

Новые решения СОРМ для сети Skype

**Б.С. ГОЛЬДШТЕЙН, заведующий кафедрой СПбГУТ, доктор технических наук,
В.С. ЕЛАГИН, научный сотрудник НТЦ Протей**

Про "старые" решения СОРМ "Вестник связи" опубликовал серию статей в четырех выпусках журнала №№ 9 — 12 за 2005 г. с характерными названиями "Инженерные аспекты СОРМ", "Инженерные аспекты СОРМ в сетях NGN", "Инженерные аспекты тестирования СОРМ" и "Инженерные аспекты конвертирования протоколов СОРМ". Ровно через год в № 12 за 2006 г. была опубликована статья "Проблемы и решения СОРМ-2", а в № 3 за 2007 г. — статья "Законный перехват сообщений: подходы ETSI, CALEA и СОРМ". Такое пристальное внимание к этой области телекоммуникационных технологий, достаточно уникальное для отечественной журналистики, оказалось созвучным общемировым тенденциям. Одновременно с публикациями "Вестника связи" начали проводиться ежегодные международные симпозиумы по СОРМ под названием ISS World (Intelligence Support

Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering), причем каждый год и в Европе (Прага), и в Азии (Дубай), и в США. По материалам этих симпозиумов в № 4 за 2010 г. была опубликована очередная статья "Новая парадигма законного перехвата сообщений в NGN/IMS". Ее название совпало с основной темой, обсуждавшейся 2 сентября с.г. на первой российской конференции по СОРМ "Актуальные вопросы обеспечения проведения оперативно-розыскных мероприятий в сетях электросвязи Российской Федерации". Это и неудивительно: сегодняшние инженерные проблемы СОРМ полностью интернациональны, а наиболее "модной" из этих проблем и часто упоминавшейся на этой конференции является, пожалуй, СОРМ для Skype. Об этом — публикуемая ниже новая статья наших постоянных авторов.

Общая ситуация

Перехват трафика реального времени (СОРМ) для выполнения оперативно-розыскных мероприятий правоохранительными органами теоретически не должен зависеть от той или иной телекоммуникационной технологии. На практике же законный перехват трафика IP-телефонии гораздо сложнее аналогичных процедур СОРМ-1 для сетей с TDM-коммутацией, в частности, из-за независимости потоков сигнализации и пользовательского трафика.

Для поддержки СОРМ операторам приходится дополнительно проксировать весь речевой трафик на пограничных контроллерах сессий SBC. Для закрытых же сетей типа Skype и такие возможности исключаются. К тому же в компании Skype, например, твердо и последовательно настаивают, что перехват трафика — не их забота, так как правоохранительные ведомства по закону получают разрешение на прослушивание проводных или сотовых сетей связи, а Skype не является "настоящей" телефонной компанией и не имеет своих собственных телефонных

станций, кабелей, сооружений сети доступа. Это обстоятельство, убеждены в Skype, освобождает их от подчинения жестким государственным законам, которые, например, в США требуют, чтобы все телефонные компании на территории страны обеспечивали правоохранительные органы возможностью беспрепятственного прослушивания абонентов.

Имеющиеся в Skype платные сервисы SkypeIn и SkypeOut обеспечивают ей прибыльность, а абонентам — возможность звонить с обычных телефонов на компьютер или, напротив, с компьютера в традиционную телефонную сеть. При этом те звонки, которые идут через коммутируемые телефонные сети общего пользования, вполне подпадают под существующие законы о СОРМ, перехват этих звонков — всецело забота тех телефонных компаний, в сетях которых приземляется этот VoIP-трафик.

Что же касается онлайновых телефонных разговоров Skype-to-Skype, да еще с полным шифрованием пакетов, то они составляют большую проблему для СОРМ. Дело в том, что Skype использует разовые ключи шифрования, которые

две переговаривающиеся стороны генерируют и передают друг другу в каждом сеансе. Эти ключи никогда не передаются центральному серверу или кому-либо еще, кто мог бы использовать их для расшифровки звонков. Единый сертификационный центр Skype подтверждает сторонам, что их собеседники именно те, за кого себя выдают, но далее этот центр никак не связан с процессом шифрования, засекречивающим собственно переговоры. Кроме того, в такой пиринговой системе нет централизованного метода для отслеживания фактов звонков, вроде журнала с отметками о том, кто, кому и когда звонил. Очевидно, что в подобных условиях довольно трудно придумать, каким образом система сможет обеспечивать подслушивание абонентов без централизованного реестра.

Доступ к Skype может быть заблокирован аппаратными средствами. Подобные решения предлагаются на рынке компании Cisco, Verint, Narus, Verso Technologies. Успешно используют решения этих компаний в Китае, Вьетнаме, Египте, Пакистане, Саудовской Аравии и Ливии. В России есть свои успешные компании в области СОРМ:

НТЦ Протей, Малвин, МФИ-софт. В ответ на это разработчики Skype начали внедрять в программное обеспечение средства маскировки трафика для обхода блокировки VoIP. Однако работа в направлении СОРМ для VoIP-трафика продолжается и не безуспешно.

Именно технологические аспекты, которые позволяли бы эффективно распознавать, анализировать, перехватывать, дешифровать подлежащий СОРМ трафик IP-телефонии, обсуждаются в этой статье. Основное внимание уделяется техническим особенностям нового вероятностного подхода к перехвату трафика Skype.

Технологические аспекты

Рассмотрим модель законного перехвата трафика VoIP при непосредственном подключении к транспортной сети с условием, что оператор организовал точки концентрации, через которые проходит 100 % трафика, а также осуществляет законный перехват межсетевого трафика при помощи подключения к пограничным устройствам сети. В такой модели наиболее подходящими представляются две реализации архитектуры системы СОРМ-2.

Вариант 1. Распределенная архитектура. Схема организации распределенной архитектуры системы СОРМ-2 приведена на рис. 1. Работа СОРМ-2 предполагает единовременную обработку больших потоков трафика и выделения из них информации, которая подлежит перехвату. В связи с этим целесообразно разделить весь поток получаемой информации на отдельные направления. Исходя из того, что в сетях коммутации пакетов передаются данные нескольких типов, нужно будет разделять эти потоки и обрабатывать их отдельными специализированными блоками. Управление отдельными блоками осуществляется ПУ СОРМ. Для доставки команды к нужному блоку предусматривается соответствующая логика.

Вариант 2. Двусторонняя архитектура. Модель СОРМ-2 может

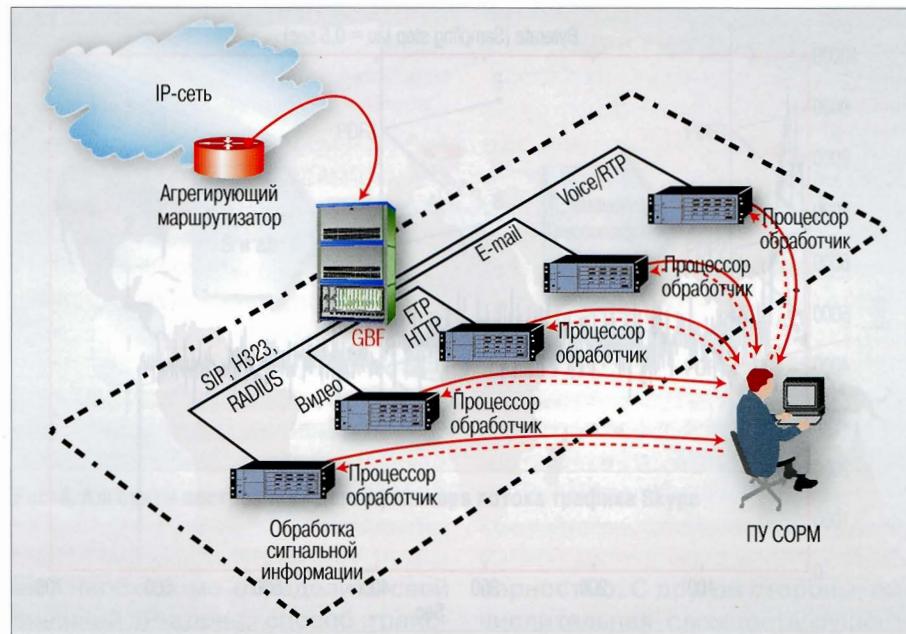


Рис. 1. Схема организации распределенной архитектуры СОРМ-2

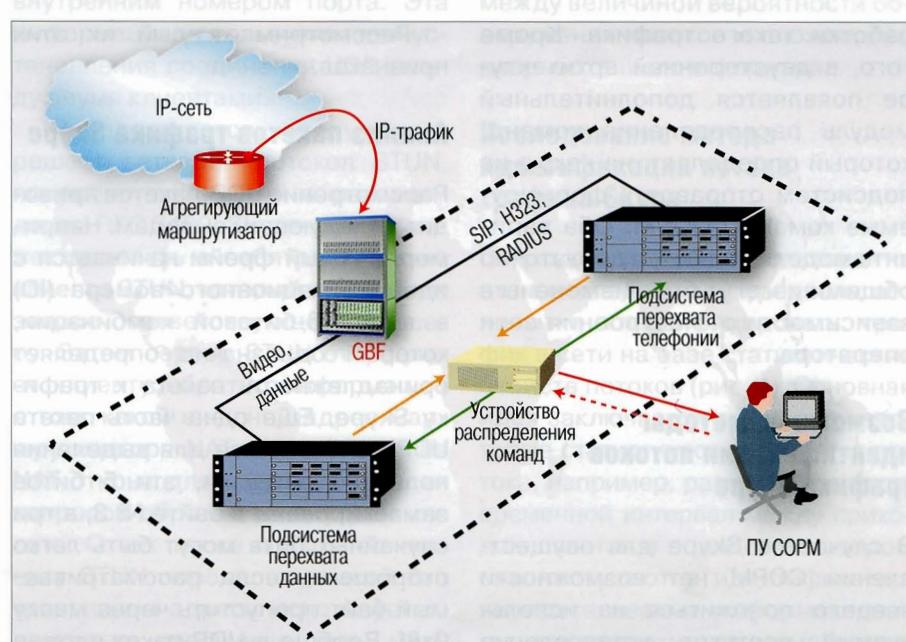


Рис. 2. Схема организации двусторонней архитектуры

строиться на базе двусторонней архитектуры, схема которой представлена на рис. 2. В ее основе лежит тот же принцип глобального перехвата трафика на специализированном узле пакетной сети связи.

Основное отличие от распределенной архитектуры заключается в самом принципе обработки перехваченной информации, согласно которому весь поток поступающей информации распределяется на два подпотока: речевые соедине-

ния и связанная с ними сигнальная информация и остальные перехватываемые данные (видео, e-mail, HTTP и т. д.).

Главным различием двух подсистем обработки является то, что для трафика реального времени (VoIP, видеоконференций и т. д.) выработаны отдельные требования обработки перехваченной информации, взятые из СОРМ-1 и отличные от СОРМ-2. Этим определяется и логика об-

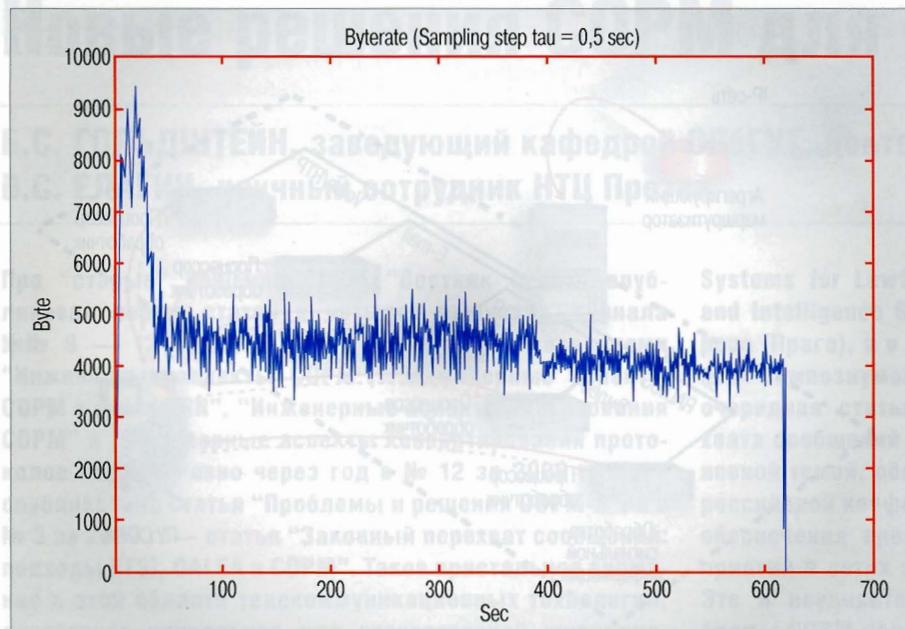


Рис. 3. Битрейт работы кодека

работки такого трафика. Кроме того, в двусторонней архитектуре появляется дополнительный модуль распределения команд, который определяет, на какую из подсистем отправлять формируемые команды СОРМ. Оба варианта модели являются достаточно общими и могут быть изменены в зависимости от построения сети оператора.

Возможные методы идентификации потоков трафика Skype

В случае со Skype для осуществления СОРМ нет возможности всецело положиться на используемый протокол установления соединения, так как это закрытый протокол, и вся информация о нем получена методами реинженеринга — дизассемблирование Skype-клиента, анализ перехватываемого трафика и т. п.

Но все же на основе проведенного анализа Skype были выявлены отдельные признаки, которые с некоей вероятностью могут идентифицировать потоки трафика, принадлежащие Skype:

- отдельно взятые пакеты TCP, UDP;
- потоки трафика, принадлежащего Skype;
- архитектура сети Skype.

Рассмотрим каждый из этих признаков.

Анализ пакетов трафика Skype

Рассмотрение UDP-пакетов приводит к следующим выводам. Например, каждый фрейм начинается с идентификационного номера (ID) в виде 16-битовой комбинации, который однозначно определяет принадлежность пакета к трафику Skype. Еще одна часть пакета UDP используется для выделения полезной нагрузки, эти 5 битов замаскированы в байте № 3, а три случайных бита могут быть легко отброшены, если рассматриваемый байт пропустить через маску 0x8f. Вообще в UDP-пакет вложен 39-байтовый NACK-пакет, который пропущен через обфускатор (функция, маскирующая информацию) и содержит следующие данные:

- идентификатор пакета (не постоянен и варьируется от пакета к пакету);
- номер функции (func), пропущенный через обфускатор;
- IP отправителя;
- IP получателя.

Остальная часть сообщения содержит информацию о соединении и блоки речевой информации, анализ которых представляет собой весьма непростую задачу, так как

Skype применяет довольно сложные алгоритмы шифрования. На веб-сайте компании отмечено, что Skype использует AES (Advanced Encryption Standard), который применяется правительственными организациями США для защиты важной информации. Речь идет об использовании 256-битового шифрования с $1,1 \times 10^{77}$ возможных комбинаций ключей шифрования.

Анализ потока трафика, принадлежащего Skype

Анализ трафика Skype может также служить для разработки методов выделения его из общих потоков данных, циркулирующих в сети. Выше уже упоминались некоторые особенности протокола Skype: закрытая спецификация протокола, применение сложных алгоритмов шифрования и функций обфускации, гибкость системы относительно номеров рабочих портов, которые препятствуют обнаружению трафика протокола на сетевом и вышележащих уровнях модели OSI.

Частотно-временной анализ трафика позволил сделать некоторые выводы. Сложно определить тип передаваемого трафика Skype, так как при передаче файлов речи или просто молчания частотно-временные диаграммы были фактически идентичны. Вместе с тем, было обнаружено, что в начальный период сеанса связи битовая скорость возрастала почти в два раза относительно остального периода сеанса (рис. 3). Это может быть связано с начальным периодом работы кодека. Предполагается, что в этот промежуток времени (около 30 с) он настраивает свои рабочие характеристики для работы в сети. Возможно, это поведение кодека может быть применено в качестве идентификатора трафика Skype при условии установки специальных фильтров в модуле СОРМ, которые выявляли бы характерные признаки работы кодека и сигнализировали об обнаружении трафика Skype.

Подчеркнем, что когда соединение уже установлено и речевая

информация передается поверх UDP-протокола, TCP-соединение не разрушается и продолжает функционировать параллельно, поддерживая процесс сопровождения сеанса связи. Таким образом, желательно выявлять оба соединения, что, с одной стороны, усложняет работу модуля СОРМ, а с другой, может также послужить неким признаком, повышающим вероятность обнаружения функционирования Skype-клиента в сети. На основе анализа трафика могут быть разработаны алгоритмы его идентификации при рассмотрении таких параметров, как:

средняя длина пакета;
битовая скорость;
пакетная скорость;
среднеквадратичное отклонение значения длины пакета.

Как правило, эти параметры применяются совместно, и это может быть выражено математически. Например, можно идентифицировать с некой вероятностью поток по теореме Байеса. Это не единственная математическая модель, которая может быть разработана, чаще всего в такие модели включаются дополнительные параметры, приводящие к более сложному алгоритму вычисления, но повышающие вероятность выявления трафика Skype.

Анализ архитектуры сети Skype

Относительно анализа архитектуры сети Skype следует отметить следующее.

Децентрализованная структура и архитектура P2P сети Skype существенно осложняет выполнение процедур СОРМ. Для обнаружения пакетов Skype оператору необходимо будет установить системы мониторинга на всех точках выхода в сеть или предусмотреть некоторую точку концентрации, через которую будет проходить весь трафик, циркулирующий в сети для обнаружения всех пользовательских операций, связанных с работой Skype.

При функционировании Skype-клиента, находящегося за сервером трансляции адресов (или за несколькими такими серверами),

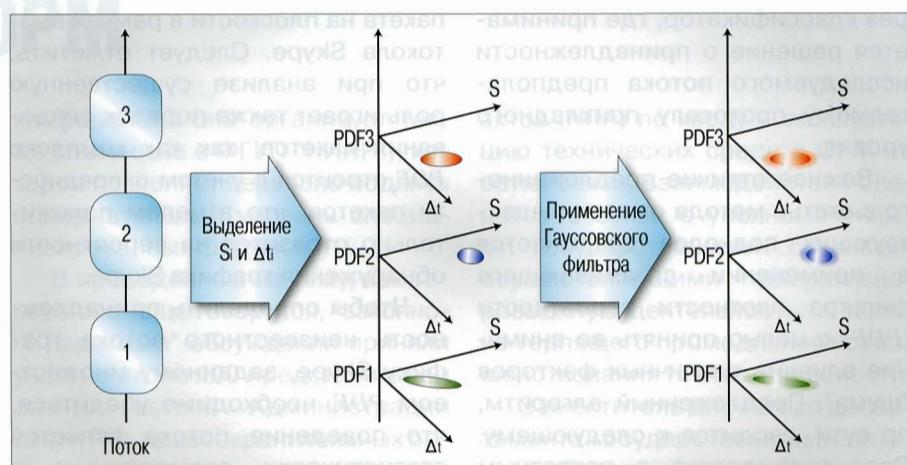


Рис. 4. Алгоритм построения идентификатора потока трафика Skype

ему необходимо определить свой внешний IP-адрес, способ трансляции адреса и порт во внешней сети, связанный с определенным внутренним номером порта. Эта информация используется для установления соединения UDP между двумя клиентами.

Предполагается, что эту задачу решает сетевой протокол STUN, подробно описанный в рекомендации RFC 3489. Skype-клиент может включать в себя реализацию клиента STUN, который отправляет запрос соответствующему серверу. Затем сервер STUN отправляет клиенту обратно информацию о том, какой внешний адрес маршрутизатора NAT и какой порт на NAT открыт для приема входящих запросов обратно во внутреннюю сеть. Ответ также позволяет клиенту STUN определить, какой тип трансляции адреса используется, поскольку различные типы маршрутизаторов NAT обрабатывают входящие UDP-пакеты по-разному. Можно попытаться проконтролировать эти процессы в сети и отследить работу клиента.

Из всего вышесказанного можно сделать вывод, что рассмотренные методы идентификации трафика Skype не дают 100 % уверенности его обнаружения, но все методы способны это сделать с некоей вероятностью. При использовании разных методов совместно может быть разработан алгоритм выявления потоков данных Skype с весьма неплохой досто-

верностью. С другой стороны, вычислительная сложность существенно возрастет. Таким образом, необходимо найти некий баланс между величиной вероятности обнаружения потоков и сложностью разработанного алгоритма.

Исследование метода идентификации потока трафика Skype

Подход, который использован в этом исследовании, предполагает попытки классифицировать трафик в сети на базе статистических свойств потоков (рис. 4). Основная идея заключается в том, что некоторые статистические свойства потока, например, размер IP-пакетов, временной интервал между приходом пакетов и порядок, в котором они поступают в идентификатор, являются весьма информативными для принятия решения о том, какое приложение генерирует этот трафик. Эти три вышеупомянутых свойства могут быть объединены в компактный и эффективный инструмент идентификации потоков.

В этом инструменте используются элементы теории вероятностей, которые позволяют описать поведение потока IP-пакетов протокола Skype, и элементы математической статистики, которые позволяют показать то, насколько "далеки" характеристики неизвестного протокола от основных характеристик предполагаемого протокола. Пакеты проходят че-

рез классификатор, где принимается решение о принадлежности исследуемого потока предполагаемому протоколу прикладного уровня.

Важное отличие предложенного в статье метода от всех существующих подходов заключается в применении сглаживающего фильтра плотности вероятности (*PDF*) с целью принять во внимание влияние различных факторов "шума". Предложенный алгоритм, по сути, сводится к следующему. Сравнение потока с известным *PDF* осуществляется путем алгебраического сложения нескольких членов, полученных путем поиска значений в таблицах *PDF*.

Идентификация IP-потоков протокола Skype производится через UDP- и TCP-порты. Определим поток F как одностороннюю, упорядоченную последовательность IP-пакетов, передаваемых между участниками соединения (соответственно, существует второй поток IP-пакетов, который направлен противоположно потоку F). Рассматриваемый поток пусть состоит из $(N+1)$ IP-пакетов, от $P_{k,0}$ до $P_{k,N}$, где $P_{k,i}$ — i -й пакет рассматриваемого потока. На уровне IP этот поток будем описывать последовательностью из N пар параметров $P_i = \{S_i; \Delta t_i\}$, где i принадлежит $[1; N]$. S_i — длина пакета, Δt_i — время между приходом пакетов. Основной причиной того, что за основу взяты два параметра S_i и Δt_i , является то обстоятельство, что в большинстве случаев статистика, связанная с этими величинами, зависит от протокола, работающего на прикладном уровне и, следовательно, порождающего этот поток. Примерами тому могут служить процессы аутентификации в POP3 или HTTP-запросы, в которых совокупность двух параметров S_i и Δt_i отлично может выступить в роли идентификатора.

В ходе исследования потоков строятся функции плотности вероятностей на основе i -ых пар P_i (на базе так называемой обучающей выборки), которые образуют комплекс, состоящий из L *PDF*. Цель *PDF*, заключается в описании i -го

пакета на плоскости в рамках протокола Skype. Следует отметить, что при анализе существенную роль играет также порядок следования пакетов, так как комплекс *PDF*, строится с учетом очередности пакетов, что в целом положительно отразится на вероятности обнаружения трафика Skype.

Чтобы определить принадлежность неизвестного потока трафику Skype, заданному множеством *PDF*, необходимо убедиться, что поведение потока является статистически совместимым с описанием, которое задано множеством *PDF*. Для этого находится параметр, определяющий "насколько статистически далек" неизвестный поток F от данного протокола Skype, описанного этими *PDF*. Значение этого параметра определяет корреляцию между поведением i -ого пакета и протоколом прикладного уровня, заданным плотностью распределения вероятности. Чем выше значение, тем выше вероятность того, что поток был вызван именно этим протоколом. Тем не менее, случайные величины, которые используются для создания каждой *PDF*, подвергаются воздействию разного рода "шумов", например разное время прихода пакетов, что вызвано разными маршрутами их перемещения вследствие перегрузки сети и т. п.

Необходимо принимать во внимание эти "шумы" при расчете. Для этого вводится понятие маски M , являющейся компонентом, предназначенным учесть различного рода искажения при расчете. Вектор M определяется вектором матриц L в результате применения Гауссовского фильтра к каждому компоненту вектора этих *PDF* и изменения масштаба каждой результирующей матрицы.

Ясно, что описанный выше алгоритм требует проведения большого числа экспериментов и сложных вычислений для достижения положительных результатов. Это серьезное исследование, которое является темой отдельной публикации. Здесь же мы ограничимся рассмотрением построения *PDF* для

протокола Skype и не будем вникать в тонкости построения Гауссовского фильтра. При построении результирующего *PDF* не учитываются шумы, которые характерны для всей сети, так как это делается для определенного ее участка, где непосредственно предполагается съем информации, причем выполняется для каждого такого элемента индивидуально.

Следует также отметить, что в протоколе Skype используется кодек iLBC (internet Low Bitrate Codec) для кодирования речи при ее передаче через Интернет. Кодек предназначен для узкополосных Интернет-каналов со скоростью передачи аудиосигнала (человеческой речи) 13,33 кбит/с при длительности кадра в 30 мс или 15,20 кбит/с при 20 мс. Кодек iLBC позволяет добиться хорошего качества передачи аудиосигнала даже при некоторых искажениях, которые происходят в связи с потерей или задержкой пакетов. iLBC описан в стандарте в RFC 3951. Его основные свойства: частота дискретизации 8 кГц/16 бит (160 отсчетов для кадров 20 мс, 240 отсчетов для кадров 30 мс); фиксированный битрейт (15,2 кбит/с для кадров 20 мс, 13,33 кбит/с для кадров 30 мс); фиксированный размер кадра (304 бита в кадре для кадров 20 мс, 400 битов в кадре для кадров 30 мс); тестирование PSQM при идеальных условиях приводит к усредненной субъективной оценке (MOS) в 4,14 для iLBC (15,2 кбит/с), сравнимой с оценкой 4,45 для G.711.

Именно использование протоколом Skype фиксированного размера кадра вносит положительный вклад в общую вероятность обнаружения потока трафика, принадлежащего протоколу Skype.

При проведении экспериментов и идентификации трафика по данной методике были получены результаты, которые давали порядка 80 % вероятности того, что перехваченный трафик является трафиком Skype. При большем количестве измерений можно получить значительно более точные результаты.