012
RU2658181 C2, 19.06.2018
US2016205015 A1, 14.07.2016
CN114422249 A, 29.04.2022

(54) **УСТРОЙСТВО, СИСТЕМА И СПОСОБ УЛУЧШЕННОЙ ГЛУБОКОЙ ПРОВЕРКИ ПАКЕТОВ (DPI) И КЛАССИФИКАЦИИ ПОТОКОВ ТРАФИКА В КОММУНИКАЦИОННОЙ СЕТИ**

(57) Представлены системы, устройства и методы эффективного и инновационного комбинирования блоков глубокой проверки пакетов (DPI), имеющих большой объем приложений и быстрое время классификации, с блоками поведенческой классификации потоков (BFC), которые остаются функционирующими несмотря на полное шифрование. В варианте реализации объединена система DPI, имеющая систему BFC классификации категории приложения (ACC), с набором систем BFC детализированной глубокой проверки потоков (DFI), которые идентифицируют приложение с учетом известной категории приложения. Объединенная система извлекает выгоду из скорости, эффективности, точности и широкого охвата систем DPI для незашифрованных и частично зашифрованных случаев, при этом оставаясь функциональной для полностью зашифрованных случаев. Некоторые варианты реализации изобретения улучшают производительность и/или надежность, и/или безопасность, и/или устойчивость системы информационных технологий и/или коммуникационной сети. Настоящее изобретение может обеспечивать безопасное для окружающей среды и экономичное в части мощности решение для классификации и идентификации потоков трафика коммуникационной сети, а также может использовать меньше энергии или мощности, или ресурсов обработки, по сравнению с традиционными системами классификации.

(19) KZ (13) B (11) 36557

ОБЛАСТЬ ТЕХНИКИ

[0001] Настоящее изобретение в целом относится к классификации потоков трафика в коммуникационной сети и, в частности, к глубокой проверке пакетов (DPI) и поведенческой проверке потоков. Более конкретно, в вариантах реализации изобретения представлены устройства, системы и методы, которые классифицируют потоки трафика линии коммуникации, когда некоторые из этих потоков трафика полностью зашифрованы.

УРОВЕНЬ ТЕХНИКИ

[0002] Поток пакетов в сети пакетной передачи данных представляет собой набор связанных пакетов, обмен которых происходит между одними и теми же конечными точками, например, между клиентом и сервером в случае веб-служб или между двумя одноранговыми узлами в случае конференц-коммуникации. Классификация потока трафика линии коммуникации означает присвоение ему категории приложения (например, трансляция видео или видео-конференция) и/или идентификатора приложения (например, YouTube или Zoom), и/или типа устройства (например, смартфон или ПК).

[0003] Классификация обычно выполняется с помощью глубокой проверки пакетов или DPI. Блок DPI наблюдает за метаданными пакета по значению поля, например, адресами Интернет-протокола (IP), полями ответов системы доменных имен (DNS), номером протокола, портами протокола управления передачей (TCP), указанием имени сервера (SNI) и/или данными согласования протокола прикладного уровня (ALPN) из индивидуальных пакетов (или связанных с ними), содержащих поток, и сопоставляет эти метаданные по каждому пакету с опорными значениями, ожидаемыми для конкретных приложений. Системы DPI, известные из уровня техники, таким путем зачастую могут распознавать тысячи различных приложений из десятков категорий приложений, а также зачастую могут точно классифицировать потоки трафика после наблюдения за небольшим количеством пакетов.

[0004] Недавно возникла тенденция шифрования все большего количества значений поля по каждому пакету из соображений конфиденциальности. Хотя эта тенденция направлена на пресечение сквозного мониторинга, она препятствует функционированию DPI и/или может отрицательно сказываться на реализации вышеуказанных целей классификации потоков трафика.

[0005] Частичным решением, известным из уровня техники, является поведенческая классификация потоков, в которой используются технологии машинного обучения (ML) для распознавания характерных моделей поведения приложений и/или пользователей на основе характеристик по каждому потоку, например, значений внутрипакетного хронометрирования и последовательности размеров пакетов, что при этом не требует получения доступа к значениям поля по каждому пакету. Системы для поведенческой классификации пакетов, известные из уровня техники, таким путем иногда могут распознать несколько десятков различных приложений из небольшого количества категорий приложений, а также точно классифицировать потоки трафика после наблюдения за относительно малым количеством пакетов. Методы с машинным обучением также требуют все больших вычислительных ресурсов и потребляют больше энергии по сравнению с методами DPI.

[0006] Ввиду этих причин, существующие технологии классификации потоков могут лишь частично заменить системы DPI для ограниченных сценариев использования и не могут рассматриваться как полная замена DPI для всех целей классификации потоков трафика.

РАСКРЫТИЕ СУЩНОСТИ ИЗОБРЕТЕНИЯ

[0007] В настоящем изобретении представлены системы и методы комбинирования систем глубокой проверки пакетов (DPI), имеющих большой объем приложений и быстрое время классификации, с системами поведенческой классификации потоков (BFC), которые остаются функционирующими несмотря на полное шифрование.

[0008] Варианты реализации настоящего изобретения относятся к комбинированным системам, содержащим подсистемы DPI и BFC, которые быстро и точно классифицируют потоки трафика линии коммуникации, когда большинство потоков (но не все) полностью зашифрованы. Такие ситуации будут преобладать в период от исходного включения полного шифрования и до обновления последних приложений и служб.

[0009] В варианте реализации настоящего изобретения представлены подсистема DPI и подсистема BFC, которые предпринимают попытку идентифицировать приложение потока трафика, а также могут вернуть связанную с ним категорию приложения. В этом варианте реализации комбинированная система сперва предпринимает попытку идентификации приложения потока трафика посредством DPI и, в случае успеха, комбинированная система возвращает детализированную классификацию приложения и, при необходимости, связанную с ним категорию приложения. Если DPI не прошла успешно ввиду шифрования необходимых значений поля по каждому пакету, то далее предпринимается попытка BFC. Если идентификация приложения посредством BFC прошла успешно, то комбинированная система возвращает классификацию BFC на приложение и, при необходимости, связанную с ним категорию приложения.

[00010] В другом варианте реализации настоящего изобретения представлены подсистемы DPI, классификации адресов серверов (SAC) и BFC. В этом варианте реализации комбинированная система сперва предпринимает попытку идентификации приложения потока трафика посредством DPI и, в случае успеха, комбинированная система возвращает детализированную классификацию приложения и, при необходимости, связанную с ним категорию приложения. Если DPI не имела успеха, то предпринимается попытка SAC. Если SAC имела успех, то комбинированная система возвращает классификацию SAC. Если SAC не имела успеха, то предпринимается попытка BFC. Если идентификация приложения посредством BFC имела успех, то комбинированная система возвращает классификацию BFC.

[00011] В предпочтительном варианте реализации настоящего изобретения представлена подсистема (или блок, или компонент), которая предпринимает попытку идентификации приложения потока трафика и также может возвращать связанную с ним категорию приложения, систему BFC классификации категории приложения (ACC), которая предпринимает попытку классификации потоков трафика на категории приложения, и набор подсистем BFC глубокой проверки потоков (DFI), которые предпринимают попытку идентификации конкретных приложений с учетом известной категории приложения. В этом варианте реализации комбинированная система сперва предпринимает попытку идентификации приложения потока трафика посредством DPI и, в случае успеха, комбинированная система возвращает классификацию DPI на приложение и, при необходимости, связанную с ним категорию приложения. Если DPI не прошла успешно ввиду шифрования необходимых значений поля по каждому пакету, то далее предпринимается попытка классификации категории приложения. Если ACC

не прошла успешно, то комбинированная система принимает аннулирование и, при необходимости, сохраняет характеристики для дальнейшего улучшения. Если ACC прошла успешно, то предпринимается попытка детализированной классификации приложения путем применения соответствующей системы глубокой проверки потока из набора систем DFI. Если DFI прошла успешно, то комбинированная система возвращает классификацию системы DFI, которая была применена. Если DFI не прошла успешно, то комбинированная система возвращает категорию приложения, определенную путем ACC.

[00012] Данное раскрытие было представлено исключительно в целях краткого описания замыслов, которые будут более полно описаны ниже в разделе «Подробное описание». Оно не предназначено для ограничения объема заявленного изобретения.

КРАТКОЕ ОПИСАНИЕ ФИГУР

[00013] На Фигуре 1 изображены различные сценарии использования классификации потоков пакетов.

[00014] На Фигуре 2 изображена высокоуровневая структура традиционной системы DPI.

[00015] На Фигуре 3 изображена высокоуровневая структура системы поведенческой классификации потоков (BFC).

[00016] На Фигуре 4 изображена комбинированная система, содержащая подсистему DPI и подсистему BFC.

[00017] На Фигуре 5 изображена комбинированная система, содержащая подсистему DPI, которая дополнительно определяет то, являются ли открытыми адреса слоя 3, подсистему SAC и подсистему BFC.

[00018] На Фигуре 6 изображена комбинированная система, содержащая подсистему DPI, подсистему SAC и подсистему BFC.

[00019] На Фигуре 7 изображена комбинированная система, содержащая подсистему DPI, подсистему ACC и пример набора подсистем DFI.

ПОДРОБНОЕ ОПИСАНИЕ

[00020] В современных коммуникационных сетях, таких как Интернет, обмен информацией происходит дискретными единицами, известными как пакеты, а последовательность связанных пакетов, которыми обмениваются одни и те же стороны, известна как поток пакетов. Например, голосовой вызов, осуществляемый по Интернет-

протоколу (VoIP), содержит двунаправленный поток пакетов, при этом каждый отдельный пакет содержит некоторый временной интервал закодированного аудио от одной стороны.

[00021] В стеке Интернет-протоколов (IP) пакеты создаются так, чтобы быть *самоописываемыми*, при этом они содержат последовательность *заголовков* пакетов перед пользовательским *контентом* (например, закодированным аудио). Эта структура упрощает рекурсивный парсинг на основе стандартов целевым получателем, однако имеет непредусмотренные последствия получения всей информации пакета потенциально злоумышленными сторонами, которые могут наблюдать за пакетом на его пути от источника к месту назначения. Данная ситуация была исправлена путем добавления различных криптографических механизмов, при этом часто заявляется, что подавляющее большинство Интернет-трафика зашифровано.

[00022] Однако утверждение касательно повсеместности шифрования на самом деле говорит о том, что зашифрован лишь пользовательский контент, тогда как из заголовков Интернет-пакетов по-прежнему происходит утечка метаданных (данных о данных). Эти метаданные стандартно используются провайдерами Интернет-услуг (ISP) для идентификации используемого приложения, при этом данная идентификация является ключевой для различных целей, в том числе для дифференциального взимания платы, управления трафиком, оценки качества услуг, аналитики, негласного контроля, перехвата и снятия информации, передающейся по коммуникационным сетям, цифрового правоприменения и обеспечения безопасности коммуникации.

[00023] Дифференциальное взимание платы – это взимание платы с потребителя за полученные услуги; например, некоторые услуги могут быть бесплатными, еще одни могут предоставляться по заниженной цене вплоть до порога использования, а другие могут представлять собой премиум-услуги, влекущие за собой дополнительную плату. Оценка качества услуг – это назначение приоритетов доставки пакетов в соответствие с требованиями каждого приложения, например, интерактивных приложений, таких как приложения для видео-конференций и игровые приложения, которые требуют минимального времени ожидания, но могут потреблять данные со скоростью от низкой до средней, тогда как потоковая трансляция видео требует высокой скорости передачи данных, но является относительно нечувствительной к времени ожидания. Управление трафиком – это поддержание рабочей мощности несмотря на перегрузку или условия отказа, что обычно влечет за собой придание первостепенного приоритета критическому трафику по сравнению с фоновым трафиком. Аналитика – это подготовка отчетов по

использованным приложениям и их качеству услуг для целей планирования и поддержки клиентов. Негласный контроль, перехват и снятие информации, передающейся по коммуникационным сетям, – это выявление и сбор специфического трафика согласно требованиям правоохранительных органов, например, когда по распоряжению суда необходимо фиксировать голосовой трафик от конкретного подозреваемого. Цифровое правоприменение – это другие юридические или отечественные меры безопасности, например, блокировка детской порнографии или видеоролики о создании бомб, или выслеживание террористических ячеек. Безопасность – это защита потребителей от потенциально опасного трафика, например, вредоносного программного обеспечения, и защита серверов от атак типа «отказ в обслуживании» (DoS) или от распределенных атак типа «отказ в обслуживании» (D-DoS).

[00024] Сценарии использования, представленные в предыдущем абзаце, не охватывают весь спектр целей использования DPI. Другие варианты применения включают в себя гео-спуфинг виртуальных частных сетей (VPN) для осуществления управления цифровыми правами (DRM), анализа первопричин на выявление деградаций и сбоев сети, получения статистических данных для оценки производительности и качества по требованием регуляторных органов, выявления перегрузки и ослабления, и многого другого. Кроме того, системы DPI зачастую вызывают для выполнения дополнительных функций, таких как идентификация типа устройства или количества подключенных устройств. Например, провайдер услуг может предлагать план мобильных услуг и более дорогостоящий план фиксированного беспроводного доступа (FWA). План мобильных услуг может накладывать ограничивать пользователя использованием максимум трех связанных устройств одновременно, тогда как план FWA позволяет одновременно подключать неограниченное количество устройств. Также могут быть предусмотрены специальные планы услуг для умного дома, разработанные для обслуживания многочисленных устройств по концепции «Интернет вещей» (IoT), тогда как другие планы могут блокировать или ограничивать такие устройства.

[00025] На Фигуре 1 изображено несколько сценариев использования DPI. Потоки пакетов во входящем направлении (от Интернета к локальным хостам) и исходящем направлении (от локальных хостов к Интернету) подвергаются наблюдению со стороны системы DPI, которая может работать в линейном режиме или работать в режиме TAP. Линейный режим означает, что DPI вводит пакеты, обрабатывает их и затем передает их. Режим TAP означает, что система DPI принимает копию пакетов, но не отвечает за

их передачу. Результаты DPI отправляются в виде записей о потоке на механизм составления отчетов или на другие функционалы, согласно требованиям сценария использования. Когда сценарием использования является аналитика или дифференциальное взимание платы, то достаточно режима TAP, а механизм составления отчетов либо вычисляет различные статистические данные, согласно требованиям провайдера услуг или регуляторных норм, либо обновляет функцию взимания платы в отношении используемого приложения. Когда сценарием использования является безопасность или управление трафиком, то линейный компонент, который может быть встроен или не встроен в DPI, блокирует трафик или накладывает на него ограничение скорости, согласно классификации DPI.

[00026] Идентификация потоков пакетов как относящихся к специфическим приложениям или услугам обычно выполняется посредством DPI (глубокой проверки пакетов). Системы DPI являются высокотехнологичными классификаторами, которые используют вышеуказанную утечку метаданных в своих целях. DPI содержит аккуратно составленные наборы правил, которые сопоставляют логические комбинации метаданных с приложениями. Во время работы, DPI связывает пакеты с потоками пакетов и подвергает синтаксическому анализу каждый отдельный пакет, использующий самоописывающий характер незашифрованных пакетов, соответствующий стеку IP-протоколов. Синтаксический анализ обеспечивает возможность извлечения незашифрованных метаданных по каждому пакету. Затем система DPI сравнивает все метаданные, собранные из пакетов, относящихся к потоку пакетов, с подписями приложений, хранящимися в наборе правил подписи приложения, пока не будет выявлено соответствие. Системы DPI, известные из уровня техники, таким путем могут распознавать тысячи различных приложений из десятков категорий приложений, а также точно классифицировать потоки трафика после наблюдения за очень малым количеством пакетов. В US 8,902,776 под названием «*Распределитель матрицы DPI*» авторства Keynan et al описано использование DPI для управления трафиком.

[00027] На Фигуре 2 изображена высокоуровневая структура традиционной системы DPI. Потоки пакетов во входящем и исходящем направлении подвергаются наблюдению со стороны системы DPI, которая может работать в линейном режиме или работать в режиме TAP. Система содержит инструмент извлечения полей по каждому пакету, которое подвергает синтаксическому анализу оба общеизвестных поля, как указано организациями стандартизации (например, IP-адреса, IP-протокол, номера

портов TCP и протокола пользовательских диаграмм (UDP), опции TCP, поля защиты транспортного уровня (TLS), такие как SNI и ALPN, поля http, такие как метод запроса и пользовательский агент), и специфические для приложения поля, которые необходимо исследовать посредством протокольного анализа и/или обратной разработки. Инструмент извлечения полей по каждому пакету должно работать в режиме реального времени, в среднем завершая синтаксический анализ пакета перед получением следующего пакета. Для одной линии 100 Гбит/с это означает выполнение синтаксического анализа приблизительно 150 миллионов пакетов в секунду (предполагая, что пакеты имеют минимальный размер) или приблизительно 6,7 наносекунд на каждый пакет.

[00028] Система DPI дополнительно содержит алгоритм сопоставления подписи приложения. Этот алгоритм получает доступ к набору правил приложения, который содержит подписи приложения, то есть логические комбинации полей по каждому пакету для пакетов в потоке, которые характерны для потоков, поступающих от конкретного приложения или услуги. Сравнивая извлеченные поля по каждому пакету с набором правил приложения, может быть найдено соответствие. Метка приложения правила сопоставления выдается в виде записи о потоке. Если соответствие не найдено, то возвращается указание о сбое. При необходимости, категория приложения, соответствующая идентифицированному приложению, может быть возвращена в виде части записи о потоке.

[00029] В качестве простейшего примера, конкретное приложение может характеризоваться наличием всех пакетов, где в поле протокола указан TCP, и наличием пакетов от клиента к серверу с использованием TCP-порта назначения 443, указывающего HTTP по TLS, и наличием конкретного значения поля SNI в пакете TLS Client Hello.

[00030] Выше было указано, что подавляющее большинство Интернет-трафика зашифровано. Например, в настоящее время более 80% всех веб-пакетов используют HTTPS (протокол защищенной передачи гипертекста), который использует TLS (защиту транспортного уровня), т.е. криптографический протокол, обеспечивающий аутентификацию, целостность данных и конфиденциальность. Однако в текущей практике DNS (система доменных имен) отправляет запросы и ответы, которые сопоставляют имя сервера с его IP-адресом; пакет TLS Client Hello, которые включает такие метаданные, в виде SNI (указание имени сервера) и ALPN (согласование протокола прикладного уровня); номера и опции TCP-порта, а также различные другие

поля заголовка отправляются все еще в незашифрованном виде. За этими полями наблюдают системы DPI, а их появление отдельно или в комбинации может использоваться для составления заключения об используемом приложении или услуге, типе пользовательского устройства и качестве полученной услуги.

[00031] Недавние тенденции в сторону повышения конфиденциальности пользователей в Интернете, в частности, относительно повсеместного мониторинга государственными органами, привели к постепенно увеличивающемуся шифрованию заголовков пакетов помимо пользовательского контента. Например, конечный пользователь, желающий скрыть опции TCP, может использовать более новый протокол QUIC. Если необходимо цензурировать метаданные TLS, например, SNI, можно использовать расширение Encrypted Client Hello (ECH). А если необходимо скрыть практически все метаданные, то можно использовать технологию виртуальной частной сети, в которой все заголовки пакетов скрыты и весь зашифрованный пакет размещается за внешним заголовком, который не несет релевантные для приложения метаданные.

[00032] Скрытие метаданнных – это эффективное средство при борьбе с повсеместным мониторингом и предоставлением конфиденциальной информации злоумышленникам, но сопутствующим ущербом является то, что работа систем DPI становится более сложной или даже невозможной. Это напрямую влияет на ключевые функции, для которых изначально была реализована DPI, в том числе на дифференциальное взимание платы, управление трафиком, оценку качества услуг, аналитику и безопасность коммуникации.

[00033] Однако даже шифрование всех полей заголовка пакета в действительности не удалит все отличительные метаданные. Остается по меньшей мере три характеристики. Во-первых, последовательность направлений пакетов, содержащих поток пакетов (например, от клиента к серверу или от сервера к клиенту), может указывать на тип услуги. Например, потоковая трансляция видео характеризуется небольшим количеством пакетов *запроса* (GET) от клиента к серверу, после которого следует большое количество пакетов ответов (блочных) от сервера назад к клиенту; видеозвонки в общем являются симметричными с приблизительно одинаковыми количествами пакетов в каждом направлении. Во-вторых, размер пакетов в целом сохраняется посредством технологий скрытия метаданных или, в лучшем случае, модифицируется путем добавления дополнительного(-ых) заголовка(-ов). Таким образом, даже полностью зашифрованный поток пакетов может характеризоваться демаскирующей последовательностью размеров пакетов. Например, потоковая

трансляция видео будет состоять из большого количества очень больших пакетов ответа или блочных пакетов от сервера к клиенту с вкраплениями небольших (ACK) пакетов от клиента к серверу, подтверждающих их получение. В-третьих, значения хронометрирования пакетов в целом незначительно искажаются маскировкой метаданных, хотя на них влияет свойственные в сети задержки. Связывание этих трех характеристик по каждому пакету образует временной ряд, представляющий зашифрованный поток пакетов, где каждый элемент временного ряда содержит временную метку, направление и размер пакета.

[00034] Классификация используемого приложения или услуги, обеспечиваемая исключительно на основе вышеуказанного временного ряда, называется поведенческой классификацией потока (BFC). Поведенческие классификаторы потока в целом используют технологии машинного обучения для распознавания характерных моделей поведения приложений и/или пользователей исключительно на основе временного ряда потока без необходимости в получении доступа к значениям поля заголовка по каждому пакету. Для решения данной проблемы применялось много различных технологий машинного обучения, в том числе деревья решений, наивные классификаторы Байеса, методы случайного леса (RF), Adaboost и XGboost, скрытые модели Маркова (HMM), машины опорных векторов (SVM), сверточные нейронные сети (CNN), рекуррентные нейронные сети, такие как GRU и LSTM, глубокое обучение, трансформеры и многие-многие другие. Системы BFC, известные из уровня техники, таким путем могут распознать десятки различных приложений из небольшого количества категорий приложений, а также точно классифицировать потоки трафика после наблюдения за относительно малым количеством пакетов. Методы с машинным обучением также требуют все больших вычислительных ресурсов и потребляют больше энергии по сравнению с методами DPI. Наконец, методы машинного обучения могут неправильно классифицировать (т.е. классифицировать поток, относящийся к одному приложению, как поток, который относится к другому приложению) и делать это с высоким уровнем достоверности.

[00035] На Фигуре 3 изображена высокоуровневая структура системы поведенческой классификации потоков (BFC). Потоки пакетов во входящем и исходящем направлении подвергаются наблюдению со стороны системы BFC, которая может работать в линейном режиме или работать в режиме TAP. Система содержит инструмент наблюдения за пакетами по каждому потоку, который наблюдает за каждым пакетом, связанным с потоком, и извлекает модель поведения по каждому пакету, в том

числе его направление (входящее или исходящее), время его прибытия (предпочтительно, по сравнению с первым пакетом в потоке) и его размер (в байтах). Возможно объединить данные о направлении и размере пакета путем умножения размеров исходящих пакетов на -1, тем самым создавая одну последовательность с положительными размерами пакетов для входящих пакетов и отрицательными размерами пакетов для исходящих пакетов. Эта последовательность вместе с временем прибытия каждого пакета определяет временной ряд.

[00036] Система BFC дополнительно содержит машину вывода на машинном обучении. Эта машина вывода в целом является предварительно обученной с помощью обучающей выборки, содержащей временной ряд, исходящий из набора многих приложений, вместе с метками, представляющими каждое соответствующее приложение. Во время прогона машина вывода вводит временной ряд и получает вектор, представляющий вероятность того, что поток принадлежит к каждому приложению в наборе из многих приложений в обучающих данных. Наиболее вероятная метка приложения возвращается в виде *записи о потоке*. Если предсказанная метка приложения не отвечает заранее определенным критериям правильности, то возвращается указание о сбое.

[00037] Сравнение DPI с BFC демонстрирует преимущества и недостатки каждого из этих подходов. Недостатком DPI является маскировка заголовков пакетов, тогда как BFC требует лишь данные временного ряда. Системы DPI могут распознавать тысячи различных приложений и услуг, тогда как несколько современных систем BFC приближаются к сотне. Системы DPI обычно выполняют классификацию в пределах небольшого количества пакетов, тогда как системы BFC могут требовать десятки пакетов или десятки секунд трафика.

[00038] Для некоторых сценариев использования критически важной является скорость классификации. Например, при том, что аналитика может требовать только сбора данных за 15-минутные периоды и генерирования отчетов один раз в день, блокирование вредоносного программного обеспечения или блокирование просмотра незаконных видео должна быть почти мгновенной для того, чтобы она была эффективной. Для некоторых сценариев использования критически важной является минимизация потребления вычислительного ресурса. Например, количество ядер центрального процессора (CPU) и объем памяти ограничены для SMB или филиалов предприятия, подключенных к каналам 1 Гбит/с или 10 Гбит/с, но крупному провайдеру услуг, обслуживающему большой город, может понадобиться классифицировать

потоки, получаемые со скоростью больше 1 Тбит/с, что приводит к необходимости установки центра хранения и обработки данных соответствующего размера. В некоторых сценариях использования (например, управлении трафиком) требуется лишь классификация на небольшое количество широких категорий приложения, тогда как в других (например, при дифференциальном взимании платы, цифровом правоприменении) требуется детализированная классификация тысяч приложений. Наконец, сбои системы DPI почти всегда являются проблемами покрытия, т.е. неизвестности рассматриваемого приложения. Неправильная классификация происходит между связанными приложениями (например, когда услуга, предоставляемая заданным провайдером, вступает в конфликт с другой услугой от того же провайдера ввиду общей инфраструктуры). Как было указано выше, при BFC может произойти масштабный сбой, который приведет к конфликту абсолютно несвязанных друг с другом приложений.

[00039] Это сравнение подчеркивает причины того, что существующие технологии BFC могут заменить системы DPI лишь для ограниченных сценариев использования и не могут рассматриваться как полная замена DPI для всех целей классификации потоков трафика.

[00040] Однако не предполагается, что все пользователи, приложения и услуги будут использовать наиболее объемные формы скрытия метаданных немедленно после их стандартизации. В действительности, типичные кривые внедрения нового протокола имеют изначальный низкий период внедрения, где только небольшой процент пользователей будут пытаться его использовать, после которого следует период быстрого роста за счет крупных участников, внедряющих протокол, после которого следует длительный период, в ходе которого существующие системы в конечном итоге переходят на новый протокол.

[00041] Например, в течение многих лет были доступны технологии VPN, однако кроме дистанционных работников и торгового персонала в командировках, лишь некоторые люди знали о ней до возникновения тенденции работы на дому, которая была вызвана вспышкой COVID, что превратило их в рабочие VPN. По этой причине, использование выросло с нескольких процентов до более, чем 30 процентов. С тех пор было незначительное увеличение, хотя технология iCloud Private Relay от Apple может привести к еще одному резкому увеличению в некоторый момент времени.

[00042] В качестве еще одного примера, процент использования QUIC также был низким в течение долгого времени до принятия решения несколькими основными

участниками о том, чтобы сделать его протоколом по умолчанию, что увеличило процент его использования приблизительно до 30. С тех пор увеличение использования остановилось, оставив после себя большое количество неприспособившихся пользователей, которые не усматривают никаких преимуществ в дорогостоящих обновлениях. Ожидается, что TCP по-прежнему будет использоваться для передачи значительной части трафика в течение следующих лет, если не десятилетий.

[00043] Еще одним примером является зашифрованный DNS, где DNS поверх TLS (DoT), DNS поверх HTTPS (DoH) и наиболее новый DNS поверх QUIC (DoQ) вместе составляют менее 5% DNS-трафика от конечных пользователей до первых определителей. Наконец, ECH, который, как ожидается, будет использоваться как предлагаемый стандарт в начале 2024 года, пока что лишь осторожно пробуют использовать «пионеры» в данной области техники, однако нет оснований ожидать значительный рост его использования в течение некоторого времени.

[00044] Ввиду этих причин предполагается, что большинство популярных услуг и пользовательских приложений будут оперативно использовать полное скрытие метаданных, тогда как широкий ряд более мелких и менее популярных услуг и приложений на многие годы останется на текущей фазе с зашифрованным пользовательским контентом, но только лишь частично скрытыми метаданными. Несмотря на то, что может быть до десяти очень популярных приложений, они могут требовать большинства Интернет-объема, тогда как каждое из тысячи менее популярных приложений занимает очень малое количество трафика.

[00045] За период времени, в течение которого полное скрытие метаданных используется не полностью, может быть преимуществом комбинация глубокой проверки пакетов и поведенческой классификации потоков для извлечения выгоды из обоих этих подходов. DPI может быстро и точно классифицировать потоки пакетов, содержащие по меньшей мере некоторые нескрытые метаданные, тогда как BFC будет брать на себя полностью скрытые потоки. При этом освобождение BFC от необходимости брать на себя популярные приложения, которые требуют большинства объема, минимизирует потребление вычислительного ресурса BFC.

[00046] В некоторый момент, в более отдаленном будущем подавляющее большинство трафика будет полностью зашифровано, а зона охвата DPI более не будет гарантировать его сохранение. К этому времени BFC станет более обогащенной в части зоны охвата и более точной, так что она будет иметь все возможности для удовлетворения функций, которые сегодня выполняет DPI. Более того, к этому времени

могут быть разработаны альтернативные механизмы, такие как прямая коммуникация между приложениями и сетевыми элементами.

[00047] В первом варианте реализации описанного изобретения, изображенного на Фигуре 4, поток пакетов сначала проверяется традиционной системой DPI, выступающей в роли подсистемы DPI в комбинированной системе. Если пакет не полностью зашифрован, то есть достаточное количество распознаваемых метаданных является видимым для подсистемы DPI, то комбинированная система вернет запись о потоке, содержащую классификацию DPI. В случае неуспеха, вместо отправки указания о сбое, поток пакетов затем проверяется подсистемой BFC. Если машина вывода в подсистеме BFC успешно идентифицировала приложение, то возвращается запись о потоке, содержащая классификацию BFC. Если BFC не имела успеха, то возвращается указание о сбое.

[00048] В другом варианте реализации описанного изобретения, изображенного на Фигуре 5, поток пакетов сначала еще раз проверяется традиционной системой DPI, выступающей в роли подсистемы DPI в комбинированной системе. Если достаточное количество распознаваемых метаданных является видимым для этой системы DPI, то комбинированная система вернет запись о потоке, содержащую классификацию DPI. В случае неуспеха, подсистема DPI дополнительно определяет то, остается ли видимым адрес слоя 3 исходного сервера (IP-адрес пункта назначения для исходящих пакетов) или же он скрыт. Например, ECH шифрует только слой 4 и выше, оставляя видимыми заголовки слоя 3, тогда как VPN скрывают также и заголовок слоя 3. Если IP-адрес сервера скрыт, то выполняется вызов подсистемы BFC, как в первом варианте реализации. Если IP-адрес сервера остается видимым, то выполняется вызов подсистемы классификатора адреса сервера (SAC). SAC предпринимает попытку ассоциации приложения с адресом сервера. В случае успеха, комбинированная система возвращает запись о потоке, содержащую классификацию SAC; в случае неуспеха, возвращается указание о сбое.

[00049] Ассоциация приложения с адресом сервера может выполняться пассивно или активно. Пассивная SAC может предпринимать попытку выполнения поиска обратного IP-адреса на адресе сервера для получения унифицированного указателя ресурса (URL) сервера, т.е. веб-адреса, который в большинстве случае уникальным образом сопоставляется с приложением или услугой. Альтернативно, пассивная SAC может наблюдать в фоновом режиме за всеми DNS-ответами и сохранять URL сервера для каждого наблюдаемого IP-адреса сервера; во время работы выполняется поиск для

сопоставления IP-адреса сервера с URL, а URL ассоциируется с приложением. Даже если клиент текущего потока использовал зашифрованную DNS для поиска IP-адреса сервера, для того, чтобы эта схема была успешной, определенному клиенту достаточно выполнить поиск этого же адреса сервера с использованием незашифрованной DNS. Активная SAC может периодически выполнять DNS-запросы популярных URL и создавать подобную справочную таблицу.

[00050] В альтернативном варианте реализации раскрытого изобретения, изображенного на Фигуре 6, поток пакетов сначала еще раз проверяется традиционной системой DPI, выступающей в роли подсистемы DPI в комбинированной системе. Если достаточное количество распознаваемых метаданных является видимым для этой системы DPI, то комбинированная система вернет запись о потоке, содержащую классификацию DPI. В случае успеха, выполняется немедленный вызов SAC для попытки ассоциации приложения с адресом сервера. В случае успеха, возвращается запись о потоке, а в случае неуспеха, выполняется вызов подсистемы BFC. В случае успеха, комбинированная система возвращает запись о потоке, содержащую классификацию подсистемы BFC. В случае неуспеха, возвращается указание о сбое.

[00051] В предпочтительном варианте реализации описанного изобретения, изображенного на Фигуре 7, поток пакетов сначала еще раз проверяется традиционной системой DPI, выступающей в роли подсистемы DPI в комбинированной системе. Если достаточное количество распознаваемых метаданных является видимым для этой системы DPI, то комбинированная система вернет запись о потоке, содержащую классификацию DPI. В случае неуспеха, выполняется вызов классификатора категории приложения (ACC), который использует машину вызова на машинном обучении для предсказания категории приложения из небольшого количества широких категорий приложений, таких как «видео-конференция», «трансляция потокового видео» (т.е. видео по запросу), голос через IP (VoIP), игровые приложения, «социальные сети», «передача файлов», покупки или «обычный просмотр страниц». В целом, достаточно небольшого количества категорий приложений.

[00052] Для многих сценариев использования классификации потока может быть необходима только категория приложения. Например, для управления перегрузкой может быть предусмотрена политика, заключающаяся в том, что во время интенсивного использования ресурса коммуникации скорость передачи файлов должна быть ограничена (тем самым снижая ее, но с поддержанием работы), тогда как VoIP и коммуникации по видео-конференции не должны ограничиваться. Подобным образом,

может быть ограничена скорость потоковой трансляции видео, приводя к некоторому снижению качества, но с поддержанием работы.

[00053] Если ACC не имела успеха в определении широкой категории приложения, то возвращается указание о сбое. В случае успеха, комбинированная система затем предпринимает попытку определения детализированной классификации приложения. Для этой цели выполняется вызов BFC глубокой проверки пакетов (DPI) из набора DFI.

[00054] Поскольку ACC имела успех, комбинированная система знает о широкой категории приложения и может вызвать DFI, специфическую для выявленной категории приложения. DFI, являющаяся специфической для конкретной категории приложения, может быть меньшей и более точной, чем BFC, которые требуют одновременно отличать друг от друга многие приложения, относящиеся к разным категориям.

[00055] В этом варианте реализации будет несколько DFI по меньшей мере для некоторых из категорий приложений. Например, DFI-VC для коммуникации по видео-конференции, которая была обучена отличать между собой различные общие приложения для коммуникации по видео-конференции. Подобным образом, DFI-VoD для видео по запросу, которая была обучена отличать между собой различные общие приложения для потоковой трансляции видео. Подобным образом, DFI-игры для игровых служб, которая была обучена отличать между собой различные общие онлайн-игры.

[00056] Для соотнесения обычного просмотра страниц с конкретными вебсайтами может быть реализована технология создания отпечатков вебсайтов, некоторые примеры которой уже известны из уровня техники. В некоторых случаях может подойти технология, описанная в US 11,52,867 под названием «СИСТЕМА, УСТРОЙСТВО И МЕТОД КЛАССИФИКАЦИИ ЗАШИФРОВАННЫХ КОММУНИКАЦИОННЫХ СЕТЕЙ» авторства Vega et al.

[00057] Если вызов DFI был успешным, то комбинированная система возвращает запись о потоке, содержащую детализированное приложение, как было выявлено вызванной DFI, и, необязательно, категорию приложения, которая была определена посредством ACC. Если DFI не прошла успешно, то комбинированная система возвращает только категорию приложения, определенную путем ACC.

[00058] Некоторые варианты реализации могут быть осуществлены путем использования одного или более компонентов аппаратного обеспечения и/или компонентов программного обеспечения; путем использования, например: аппаратного

процессора, выполненного с возможностью исполнения кода и обработки данных; блока памяти (например, оперативного запоминающего устройства (ОЗУ), флэш-памяти, энергозависимой памяти), выполненного с возможностью хранения кода и/или данных; хранилища (например, энергонезависимого хранилища, жесткого диска, твердотельного накопителя); одного или более блоков ввода (например, клавиатуры, мыши, кнопочной панели, микрофона); одного или более блоков вывода (например, экрана, монитора, звуковых динамиков); одного или более блоков беспроводной и/или проводной коммуникации (например, приемопередатчика, передатчика, приемника, передатчика-приемника, модема, маршрутизатора, сетевого коммутатора, концентратора, другого сетевого элемента); источника питания (сетевого электричества, аккумулятора, перезаряжаемого аккумулятора, солнечной панели или источника с солнечной панелью, источника питания на возобновляемой энергии); операционной системы (ОС) с драйверами и приложениями или «app»; и/или других блоков или модулей.

[00059] В частности, в некоторых вариантах реализации могут быть предусмотрены устройства, система и методы для обеспечения информационных технологий и коммуникации (например, коммуникации между компьютерами, коммуникации по сети Интернет, коммуникации по сети сотовой связи), и/или для улучшения потока пакетов и/или данных по системе связи; и/или для улучшения качества услуг (QoS) и/или качества восприятия (QoE) таких систем информационных технологий и/или систем связи; и/или для улучшения надежности и/или устойчивости таких систем информационных технологий и/или систем связи. Например, некоторые варианты реализации могут помогать сетевому провайдеру или оператору телекоммуникационных услуг корректно выявлять то, что конкретный поток трафика является потоковым видео в реальном времени с видео-конференции в реальном времени, что, в свою очередь, может вызвать увеличение ширины полосы и/или вычислительных ресурсов, которые выделены для такого приложения или потока; в то же время, в отличие от этого, некоторые варианты реализации могут корректно выявлять то, что другой конкретный поток трафика представляет собой загруженный крупный файл данных не в реальном времени, которому, таким образом, может быть назначен более низкий приоритет по сравнению с видеопотоком трансляции в реальном времени, и которому, таким образом, может быть выделена меньшая ширина полосы или меньшее количество вычислительных ресурсов. В дополнение или в качестве альтернативы, правильная, точная и эффективная классификация потока трафика или потоков пакетов, благодаря некоторым вариантам реализации настоящего изобретения, может

дополнительно улучшать безопасность и/или надежность и/или устойчивость коммуникационных сетей, а также связанных систем информационных технологий и сервера; например, за счет того, что эти сети и система могут определять, что конкретная трансляция или поток трафика является правомерным (например, трансляция видео через приложение для трансляции видео-конференций в реальном времени) и, таким образом, должны обслуживаться или ретранслироваться; или наоборот, для выборочного определения или оценки того, что конкретный поток трафика возможно является частью атаки или кибератаки (например, частью распределенной атаки типа «отказ в обслуживании» (D-DoS)), или другим типом неправомерного потока трафика, который должен быть заблокирован или помещен в карантин, или отброшен, или обработан иным образом; таким образом, повышается общая надежность и/или безопасность и/или устойчивость релевантной(-ых) сети(-ей) коммуникации и их инфраструктуры информационных технологий (например, сервера, маршрутизатора, релейного блока, сетевого элемента).

[00060] Некоторые варианты реализации могут быть специально реализованы в виде «зеленых» или безопасных для окружающей среды систем, и/или они могут активно снижать потребление электроэнергии и/или потребление энергии, которую требует обычная/традиционная система для достижения подобных целей. Например, обычная система может предпринимать попытку использования системы на машинном обучении (ML), что требует больших вычислительных усилий и/или высокой вычислительной мощности, и/или большого времени обработки, и, таким образом, потребляет большое количество энергии при попытке классификации конкретного потока пакетов; тогда как некоторые варианты реализации настоящего изобретения могут достигать цели правильной классификации потока трафика путем использования меньшего количества энергии и/или мощности, и/или вычислительных ресурсов, и/или ресурсов обработки, тем самым обеспечивая безопасное для окружающей среды и экономичное решение по сравнению с обычными системами, а также обеспечивая возможность экономии энергии и мощности, потребляемой сетями и устройствами коммуникации.

[00061] В некоторых вариантах реализации представлена система для классификации потоков пакетов в коммуникационной сети, содержащая: подсистему (или блок) глубокой проверки пакетов (DPI); по меньшей мере одну подсистему (или блок) поведенческой классификации потока (BFC); причем указанная подсистема DPI сперва предпринимает попытку классификации потока пакетов посредством анализа

DPI, и в случае успеха, указанная по меньшей мере одна подсистема BFC предпринимает попытку классификации указанного потока пакетов посредством анализа BFC.

[00062] В некоторых вариантах реализации система дополнительно содержит: классификатор адреса сервера (SAC), который вызывается в случае, если подсистема DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI; причем вызов подсистемы BFC выполняется только в случае, если подсистема DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI.

[00063] В некоторых вариантах реализации в случае, если подсистема DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI, то дополнительно выполняется генерирование сигнала, указывающего на то, являются ли видимыми адреса Интернет-протокола (IP), ассоциированные с указанным потоком пакетов, или нет; причем если указанный сигнал указывает на то, что IP-адреса, ассоциированные с указанным потоком пакетов, являются видимыми, то выполняется вызов SAC для классификации указанного потока пакетов; и при этом наоборот, если указанный сигнал указывает на то, что IP-адреса, ассоциированные с указанным потоком пакетов, не являются видимыми, то вызов SAC не выполняется.

[00064] В некоторых вариантах реализации указанная по меньшей мере одна подсистема BFC содержит: первый блок BFC, который содержит классификатор категории приложения (ACC); а также второй блок BFC, который содержит классификатор глубокой проверки потока для приложений, относящихся к конкретной категории приложений.

[00065] В некоторых вариантах реализации подсистема DPI генерирует первый вывод, который указывает на то, успешно ли подсистема DPI классифицировала конкретный поток трафика или нет; причем указанный первый вывод принимается аппаратным процессором; причем аппаратный процессор, на основе указанного первого вывода и выборочно по каждому потоку трафика, динамически определяет то, необходимо ли активировать указанную по меньшей мере одну подсистему BFC для классификации указанного конкретного потока трафика или нет.

[00066] В некоторых вариантах реализации аппаратный процессор выполнен с возможностью: (а) осуществления первой попытки классификации конкретного потока трафика посредством анализа DPI; и (б) осуществления второй попытки классификации конкретного потока трафика посредством анализа классификатора адреса сервера (SAC) в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI; и (в) осуществления третьей попытки классификации конкретного потока

трафика посредством анализа BFC в случае неуспеха попытки классификации конкретного потока трафика посредством анализа SAC.

[00067] В некоторых вариантах реализации аппаратный процессор выполнен с возможностью: (А) осуществления первой попытки классификации конкретного потока трафика посредством анализа DPI; и (Б) осуществления второй попытки классификации конкретного потока трафика посредством анализа классификатора адреса сервера (SAC) в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI и в случае, если анализ DPI определил, что IP-адреса, ассоциированные с конкретным потоком трафика, являются видимыми; и (В) наоборот, осуществления второй попытки классификации конкретного потока трафика посредством анализа BFC в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI и в случае, если анализ DPI определил, что IP-адреса, ассоциированные с конкретным потоком трафика, не являются видимыми.

[00068] В некоторых вариантах реализации система выполнена таким образом, что она повышает производительность и/или надежность, и/или устойчивость, и/или качество услуг (QoS), и/или качество восприятия (QoE) коммуникационной сети и/или системы информационных технологий.

[00069] В некоторых вариантах реализации система выполнена таким образом, что она снижает потребление энергии и/или потребление мощности, и/или потребление электричества, которые необходимы для правильной классификации одного или более потоков трафика в коммуникационной сети.

[00070] В некоторых вариантах реализации представлен компьютеризированный метод, включающий этап, на котором: классифицируют поток пакетов в коммуникационной сети путем выполнения следующих действий: (А) сперва осуществление попытки классификации конкретного потока пакетов посредством глубокой проверки пакетов (DPI); (Б) осуществление попытки классификации указанного конкретного потока пакетов посредством поведенческой классификации потоков (BFC) только в случае неуспеха попытки классификации посредством DPI.

[00071] В некоторых вариантах реализации представлены системы, устройства и методы эффективного и инновационного комбинирования блоков глубокой проверки пакетов (DPI), имеющих большой объем приложений и быстрое время классификации, с блоками поведенческой классификации потоков (BFC), которые остаются функционирующими несмотря на полное шифрование. В варианте реализации объединена система DPI, имеющая систему BFC классификации категории приложения

(ACC), с набором систем BFC детализированной глубокой проверки потоков (DFI), которые идентифицируют приложение с учетом известной категории приложения. Объединенная система извлекает выгоду из скорости, эффективности, точности и широкого охвата систем DPI для незашифрованных и частично зашифрованных случаев, при этом оставаясь функциональной для полностью зашифрованных случаев. Некоторые варианты реализации изобретения улучшают производительность и/или надежность, и/или безопасность, и/или устойчивость системы информационных технологий и/или коммуникационной сети. Настоящее изобретение может обеспечивать безопасное для окружающей среды и экономичное в части мощности решение для классификации и идентификации потоков трафика в коммуникационной ести, а также может использовать меньше энергии или мощности, или ресурсов обработки, по сравнению с традиционными системами классификации.

[00072] Признаки, функции, блоки, компоненты и/или операции, которые изображены или описаны на конкретном чертеже и/или в конкретной части описания, могут быть объединены с одним или более других признаков, функций, блоков, компонентов и/или операций, даже если они изображены или описаны на другом конкретном чертеже и/или в другой конкретной части описания.

[00073] Несмотря на то, что изобретение было описано вместе с конкретными вариантами его реализации, специалисту в данной области техники будут ясны многие альтернативы, модификации и вариации. Следовательно, предполагается охват всех таких альтернатив, модификаций и вариаций, которые подпадают под сущность и широкий объем прилагаемой формулы изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для классификации потоков пакетов в коммуникационной сети, содержащая:

подсистему глубокой проверки пакетов (DPI) и

по меньшей мере одну подсистему поведенческой классификации пакетов (BFC);

отличающаяся тем, что указанная подсистема DPI сперва предпринимает попытку классификации потока пакетов посредством анализа DPI, а в случае неуспеха, указанная по меньшей мере одна подсистема BFC предпринимает попытку классификации указанного потока пакетов посредством анализа BFC.

2. Система по п.1, дополнительно содержащая:

классификатор адреса сервера (SAC), который вызывается в случае, если подсистема DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI; причем вызов подсистемы BFC выполняется только в случае, если подсистема DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI.

3. Система по п.2,

отличающаяся тем, что если указанная система DPI не смогла классифицировать указанный поток пакетов посредством анализа DPI, то дополнительно выполняется генерирование сигнала, указывающего на то, являются ли видимыми адреса Интернет-протокола (IP), ассоциированные с указанным потоком пакетов, или нет;

причем если указанный сигнал указывает на то, что IP-адреса, ассоциированные с указанным потоком пакетов, являются видимыми, то выполняется вызов SAC для классификации указанного потока пакетов;

и при этом наоборот, если указанный сигнал указывает на то, что IP-адреса, ассоциированные с указанным потоком пакетов, не являются видимыми, то вызов SAC не выполняется.

4. Система по п.1,

отличающаяся тем, что указанная по меньшей мере одна подсистема BFC содержит:

первый блок BFC, который содержит классификатор категории приложения (ACC);

и

второй блок BFC, который содержит классификатор глубокой проверки пакетов для приложений, относящихся к конкретной категории приложения.

5. Система по п.1,

отличающаяся тем, что подсистема DPI генерирует первый вывод, который указывает на то, успешно ли подсистема DPI классифицировала конкретный поток трафика или нет;

причем указанный первый вывод принимается аппаратным процессором; причем аппаратный процессор, на основе указанного первого вывода и выборочно по каждому потоку трафика, динамически определяет то, необходимо ли активировать указанную по меньшей мере одну подсистему BFC для классификации указанного конкретного потока трафика или нет.

6. Система по п. 5,

отличающаяся тем, что аппаратный процессор выполнен с возможностью: (а) осуществления первой попытки классификации конкретного потока трафика посредством анализа DPI; и (б) осуществления второй попытки классификации конкретного потока трафика посредством анализа классификатора адреса сервера (SAC) в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI; и (в) осуществления третьей попытки классификации конкретного потока трафика посредством анализа BFC в случае неуспеха попытки классификации конкретного потока трафика посредством анализа SAC.

7. Система по п. 5,

отличающаяся тем, что аппаратный процессор выполнен с возможностью: (А) осуществления первой попытки классификации конкретного потока трафика посредством анализа DPI; и (Б) осуществления второй попытки классификации конкретного потока трафика посредством анализа классификатора адреса сервера (SAC) в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI и в случае, если анализ DPI определил, что IP-адреса, ассоциированные с конкретным потоком трафика, являются видимыми; и (В) наоборот, осуществления второй попытки классификации конкретного потока трафика посредством анализа BFC в случае неуспеха попытки классификации конкретного потока трафика посредством анализа DPI и в случае, если анализ DPI определил, что IP-адреса, ассоциированные с конкретным потоком трафика, не являются видимыми.

8. Система по п.1,

отличающаяся тем, что система выполнена таким образом, что она повышает производительность и/или надежность, и/или устойчивость, и/или качество услуг (QoS), и/или качество восприятия (QoE) коммуникационной сети и/или системы информационных технологий.

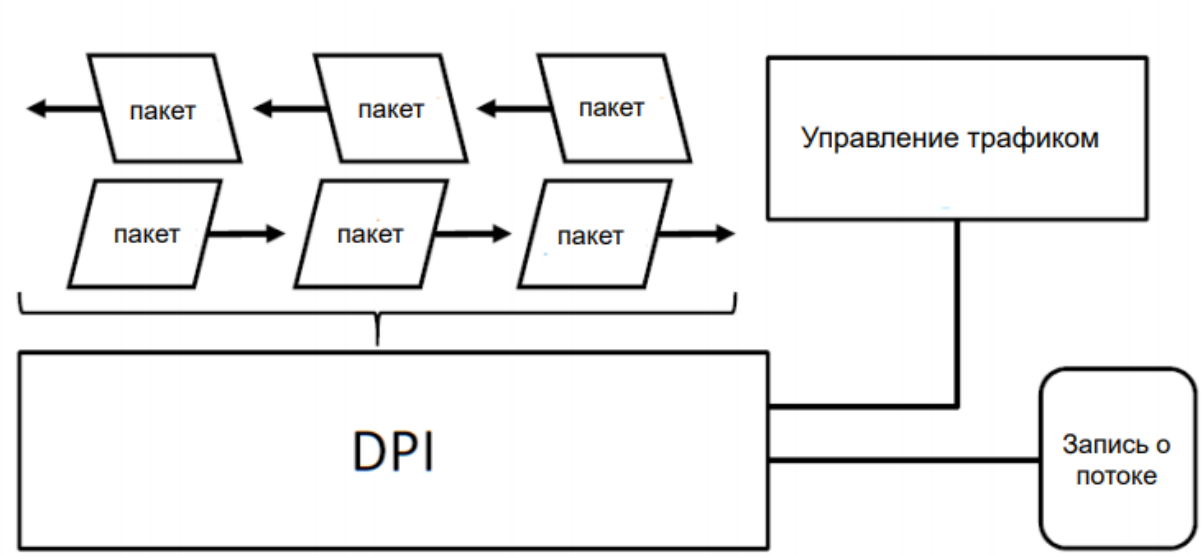
9. Система по п. 1,

отличающаяся тем, что система выполнена таким образом, что она снижает потребление энергии и/или потребление мощности, и/или потребление электричества, которые необходимы для правильной классификации одного или более потоков трафика в коммуникационной сети.

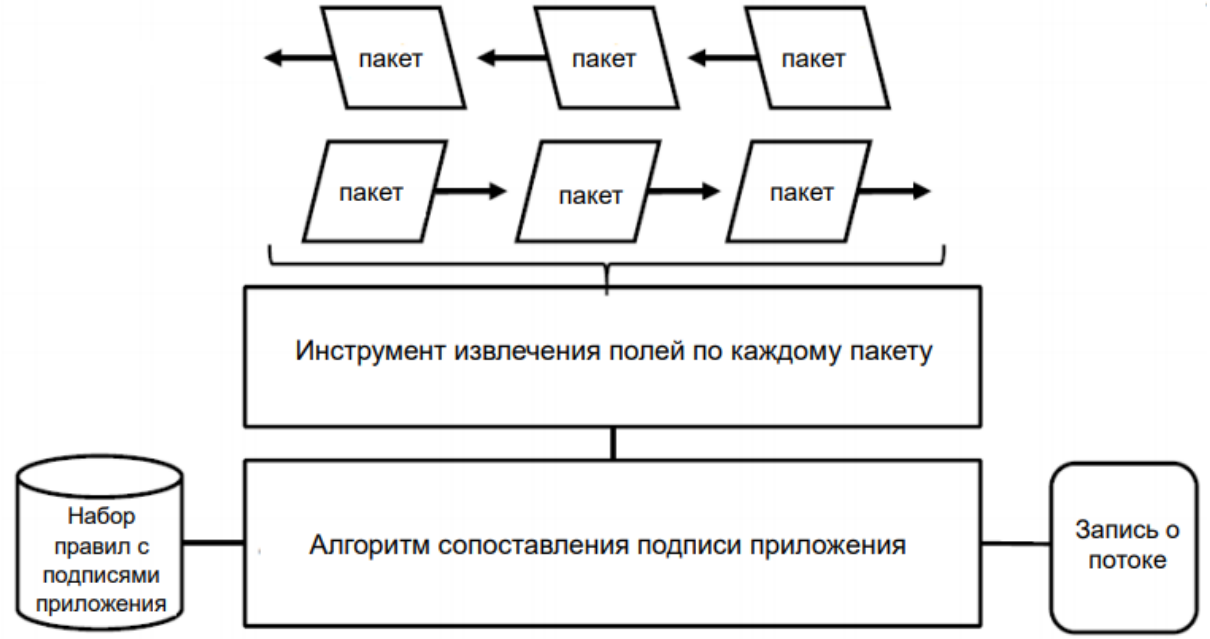
10. Компьютеризированный метод, включающий этап, на котором: классифицируют поток пакетов в коммуникационной сети путем выполнения следующих действий:

сперва осуществление попытки классификации конкретного потока пакетов посредством глубокой проверки пакетов (DPI);

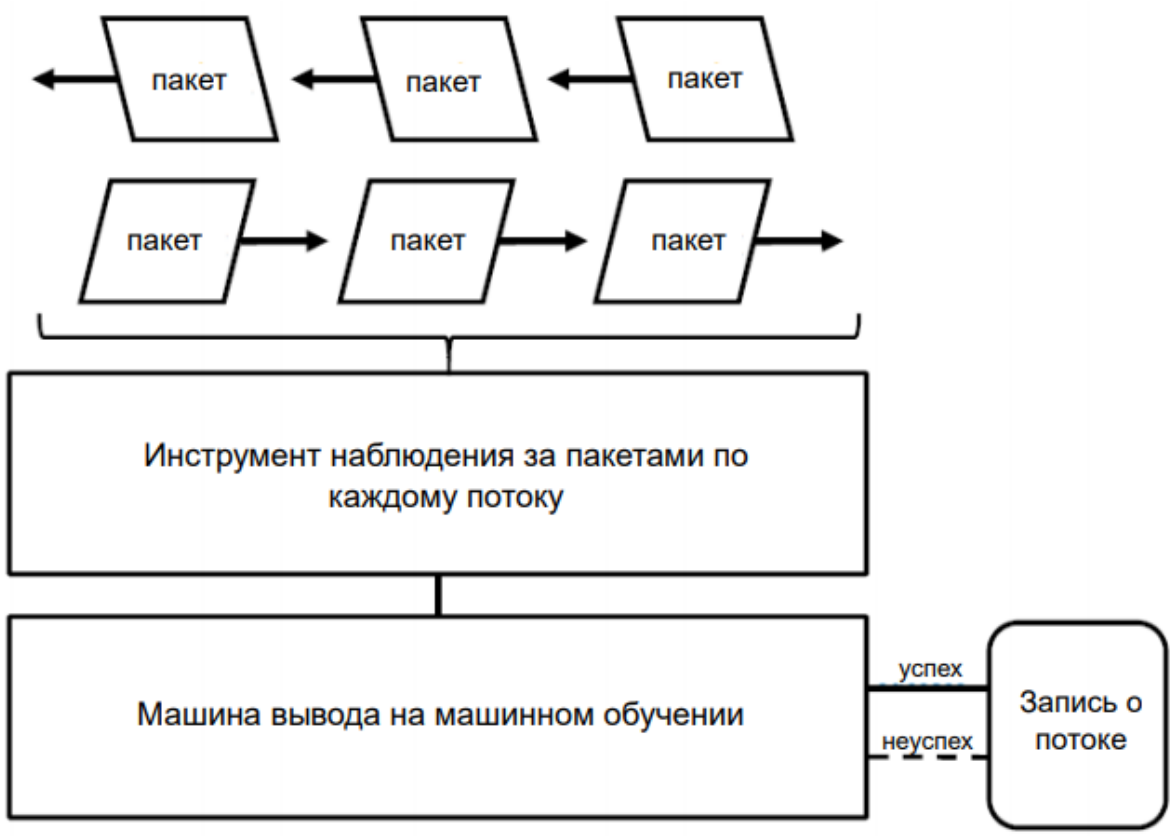
осуществление попытки классификации указанного конкретного потока пакетов посредством поведенческой классификации потоков (BFC) только в случае неуспеха попытки классификации посредством DPI.



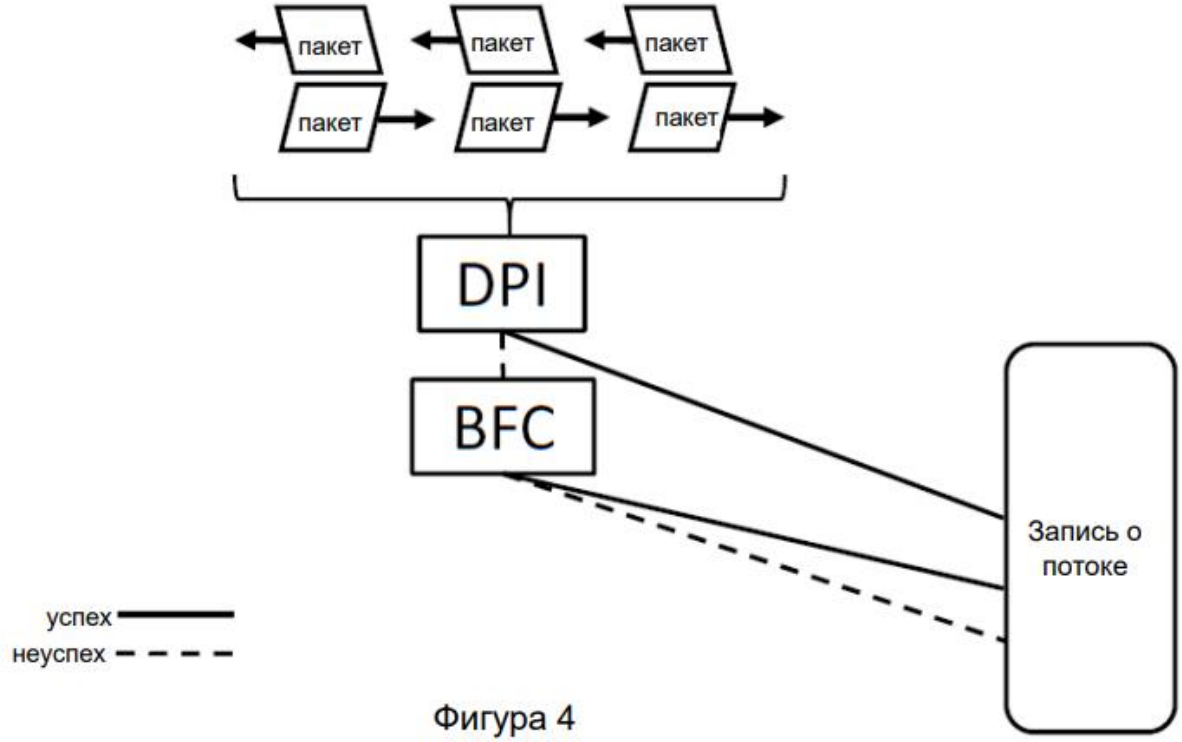
Фигура 1



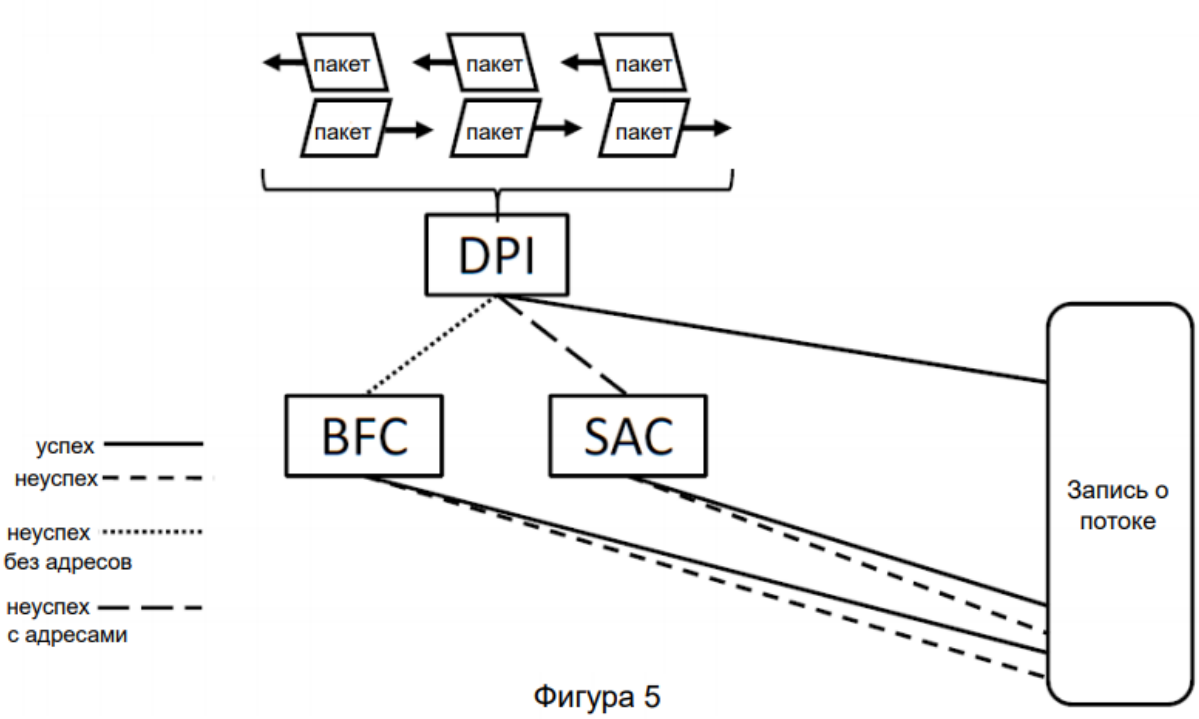
Фигура 2


пакет
пакет
пакет
пакет
пакет
пакет
Инструмент наблюдения за пакетами по каждому потоку
Машина вывода на машинном обучении
успех
неуспех
Запись о потоке

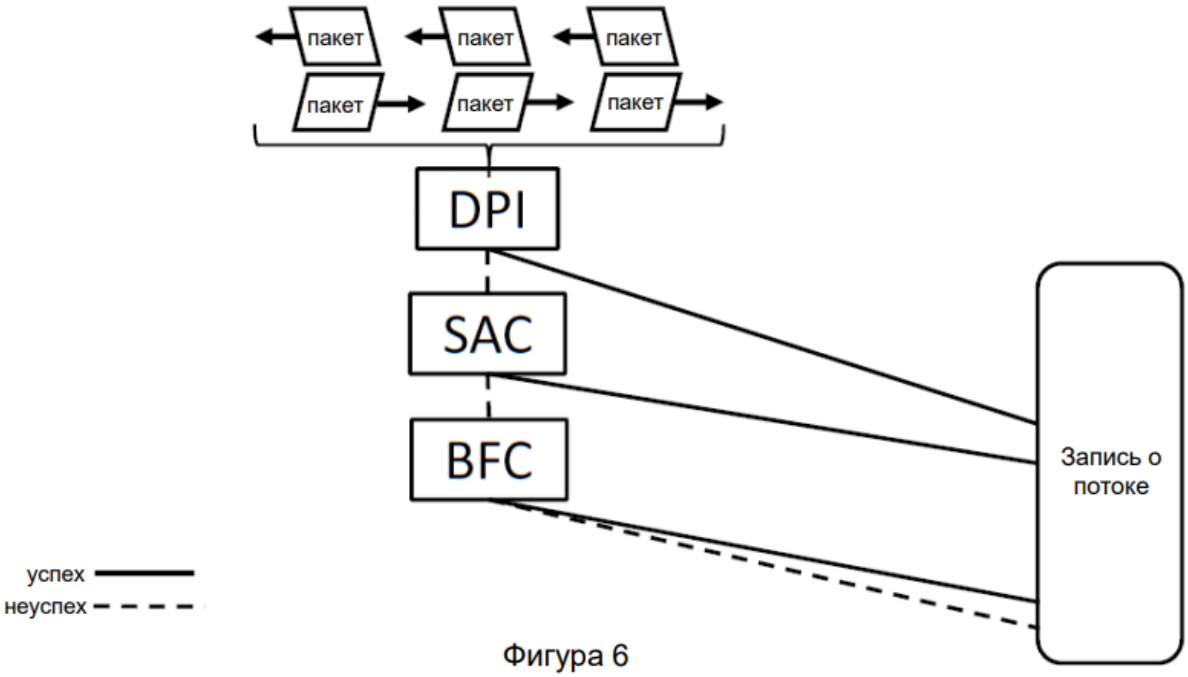
Фигура 3



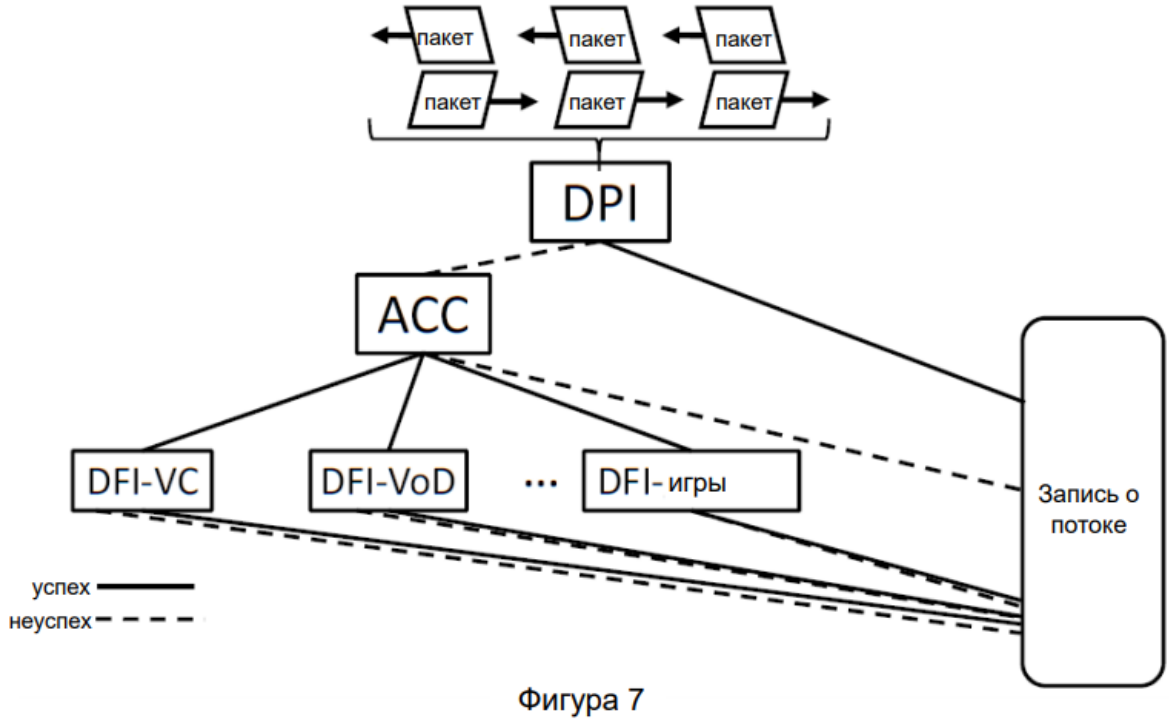
Фигура 4



Фигура 5



Фигура 6



Фигура 7

Верстка Д. Женысова
Корректор Г. Косанова