# АНАЛИТИЧЕСКИЙ ОБЗОР ПРИМЕНЕНИЯ СЕТЕВОЙ СТЕГАНОГРАФИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Каирбеков С.**

**Аннотация:** В данной статье приводится аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности, проводится сравнительный обзор различных методов стеганографии и принципов обнаружения стенаграфической активности в компьютерной сети.

**Ключевые слова:** стеганография, стеганограмма, модификация пакетов, модификация протоколов, стеганализ. криптография

Введение С того момента, как люди начали обмениваться информацией, появилась потребность в сокрытии как передаваемых данных, так и самого факта передачи информации. Именно этим занимается стеганография — наука о скрытной передаче информации. В отличие от криптографии, которая скрывает содержимое передаваемого сообщения, стеганография прячет сам факт передачи сообщения. А если сообщение не было обнаружено, то не будут обнаружены также его отправитель и получатель. Для дополнительной защиты данных можно использовать стеганографию в комплексе с криптографией.

Информационный обмен в глобальных сетях открыл массу возможностей для скрытой связи. Сообщения могут скрываться не только в обычных открытых сообщениях, как в традиционной стеганографии, но и в элементах управления протоколов связи и в результатах изменения логики протокола. В современном цифровом мире стеганография может иметь самые разные цели — от вполне безопасных и даже полезных, до преступных. В частности, одно из наиболее востребованных «мирных» приложений стеганографии — защита авторского права, когда с помощью внедренного методами стеганографии «водяного знака» можно определить автора материалов.

Стеганография может использоваться для цифровой маркировки материалов в электронных библиотеках и облачных хранилищах. Стеганографическое вложение может даже в некоторой степени подменить собой электронную подпись, потому что позволяет доказать целостность переданного материала. С другой стороны, используя стеганографию, злоумышленник может передавать через открытые каналы связи секретные данные, обходя все фильтры, установленные в сети. Стеганография может использоваться для сокрытия факта передачи запрещенных материалов и для общения преступников и террористов. Поэтому методы стеганографии и стегоанализа требуют особо тщательного изучения.

Сетевая стеганография в качестве носителей секретных данных использует сетевые протоколы эталонной модели OSI — сетевой модели

взаимодействия открытых систем. В общем виде — это семейство методов модификации данных в заголовках сетевых протоколов и в полях полезной нагрузки пакетов, изменения структуры передачи пакетов в том или ином сетевом протоколе (иногда и в нескольких сразу). Общей чертой всех методов сетевой стеганографии является создание с их помощью скрытых каналов передачи информации в любом открытом канале, в котором есть некая избыточность.

1 Методы сетевой стеганографии

1.1 Классификация методов сетевой стеганографии Методы сетевой стеганографии можно разделить на три группы. Методы модификации пакетов: – методы, изменяющие данные в полях заголовков сетевых протоколов. – методы, изменяющие данные в полях полезной нагрузки пакетов — это всевозможные алгоритмы водяных знаков, речевых кодеков и прочих стеганографических техник по сокрытию данных; – методы, объединяющие два предыдущих класса; Методы стеганографии, изменяющие структуру и параметры передачи пакетов: – методы, в которых изменяется порядок следования пакетов; – методы, изменяющие задержку между пакетами; – методы, вводящие преднамеренные потери пакетов путём пропуска порядковых номеров у отправителя; Смешанные (гибридные) методы стеганографии –изменяют и содержимое пакетов, и сроки доставки пакетов, и порядок их передачи. При этом используются два подхода: преднамеренные задержки аудио пакетов LACK (Lost Audio Packets Steganography) и ретрансляция пакетов RSTEG (Retransmission Steganography) [1].

Метод модификации сетевых пакетов Transcoding Steganography (TranSteg), изменяющий полезную нагрузку VoIP-пакета, пользуется успехом за счёт популярности программ, обеспечивающих голосовую и видеосвязь через Интернет. Как следует из названия, метод заключается в сжатии полезной нагрузки сетевого пакета за счёт перекодирования, и может применяться везде, где существует возможность сжатия — с потерями или без — открытых данных. Само сжатие требуется для ограничения размера передаваемых данных, поскольку скрытый канал связи имеет ограниченную пропускную способность. TranSteg также проводит пересжатие исходных данных с потерями, чтобы освободить место под стеганограмму.

Голосовые данные высокого битрейта (занимающие больше места в полезной нагрузке пакета) перекодируются в низкий битрейт, по возможности — с минимальными потерями качества, а на освободившееся место вносятся данные стеганограммы [8]. Метод позволяет получить неплохую стеганографическую пропускную способность в 32кб/с при наименьшей разнице в битрейте голосового потока. Польские учёные (Warsaw University of Technology, Institute of Telecommunication, [6], [7], [8]) провели ряд экспериментов, которые показали, что задержка в передаче VoIP пакета с использованием TranSteg возрастает на одну миллисекунду (1мс) в отличие от пакета без стеганограммы.

Сложность обнаружения напрямую зависит, например, от места расположения наблюдателя, в котором он может просматривать VoIP-трафик). К недостаткам данного метода стоит отнести сложность его реализации: нужно выяснить, какие кодеки используются для формирования голосового потока, и подобрать кодеки с наименьшей разницей потери качества речи (которое неизбежно будет снижаться). В качестве примера второго класса методов интересно рассмотреть использование механизмов SCTP, (Stream control transport protocol) [5] — транспортный протокол с контролем пакетов. Этот протокол реализуется в таких операционных системах как BSD, Linux, HP-UX и SunSolaris, а также поддерживает сетевые устройства операционной системы CiscoIOS и может быть использован в Windows. SCTP-стеганография использует характерные особенности данного протокола, такие как мультипоточность и использование множественных интерфейсов (multi-homing).

Методы изменения содержимого SCTP-пакетов основаны на том, что каждая часть STCP-пакета может иметь переменные параметры. Обнаружение данного метода строится на основе статистический анализ адресов сетевых карт, используемых для пересылки пакетов, с целью выявления скрытых связей. Бороться же с организацией скрытого канала передачи, основанном на этом принципе, можно изменяя адреса отправителя и получателя в случайно выбранном пакете, который содержится в повторно высылаемом блоке.

Метод RSTEG (Retransmission Steganography) основан на механизме повторной посылки пакетов. Отправитель посылает пакет, но получатель не отвечает пакетом с флагом подтверждения. Срабатывает механизм повторной посылки пакетов, и теперь посылается пакет со стеганограммой внутри, на который также не приходит подтверждения. При следующем срабатывании данного механизма посылается оригинальный пакет без скрытых вложений, на который приходит пакет с подтверждением об удачном получении.

2. Метод RSTEG Производительность RSTEG размер полезной нагрузки пакета и частота, с которой генерируются сегменты. Ни один из реальных методов стеганографии не является совершенным. Независимо от метода, скрытая информация может быть обнаружена: чем больше скрытой информации внесено в поток данных, тем больше шансов, что она будет обнаружена методами стегоанализа. Более того, чем больше пакетов используется для посылки скрытых данных, тем сильнее возрастает частота ретранслированных пакетов, что существенно облегчает обнаружение скрытого канала связи. К тому же, потери пакетов в сети тщательно контролируются, а RSTEG использует легальный трафик, таким образом увеличивая общие потери. Чтобы убедиться, что общая потеря пакетов в сети нормальна и доля RSTEG не слишком высока по сравнению с другими соединениями в той же сети, уровень ретрансляции в целях стеганографии должен контролироваться и динамично адаптироваться.

Метод стеганографии с использованием ретрансляции пакетов RSTEG является гибридным. Поэтому его стеганографическая пропускная способность примерно равна пропускной способности методов с модификацией пакета, и при этом выше, чем у методов изменения порядка передачи пакетов. Сложность обнаружения и пропускная способность напрямую связана с используемым механизмом реализации метода.

Метод RSTEG на основе RTO (Recovery Time Objective — директивное время восстановления) характеризуется высокой сложностью обнаружения и низкой пропускной способностью, а тот же метод на основе SACK (Selectiveacknowledgment — выборочное подтверждение) обладает максимальной для RSTEG пропускной способностью, но и более легко обнаруживаем.

Метод RSTEG хорошо подходит для TCP/IP, и при разумном уровне преднамеренных ретрансляций данный метод не должен вызвать подозрений у наблюдателя. Но данный метод весьма сложно реализовать, особенно те его алгоритмы, которые основаны на перехвате и исправлении пакетов обычных пользователей. Из-за резко возросшей частоты ретранслируемых пакетов или возникновения необычных задержек при передаче, стеганограммы могут вызвать подозрения у стороннего наблюдателя.

Метод LACK (Lost Audio Packets Steganography), как следует из названия, работает с протоколом VoIP. Связь через IP-телефонию состоит из двух частей: сигнальной (служебной) и разговорной. В обеих частях происходит передача информации в обе стороны. Для передачи используется сигнальный протокол SIP (Session Initiation Protocol — протокол установления сеанса) и RTP (Real-time Transport Protocol — передача трафика реального времени, собственно — разговора). Это значит, что в течении сигнальной фазы вызова конечные точки SIP (так называемые «пользовательские SIP-агенты») обмениваются некоторыми SIP-сообщениями. Обычно

SIP-сообщения проходят через SIP-серверы, что позволяет пользователям искать и находить друг друга. После установления соединения начинается фаза разговора, где аудио-поток RTP идёт в обоих направлениях между вызывающим и вызванным. И именно здесь эффективен метод LACK. Пропускная способность его не меньше, а иногда и выше, чем у остальных алгоритмов, использующих аудио-пакеты. Принцип функционирования LACK выглядит следующим образом. Передатчик выбирает один из пакетов голосового потока, и его полезная нагрузка заменяется битами секретного сообщения — стеганограммой, которая встраивается в один из пакетов.

Затем выбранный пакет намеренно задерживается. Каждый раз, когда чрезмерно задержанный пакет достигает получателя, незнакомого со стеганографической процедурой, он отбрасывается. Однако, если получатель знает о скрытой связи (именно ему адресована стеганограмма), то вместо удаления полученных RTP-пакетов он извлекает скрытую информацию [2].

При намеренном вызове потерь возникает ухудшение качества связи, что может вызвать подозрение как у обычных пользователей, так и у прослушивающего наблюдателя. Исходя из представленных результатов стегоанализа метода LACK, можно заключить, что данный метод обладает средней сложностью обнаружения. Реализация метода слишком сложна, и может быть невозможна в пределах некоторых операционных систем [1].

1.2 Сравнение методов сетевой стеганографии На диаграммах, показаны сравнительные характеристики методов сетевой стеганографии, полученные в результате исследований, описанных в [6], [7], [8].

Методы стеганографии сравнивались по пропускной способности, сложности обнаружения, стоимости и сложности реализации. Ранжирование методов осуществлено в относительных единицах и не отражает количественных характеристик. Чем больше отображенный на диаграмме параметр соответствующего метода, тем выше его характеристика. Например, самой высокой пропускной способностью обладает метод TranSteg, а самой высокой сложностью обнаружения — HICCUPS. При этом HICCUPS обладает наименьшей сложностью реализации, и находится на третьем месте по пропускной способности, что позволяет рассматривать его как фаворита.

Необходимо также учитывать, что характеристики находятся в самой тесной взаимосвязи. Так, например, сложность обнаружения будет напрямую зависеть от качества реализации, а следовательно — сложности реализации.

Сравнение методов сетевой стеганографии 2 Примеры практической реализации сетевой стеганографии 2.1 Система HICCUPS Система HICCUPS (HIdden Communication system for CorrUPted NetworkS) — стеганографическая система с распределением полосы пропускания для сетей с разделяемой средой передачи данных (shared medium). HICCUPS использует несовершенства среды передачи — шумы и помехи, которые являются естественными причинами искажения данных. Сети с разделяемой средой передачи данных, в особенности локальные сети с шинной топологией, используют различные механизмы доступа к среде, например, CSMA (Carrier Sense Multiple Access), CSMA/CD (CSMA with Collision Detection), CSMA/CA (CSMA with Collision Avoidance), Token Bus. Общая черта всех упомянутых механизмов — возможность «слышать» все кадры с данными, передаваемые в среде.

Обязательное условие для перехвата кадров — доступ к физической среде. В проводной сети — через кабельные соединения, а в беспроводных — посредством работы с радиопередающим и принимающим оборудованием на соответствующем расстоянии и частоте. «Прослушивание» всех передаваемых в среде кадров с данными и возможность отправки поврежденных кадров с неправильными значениями кодов коррекции — важнейшие сетевые функции для HICCUPS. В частности, беспроводные сети используют радиопередачу с переменной частотой битовых ошибок (BER), что создает возможность для

инъекций «искусственных» поврежденных кадров. В целом, новизна HICCUPS заключается в: использовании защищенной телекоммуникационной сети, оборудованной криптографическими механизмами, для создания стеганографической системы; новом протоколе с распределением пропускной способности для стеганографических целей, основанного на поврежденных кадрах.

Предлагаемая система предназначена для реализации в средах, обладающих следующими свойствами (обязательным является только свойство 1): Разделяемая среда передачи данных с возможностью перехвата кадров; Общеизвестный метод инициализации алгоритма шифрования, например, векторами инициализации; Механизмы целостности для зашифрованных кадров, например, односторонняя хеш-функция, циклический избыточный код — CRC.

В сети с описанными свойствами можно создать три скрытых канала данных в кадре MAC: – HDC1: канал, основанный на векторах инициализации шифра; – HDC2: канал, основанный на MAC-адресах (например, назначение и источник); – HDC3: канал на основе значений механизма целостности (например, контрольной суммы кадра). В сетях, где безопасность не обеспечивается, используются только HDC2 и HDC3. Большинство проводных сетей не поддерживают безопасность на уровне MAC, в отличие от беспроводных. Общая схема HICCUPS (рисунок 3) основана на трех режимах — система инициализации, базовый режим, режим поврежденных кадров — которые организованы следующим образом. Общая схема работы HICCUPS.

При инициализации системы все станции, включенные в скрытую группу, устанавливают секретный ключ для шифров, встроенных в стеганографическую систему. Предлагаемая система не ограничена одноадресной рассылкой (1: 1 — один отправитель одному получателю), многоадресной рассылкой (1: N — одна для многих, M: N — многие для многих) или широковещательным соединением. Решение открыто для любых процедур добавления в группу, ключевого соглашения или протокола обмена ключами [2]. Основным режимом работы HICCUPS является обмен данными на основе векторов инициализации шифра (HDC1) и MAC-адресов (HDC2). Эти скрытые каналы связи характеризуются низкой пропускной способностью — менее 1 % доступного объема кадра. Они могут использоваться для обмена контрольными сообщениями между скрытыми рабочими станциями и для связи с низкой пропускной способностью. Для установленной последовательности, передаваемой через HDC1 или HDC2, станции скрытой группы перемещаются в режим поврежденных кадров, имеющий дополнительную полосу пропускания.

В режиме поврежденных кадров информация передается внутри полезной нагрузки кадров с намеренно созданными неправильными контрольными суммами (HDC3). Этот режим обеспечивает почти 100 % пропускной способности в течение определенного периода времени. Обычно станции, которые не принадлежат к скрытой группе, отбрасывают поврежденные кадры с неправильными контрольными суммами. Общеизвестным является метод создания контрольных сумм с

поврежденным кадром для скрытых групповых станций. Последовательный перебор режимов обмена HDC1-HDC3 приводит к возврату в базовый режим. Сетевые адаптеры, работающие в режиме поврежденного кадра должны мониторить всех фреймы (даже с ошибочной контрольной суммой кадров) из среды передачи.

Основными функциональными частями предлагаемой системы являются: P1: сетевые карты, предназначенные, например, для IEEE 802.11b, IEEE 802.11g; сетевые карты должны иметь возможность контролировать HDC1-HDC3 и полезную нагрузку данных в кадре MAC; P2: система управления для контроля HDC1-HDC3 и данных в кадре MAC. Система P2 может быть программной или аппаратной и должна выполнять следующие функции: – подключение к скрытой группы; – отключение от скрытой группы; – обеспечение интерфейса для верхнего сетевого уровня для управления HDC1-HDC3 и данных в кадре MAC; с расширением криптографии: – ключевое соглашение / обмен ключами; – обновление ключа; – шифрование/дешифрование; После исследований на рынке сетевых адаптеров (включая IEEE 802.11 и IEEE 802.3) разработчики не обнаружили интерфейс, который позволял бы создать кадр с заданным CRC. Поэтому их работа направлена на разработку собственного сетевого адаптера или перепрограммирование существующего.

Некоторые из доступных сетевых адаптеровIEEE 802.11 (особенно на базе Prism II) имеют встроенный режим контроля передачи, поэтому возможен перехват всего трафика, включая поврежденный кадр. 2.2 Стеганография в VoIP-потоке Рис. 5. Принцип работы LACK Функционирование LACK подробно описано на рисунке 4. В передатчике из потока RTP выбирается один пакет, а его полезная аудио-нагрузка (голосовая информация) заменяется битами стеганограммы (1). Затем выбранный звуковой пакет намеренно задерживается перед передачей (2). Если пакет с превышенной задержкой достигает получателя, не подозревающего о стеганографической процедуре, он отбрасывается (3), потому что для не подозревающих приемников скрытые данные «невидимы». Однако, если приемник знает о скрытом сообщении, он извлекает скрытую («полезную») нагрузку вместо удаления пакета (4).

Поскольку скрытая нагрузка умышленно задерживаемых пакетов используется для передачи секретной информации получателям, осведомленным о процедуре, никаких дополнительных пакетов не генерируются [3]. Стегоанализ LACK трудно выполнить, поскольку потеря пакетов в IP-сетях является «естественным явлением», и поэтому умышленные потери, введенные LACK, нелегко обнаружить, если они находятся в разумных пределах. Потенциальные методы стегоанализа LACK включают следующее: – Статистический анализ потерянных пакетов для вызовов в подсети. Этот тип стегоанализа может быть реализован с помощью пассивного «надзирателя» (или какого-либо другого сетевого узла), например, на основе информации, включенной в отчеты протокола управления транспортным режимом (RTCP) в режиме реального времени (совокупное количество потерянных полей пакетов) между пользователями во время их обмена или наблюдения за потоками

потока RTP (порядковые номера пакетов). Если для некоторых наблюдаемых вызовов количество потерянных пакетов выше среднего (или определенного выбранного порога), этот критерий может использоваться как указание на потенциальное использование LACK. – Статистический анализ на основе длительности VoIP-звонков.

Если известно распределение вероятности продолжительности вызова для определенной подсетей, то статистический стегоанализ может быть выполнен для обнаружения источников VoIP, которые не соответствуют распределению (продолжительность вызовов LACK может быть больше по сравнению с вызовами без LACK в результате введения стеганографических данных). – Активный «надзиратель», который анализирует все RTP-потоки в сети (идентификатор источника синхронизации и поля: порядковый номер и временная метка из заголовка RTP), может идентифицировать пакеты, которые слишком задержаны и уже не могут быть использованы для восстановления голоса. Активный «надзиратель» может стирать их поля данных или просто отбросить их. Потенциальной проблемой, возникающей в этом случае, является удаление задержанных пакетов, которые все еще могут использоваться для восстановления разговора. Размер буфера дрожания в приемнике, в принципе, неизвестен активному «надзирателю». Если активный «надзиратель» отбрасывает все задержанные пакеты, тогда он потенциально может отбросить пакеты, которые могут быть использованы для восстановления голоса. Таким образом, качество разговора может значительно ухудшиться. Более того, в этом случае затрагиваются не только стеганографические звонки, но и обыкновенные.

**Заключение**

В условиях современных информационных войн, немаловажной является задача скрытной и надёжной передачи ценной информации. В последнее время приобрели популярность методы, в которых скрытая информация передается через компьютерные сети с использованием особенностей работы протоколов передачи данных. Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Кроме того, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надежного сокрытия передачи секретного сообщения. Сетевая стеганография охватывает широкий спектр методов, из которых в данной работе особенное внимание уделялось методуRSTEG, основанному на механизме повторной посылке пакетов (практический пример применения этого метода — система HICCUPS), и методу LACK-стеганографии — передаче скрытых сообщений во время разговоров с использованием IP-телефонии. В статье также приведено сравнение методов по их основным характеристикам и реализации. Описанные исследования могут быть использованы в качестве основы для разработки новых методов стеганографии или для защиты информации от утечек по скрытым каналам, созданных с помощью рассмотренных методов.

## Список использованных источников


1. Пескова, О. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет / О. Ю. Пескова, Г. Ю. Халабурда. — Таганрог: Технологический институт Южного федерального университета, 2013. — 7 с.
2. Frączek, W. Stream Control Transmission Protocol Steganography [Электронный ресурс] / W. Frączek, W. Mazurczyk, K. Szczypiorski // Warsaw University of Technology, Institute of Telecommunications. — URL: http://arxiv.org/abs/1006.0247 (дата обращения: 01.11.2017).
3. Mazurczyk, W. On steganography in lost audio packets [Электронный ресурс] / W. Mazurczyk, J. Lubacz, K. Szczypiorski. — URL: https://arxiv.org/ftp/arxiv/papers/1102/1102.0023.pdf (дата обращения: 01.11.2017).
4. Mazurczyk, W. Retransmission steganography and its detection [Электронный ресурс] / W. Mazurczyk, P. Szaga, K. Szczypiorski // IT2Net. — URL: http://cygnus.tele.pw.edu.pl/~wmazurczyk/art/RSTEG.pdf (дата обращения: 01.11.2017).
5. Mazurczyk, W. Steganography of VoIP streams [Электронный ресурс] / W. Mazurczyk, K. Szczypiorski // Wydziału Elektroniki i Technik Informacyjnych. — 2009. — URL: http://home.elka.pw.edu.pl/~wmazurcz/moja/art/OTM_StegVoIP_2008.pdf (дата обращения: 13.09.2017).
6. Mazurczyk, W. Using Transcoding for Hidden Communication in IP Telephony [Электронный ресурс] / W. Mazurczyk, P. Szaga, K. Szczypiorski // Warsaw University of Technology, Institute of Telecommunications. — URL: http://arxiv.org/pdf/1111.1250v1.pdf (дата обращения: 01.11.2017).
7. Stewart, R. Stream Control Transmission Protocol [Электронный ресурс] / R. Stewart. — RFC 4960, 2007. — URL: http://tools.ietf.org/html/rfc4960 (дата обращения: 01.11.2017).

8. Szczypiorski, K. HICCUPS: Hidden Communication System for Corrupted Networks [Электронный ресурс] / K. Szczypiorski. — URL: http://arxiv.org/abs/cs/0307050 (дата обращения: 01.11.2017).