НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2018 Том 18 № 5 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2018 Vol. 18 No 5 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.056

МЕТОД ОРГАНИЗАЦИИ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ПРОТОКОЛА ПОТОКОВОЙ ПЕРЕДАЧИ ДАННЫХ

П.М. Шипулин[a,b], В.В. Козин[b], А.Н. Шниперов[b]

[a] АО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва», г. Железногорск Красноярского края, 662972, Российская Федерация
[b] Сибирский федеральный университет, Красноярск, 660041, Российская Федерация
Адрес для переписки: pshipulin@gmail.com

Информация о статье
Поступила в редакцию 29.05.18, принята к печати 14.07.18
doi: 10.17586/2226-1494-2018-18-5-834-842
Язык статьи – русский

Ссылка для цитирования: Шипулин П.М., Козин В.В., Шниперов А.Н. Метод организации скрытого канала передачи информации на основе протокола потоковой передачи данных // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 834–842. doi: 10.17586/2226-1494-2018-18-5-834-842

Аннотация
Рассмотрены современные методы организации скрытых сетевых каналов передачи информации. Выдвинуто предположение об эффективности использования протоколов потоковой передачи данных для организации скрытых каналов. Предложен метод скрытого обмена информацией в открытых сетях. Приведена функциональная модель стеганосистемы на основе протокола RTP и показан ее программный прототип. Приведены оценочные характеристики стеганосистемы. Показаны результаты эксплуатационного тестирования программного прототипа стеганосистемы в лабораторных условиях и в сети Интернет. Программный прототип показал высокую скрытность при приемлемой для многих задач пропускной способности. Вместе с тем выявлено снижение передающих характеристик системы по мере усложнения маршрутов передачи сетевой среды. Полученные результаты исследований имеют две важнейшие области применения. Методики детектирования нелегальных сетевых стеганоканалов могут быть использованы разработчиками DLP-систем, правоохранительными органами и оборонными ведомствами. Предлагаемый метод скрытой передачи информации может быть использован для организации телеметрического канала системы связи, например, спутниковой.

Ключевые слова
стеганография, стеганосистема, скрытый информационный канал, скрытая передача информации, сетевая стеганография, протокол потоковой передачи данных

COVERT CHANNEL TECHNIQUE BASED ON STREAMING PROTOCOL

P.M. Shipulin[a,b], V.V. Kozin[b], A.N. Shniperov[b]

[a]Academician M.F. Reshetnev Information Satellite Systems, Zheleznogorsk, Krasnoyarsk region, 662972, Russian Federation
[b]Siberian Federal University, Krasnoyarsk, 660041, Russian Federation
Corresponding author: pshipulin@gmail.com

Article info
Received 29.05.18, accepted 14.07.18
doi: 10.17586/2226-1494-2018-18-5-834-842
Article in Russian

For citation: Shipulin P.M., Kozin V.V., Shniperov A.N. Covert channel technique based on streaming protocol. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 5, pp. 834–842 (in Russian). doi: 10.17586/2226-1494-2018-18-5-834-842

Abstract
The paper presents analysis of modern network covert channels. The authors set forward a hypothesis of effective streaming protocol usage for covert channel creating. Covert channel technique for open networks is proposed. RTP-based covert channel functional model is described. Estimated characteristics of software prototype are reported. The results of stegano system software prototype operational testing in laboratory conditions and the Internet are described. Software prototype demonstrated high covertness with allowable capacity for many tasks. At the same time transfer characteristics decrease with the complication of network topology. Obtained research results have two application domains of prime importance. On the one hand, illegal covert channel detection methods can be used by DLP-systems developers, law-enforcement agencies and

defense establishments. On the other hand, the proposed method for covert information transmission can be used in telemetered covert channel creation, for example, satellite communication

Keywords
steganography, stegano system, covert channel, covert information transmission, network steganography, streaming transfer protocol

Введение

Вопросы, связанные со стеганографическими методами сокрытия информации и их обнаружением, широко обсуждаются в сфере информационной безопасности в силу того, что они создают весьма существенную и вполне реальную угрозу безопасности не только в государственной, но и в коммерческой сфере [1]. В последнем случае речь идет, прежде всего, об организации утечек конфиденциальной информации и противодействия им. Интенсивное развитие информационно-вычислительных сетей и технологий, включая сервисы, базирующиеся на сетевых протоколах реального времени, например, в [2, 3], способствует развитию и методов сетевой стеганографии, позволяющих на базе телекоммуникационного канала связи организовать скрытый информационный канал.

В общем случае сетевая стеганография реализует ряд групп методов сокрытия информации посредством модификации данных в сетевых пакетах протоколов эталонной модели OSI (Open Systems Interconnection basic reference model), модификации структуры передачи пакетов или гибридным подходом [4]. Методы сетевой стеганографии, основанные на модификации данных в сетевых пакетах, осуществляют изменение полей служебных данных [5, 6] или манипулируют размером пакетов [7], например, посредством их фрагментирования. При этом содержательная часть пакетов остается без изменения, и основной коммуникационный канал не нарушается. Методы сетевой стеганографии, основанные на модификации структуры передачи пакетов, не изменяют данные в пакетах, однако вносят изменения в структуру передачи пакетов таким образом, чтобы «зашумление» основного канала передачи информации было минимальным. Для скрытой передачи могут использоваться временные задержки между пакетами [8], в том числе и такие, которые имитируют обычный сетевой трафик [9]. Гибридные методы используют оба подхода к организации скрытого канала. Заметим, что первая группа методов в современной стеганографии почти не применяется по причине ее низкой скрытности [10].

Наиболее значимыми параметрами методов сетевой стеганографии являются пропускная способность скрытого канала передачи информации, его стоимостная оценка (ухудшение характеристик основного канала), робастность (устойчивость скрытого канала в условиях естественных шумов и противодействия) и вероятность обнаружения [11]. Последний параметр является ключевым в силу самóго назначения любого стеганографического метода. Как правило, пропускная способность скрытого канала находится в прямой зависимости от вероятности его обнаружения. Исходя из этого, с точки зрения разработки стеганографического метода важно найти разумный баланс между всеми его значимыми параметрами, прежде всего, по показателю скрытности.

Как уже было отмечено, в настоящее время свою популярность приобрели различные сервисы и устройства, использующие протоколы потоковой передачи данных, например, RTP (Real-time Transport Protocol). Это IP-камеры, используемые для видеонаблюдения, а также сервисы интернет-телевидения и интернет-радио, которые передают мультимедийные данные достаточно большого объема в режиме реального времени. Их протоколы не гарантируют доставку содержимого, являются широковещательными, а также не имеют жестко заданных параметров работы [12]. Данные особенности дают ряд возможностей для организации скрытого канала передачи информации поверх основного.

В данной работе предлагается метод организации скрытого канала передачи информации на базе транспортного протокола реального времени RTP. Кроме того, в работе описывается модель сетевой стеганосистемы и протокол скрытой передачи информации. Описанная стеганосистема была реализована в виде программного прототипа. В работе приводятся оценки основных характеристик стеганоканала, полученные при передаче в лабораторных условиях и сети Интернет.

Предлагаемый метод организации скрытого канала передачи информации

В 2001 году С. Серветто в работе [13] указал на возможность умышленного пропуска пакетов при передаче потока данных для создания скрытого канала передачи информации. Суть идеи заключалась в том, что один переданный или пропущенный пакет в некоторый интервал времени соответствует одному разряду передаваемой скрытой информации. В 2004 году С. Кабук в работе [14] описал модель стеганосистемы, основанную на изменении скорости передачи пакетов: получатель может восстановить скрываемую информацию, измеряя скорость получения пакетов за определенные интервалы времени.

Описанные идеи были использованы при разработке метода организации скрытого канала передачи информации, где стеганоконтейнером выступает RTP-поток. Метод встраивания стеганосообщения базируется на передачи бинарной последовательности длины N в виде последовательности RTP-пакетов: переданный пакет соответствует единичному биту, фантомный (намеренно пропущенный) – нулевому (рис. 1). Временные промежутки t между RTP-пакетами считаются равными друг другу.

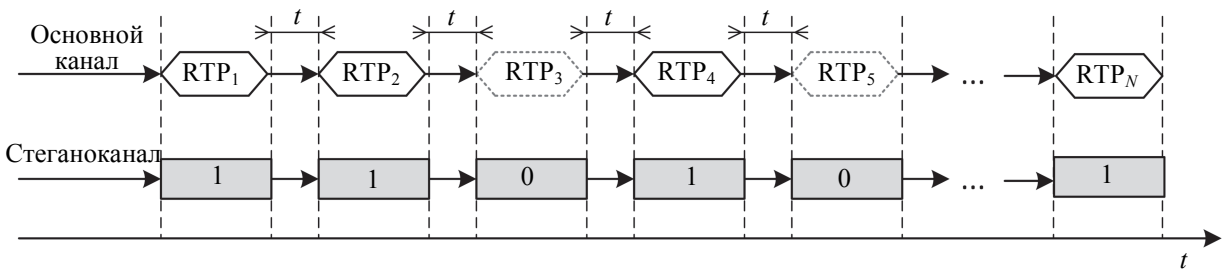

Рис. 1. Стеганоканал на базе RTP-потока

Для эффективной передачи стеганосообщений подобным способом их необходимо подготовить к передаче, добавив средства контроля целостности. Кроме того, необходимо обеспечить приемлемое «зашумление» RTP-потока, чтобы его характеристики менялись незначительно. Данные требования реализованы в предлагаемой стеганосистеме.

Структурная схема построения стеганосистемы, представленная на рис. 2, является практически классической для сетевой стеганографии [15]. Отличие заключается в том, что, кроме основного канала передачи информации – передатчик-приемник, схема включает в себя и дополнительный – управляющий канал связи передатчик-приемник, посредством которого осуществляется конфигурирование стеганосистемы. Этим управляющим каналом может быть, например, канал для управления устройством, с которого ведется широковещательная передача.

Основным элементом передатчика стеганосистемы является модулятор, который, используя выходные значения с таймера и генератора псевдослучайных чисел (ГПСЧ), модулирует стеганокодером основной канал – поток RTP-данных в соответствии с передаваемым стеганосообщением. Изменения в основном канале производятся передатчиками стеганосистемы таким образом, чтобы приемник, имеющий зеркальное строение, имел возможность извлечь стеганосообщение.

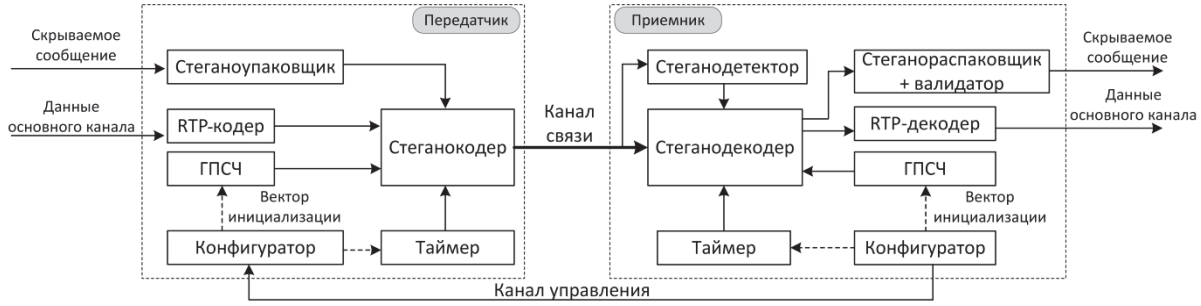

Рис. 2. Принципиальная схема стеганосистемы

Стеганокодер в процессе модулирования RTP-потока определяет, какой пакет следует в действительности передать, а какой намеренно пропустить (сделать фантомным). Таймер на стороне передатчика используется для поддержания стабильности временных задержек между всеми передаваемыми RTP-пакетами (реальными и фантомными) – это необходимо для однозначной интерпретации потока на стороне приемника при помощи синхронизированного с передатчиком таймера. Посредством конфигуратора на стороне передатчика и приемника инициализируется ГПСЧ и настраивается таймер. Применение в стеганосистеме ГПСЧ повышает скрытность канала, так как обеспечивает псевдослучайность появления фантомных пакетов, а также увеличивает конфиденциальность, затрудняя извлечение стеганосообщения из уже раскрытого стеганоканала. В качестве ГПСЧ может быть использован любой генератор, имеющий большой период.

Стегандетектор предназначен для идентификации передачи скрытого сообщения в RTP-потоке. Стегандекодер устанавливает соответствие между бинарной последовательностью скрытого сообщения, передаваемого по стеганоканалу, и потоком RTP-пакетов основного канала.

Модель стеганосистемы и протокол скрытой связи

Функциональная модель предлагаемой стеганосистемы представляет собой совокупность следующего вида:

$$\sum = (M, FC, SP, SUP, SV, Enc, Dec, PR, PC),$$

где M – множество передаваемых скрытых сообщений; FC – потоковый стеганоконтейнер (RTP-пакеты); $SP: M \to GP$ – отображение скрытого сообщения в бинарном виде в группы метапакетов (стеганоупаковщик); $SUP: GP \to M$ – отображение групп метапакетов в скрытое сообщение в бинарном виде (стеганораспаковщик); SV – валидатор, обеспечивающий проверку целостности полученного стеганосообщения;

$Enc: GP \to FC$ – отображение групп метапакетов в потоковый стеганоконтейнер (стеганокодер); $Dec: FC \to GP$ – отображение потокового стеганоконтейнера в группы метапакетов; $PR = \{pr_1, pr_2, pr_3, pr_4\}$ – стек протоколов передачи стеганосообщения; PC – протокол управления.

В предлагаемой модели стеганосистемы взаимодействие между приемником и передатчиком обеспечивает оверлейный стек протоколов – *PR*, реализованный над протоколом RTP. На рис. 3 проиллюстрирована аналогия соответствия внутреннего стека протоколов *PR* стеганосистемы и стека протоколов модели OSI[1] (избранным ее уровням: 1, 3, 4, 6). Протокол pr_4, являясь протоколом верхнего уровня, представляет стеганосообщение в открытом, бинарном виде. Протокол pr_3 предназначен для упаковки стеганосообщения в метапакеты – абстрактные сущности, предназначенные для передачи нескольких бит стеганосообщения с возможностью обнаружения двух ошибок и исправления одной. Протокол pr_2 организует группу метапакетов с заданной их избыточностью (дублированием в пределах группы от 1 до *n* раз) и контролем целостности, готовой к дальнейшей передаче. Протокол pr_1 обеспечивает передачу групп метапакетов посредством модулирования RTP-потока.

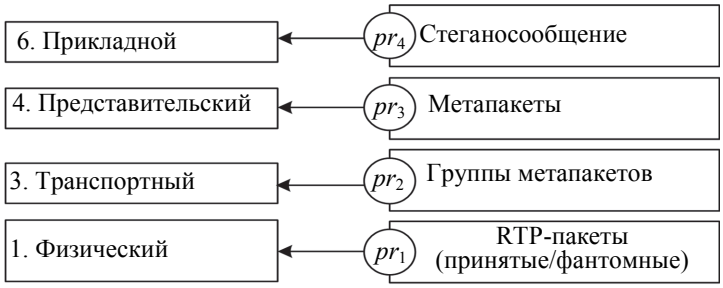

Рис. 3. Аналогия соответствия стека протоколов стеганосистемы модели OSI

Опишем предлагаемый протокол взаимодействия передатчика и приемника.

Расчет параметров стеганосистемы. При подготовке стеганосистемы к передаче данных производится ряд предварительных действий.

Шаг 1. Передатчиком производится тестовая передача пустого потокового контейнера (множества RTP-пакетов) $FC = \langle rtp_1, rtp_2, ..., rtp_k \rangle$. Приемник вычисляет потенциальную емкость потокового контейнера $Z = \sum_{i=1}^{k} z_i$, где $z_i \in [0;1]$ обозначает пришедший либо не пришедший RTP-пакет, и $T = \langle t_1, t_2, ..., t_{k-1} \rangle$ – последовательность задержек между RTP-пакетами, где t_i – задержка между получением *i*-го и (*i*+1) RTP-пакета.

Шаг 2. Приемник вычисляет $\mu = \frac{1}{k}\sum_{i=0}^{k-1}(t_{i+1} - t_i), t_i \in T$ – среднее время задержки между пакетами.

Шаг 3. Приемник генерирует вектор инициализации *IV*, который будет использоваться ГПСЧ для генерации псевдослучайных последовательностей.

Шаг 4. По каналу управления *PC* приемник передает совокупность параметров $\{Z, \mu, IV\}$ на передатчик, из которых *Z* и μ являются оценочными характеристиками пустого потокового контейнера (его потенциальная емкость и среднее время задержки между RTP-пакетами). На передатчик могут быть переданы и другие конфигурационные параметры, например, коэффициент избыточности (дублирования) передаваемой скрытой информации.

Шаг 5. На передатчике на основе полученной характеристики *Z* выбирается величина вносимых искусственных потерь RTP-пакетов *L* (регулирует среднее число фантомных пакетов). Передатчиком также устанавливается величина искусственной задержки $td >> \mu$, которая является признаком начала передачи заполненного потокового контейнера, где « >> » – знак «намного больше».

Подготовка стеганосообщения к передаче. Перед заполнением потокового контейнера *FC* скрытое сообщение $m_i \in M$ необходимо подготовить (упаковать) посредством отображения $SUP: GP \to M$, которое реализует следующий алгоритм.

Шаг 1. Скрываемое сообщение $m_i \in M$ представляется в виде бинарной последовательности $m_i \to MB_n = \langle mb_1, mb_2, ..., mb_n \rangle$.

[1]ISO/IEC 7498-4:1989. – Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing.

Шаг 2. Для контроля целостности и возможности исправления ошибок передачи сообщение упаковывается в метапакеты $MB_n \to P^\alpha = \left\langle p_1^\alpha, p_2^\alpha ..., p_m^\alpha \right\rangle$, где $p_j^\alpha = \left(j \bullet mb_i \bullet mb_{i+1} \bullet ... \bullet mb_{i+\alpha} \bullet H(mb_i \bullet mb_{i+1} \bullet ... \bullet mb_{i+\alpha}) \right)$, j – порядковый номер метапакета, $i = \left(j \cdot \alpha \right) - \alpha + 1$ – порядковый номер бита mb_i скрываемого сообщения, $H(x)$ – функция вычисления проверочных бит по битам скрываемого сообщения (на основе кодов Хемминга), «$\bullet$» – операция конкатенации, α – размер информативной части метапакета. Количество проверочных символов кода Хемминга ρ выбирается таким образом, чтобы параметры кодирования удовлетворяли условиям $(2^\rho - 1) \in Z, (2^\rho - 1 - \rho) \in Z$ и $(2^\rho - 1 - \rho) = \alpha$.

Шаг 3. Метапакеты группируются следующим образом $GP : P^\alpha \to G_\gamma^\delta = \left\langle g_1^\delta, g_2^\delta, ..., g_k^\delta \right\rangle$, где $g_i^\delta = \left(\left(p_i^\alpha * \delta \right) \bullet ... \bullet \left(p_{i+\gamma}^\alpha * \delta \right) \right) \bullet \Omega\left(p_i^\alpha \bullet ... \bullet p_{i+\gamma}^\alpha \right)$, δ – коэффициент дублирования метапакетов в группе, γ – размер группы метапакетов, $\Omega(x)$ – функция вычисления контрольной суммы CRC-8, «*» – операция повторения посредством конкатенации.

Шаг 4. Для контроля целостности всего стеганосообщения формируется начальная группа метапакетов $g_0 = \left[p_0 \bullet \Omega\left(p_0 \right) \bullet \Omega\left(p_0 \bullet \Omega\left(p_0 \right) \right) \right]$, где p_0 – метапакет, содержащий размер передаваемого скрытого сообщения. Начальная группа g_0 передается в самом начале передачи.

Передача стеганосообщения. Стеганокодер передатчика формирует последовательность RTP-пакетов посредством отображения $Enc : GP \to FC = \left\langle rtp_1, rtp_2, ..., rtp_z \right\rangle$, где rtp_i – RTP-пакет. Функция стеганокодирования (модулирования RTP-трафика) принимает следующий вид:

$$T_i = \begin{cases} T_i = b_j : b_j \in g_0 \cup G_\gamma^\delta \Leftarrow \psi_i \in \Gamma, \\ T_i = 1 \Leftarrow \psi_i \notin \Gamma, \end{cases}$$

где ψ_i – псевдослучайное число, соответствующее передаваемому RTP-пакету, b_j – текущий бит из подготовленного к передачи стеганосообщения. Если $T_i = 1$, RTP-пакет передается, если $T_i = 0$, RTP-пакет намеренно пропускается (фантомный пакет). При передаче стеганосообщения ГПСЧ формирует последовательность Γ, которая соответствует последовательности номеров позиций пакетов в RTP-потоке, которые будут переданы ($\psi_i = 1$) или намеренно пропущены ($\psi_i = 0$). При каждой новой попытке передать стеганосообщение ГПСЧ инициализируется заново для повторной синхронизации ГПСЧ на приемнике и передатчике.

Прием стеганосообщения. Стеганодекодер приемника из последовательности принятых RTP-пакетов (потокового контейнера) формирует группы метапакетов посредством отображения $Dec : FC \to GP = g_0 \cup G_\gamma^\delta$, включая стартовую группу g_0 с параметрами стеганосообщения, которое реализует следующий алгоритм.

Шаг 0. Стеганодетектор приемника регистрирует задержки между всеми принятыми RTP-пакетами, прием стеганосообщения начинается, когда очередная задержка больше или равна *td* – величине искусственной задержки, являющейся признаком начала стеганопередачи.

Шаг 1. Приемник инициализирует ГПСЧ вектором инициализации *IV* и запускает его.

Шаг 2. Предполагая равномерную передачу последовательности пакетов, стеганодекодер приемника регистрирует принятые/пропущенные RTP-пакеты, формируя бинарную последовательность $R = \left\langle r_{\psi_1}, r_{\psi_2}, ..., r_{\psi_j} : r_i \in [0;1] \right\rangle$. Регистрация наличия/отсутствия RTP-пакета осуществляется только в позициях, заданных $\psi_i \in \Gamma$ – псевдослучайным числом, полученным от ГПСЧ.

Распаковка стеганосообщения. Для распаковки скрытого сообщения приемником используется отображение $SUP : GP \to M$, которое реализует следующий алгоритм.

Шаг 1. В соответствии с параметрами стеганосистемы из полученной бинарной последовательности извлекается начальная группа g_0 с параметрами стеганосообщения, а также формируются группы метапакетов *GP*.

Шаг 2. Из каждой группы метапакетов извлекаются ее метапакеты $f : G_\gamma^\delta \to P^\alpha$, проверяется их контрольная сумма, а также контрольная сумма группы.

Шаг 3. Если удалось получить корректные метапакеты, то шаг 6.

Шаг 4. Если контрольная сумма не совпала ни для одного метапакета в группе, то для каждого из них пытаемся произвести процедуру исправления одной ошибки по коду Хемминга.

Шаг 5. Повторно проверяем CRC-8 для всех метапакетов в группе. Если корректные метапакеты получены, переходим на шаг 6, иначе посредством протокола *PC* делаем запрос на повторную передачу

стеганосообщения (корректно полученные метапакеты сохраняются для последующих попыток распаковки), и алгоритм распаковки прерывается.

Шаг 6. Из метапакетов извлекается бинарное сообщение $f : P^{\alpha} \to MB_n$.

Шаг 7. Для контроля целостности всего бинарного сообщения его контрольная сумма сравнивается с той, которая получена из начальной группы g_0 на шаге 1. Если результат проверки отрицательный, делаем запрос на повторную передачу стеганосообщения, и алгоритм распаковки прерывается.

Шаг 8. Бинарное сообщение преобразуется к оригинальному виду.

Программная реализация стеганосистемы и результаты испытаний

При разработке программного прототипа, реализующего предлагаемый метод скрытой передачи информации, необходимо учитывать следующие факторы:

– состояние сети (во время пиковой нагрузки с высокой вероятностью будут наблюдаться значительные естественные задержки между пакетами и ошибки в очередности пакетов. Вероятность успешного получения RTP-пакета падает);

– вычислительные возможности отправителя и получателя (при обработке пакетов возможно возникновение непреднамеренных временных задержек между пакетами);

– сложность алгоритма (с увеличением сложности алгоритма отправки/обработки пакетов возможно возникновение непреднамеренных временных задержек между пакетами).

В силу вышеизложенного было принято решение, что программный прототип стеганосистемы будет иметь модульную структуру. Ядро стеганосистемы, реализующее взаимодействие с пользователем и непосредственную модуляцию RTP-потока, реализовано на языке высокого уровня C++. Для работы с RTP-потоком используется библиотека JRTPLIB[1].

Для реализации подготовительных операций для передачи стеганосообщения были спроектированы модули на языке высокого уровня Python:

– расчет оценочных параметров пустого потокового контейнера (его потенциальная емкость и среднее время задержки между RTP-пакетами);

– генерация псевдослучайных чисел на основе алгоритма Xorshift [16];

– стеганоупаковщик и стеганораспаковщик.

По своему составу программный прототип представляет собой клиент-серверное приложение, состоящее из двух частей – сервера и клиента. Модули реализованы кроссплатформенно. Ядро программы реализовано как консольное приложение для операционной системы Microsoft Windows.

Для проведения тестирования программного прототипа в лабораторных условиях была создана локальная сеть из двух коммутаторов и трех маршрутизаторов.

Зависимость времени передачи стеганосообщения от начальных параметров стеганосистемы представлена в табл. 1.

Количество вносимых потерь на 50 000 RTP-пакетов	Коэффициент дублирования	Время передачи, мин		
3	0	30	70	137
	1	65	153	290
	2	100	223	430
5	0	18	44	82
	1	40	85	175
	2	72	129	260
8	0	11	25	55
	1	24	54	120
	2	39	76	188
		200	500	1024
		Размер сообщения, Б		

Таблица 1. Время передачи стеганосообщения в зависимости от начальных параметров стеганосистемы

Скорость передачи стеганосообщения напрямую зависит от величины коэффициента дублирования δ и количества вносимых потерь.

Во всех экспериментах инициализация скрытого канала проходила успешно, стеганосообщение передавалось в полном объеме, количество ошибок было минимальным. После передачи клиент стеганосистемы успешно восстанавливал стеганосообщение за счет обнаружения и исправления ошибок

[1] http://research.edm.uhasselt.be/jori/page/CS/Jrtplib.html

в метапакетах и проверки контрольных сумм. При проведении тестирования в реальных условиях сети Интернет стеганосообщение передавалось по маршруту, включающему в себя произвольное количество сегментов с разными шлюзами.

Пропускная способность стеганоканала существенно уменьшилась при переходе из локальной вычислительной сети в сеть Интернет. Инициализация скрытого канала передачи проходила успешно, однако стеганосообщение передавалось корректно не в полном объеме. Передаваемое стеганосообщение имело размер, равный 1024 Б. В табл. 2 приведена зависимость успешного получения сообщения от начальных параметров стеганосистемы и времени суток проведения эксперимента при коэффициенте избыточности, равном $\delta = 0$.

Время проведения эксперимента	Вероятность получения сообщения									
1:00-9:00	10	14	20	25	23	52	86	100	100	100
9:00-17:00	6	1	11	19	27	33	60	71	87	100
17:00-1:00	1	1	1	1	02	03	7	10	15	20
	4	10	20	40	80	200	400	800	2×10^3	10×10^3
	Количество вносимых потерь на 50 000 RTP-пакетов									

Таблица 2. Вероятность успешного получения сообщения, %, от начальных параметров стеганосистемы и времени проведения испытаний

На основании полученных результатов может быть сделан следующий вывод: нагрузка на сетевое оборудование в течение дня изменяется, что сказывается на возможности полной передачи стеганосообщения.

Оценка робастности и необнаружимости скрытого канала связи

Как уже было отмечено, при оценке стеганоканала необходимо учитывать следующие его характеристики: пропускную способность, робастность, необнаружимость (скрытность), стоимость канала [11]. Следует отметить, что максимальные значения пропускной способности, робастности и скрытности не являются совместными, а находятся в попарной обратной зависимости друг от друга.

Для разработанного программного прототипа стеганосистемы были получены следующие оценки.

Пропускная способность может быть оценена качественно скоростью передачи данных посредством скрытого канала связи (стеганоканала). В зависимости от начальных параметров стеганосистемы для передачи 200 Б потребуется от 11 до 100 мин (см. табл. 1).

Стоимость канала может быть оценена количеством намеренно пропущенных пакетов в RTP-канале. В зависимости от начальных параметров стеганосистемы количество вносимых потерь изменялось между 3, 5 и 8 пакетами на каждые 50 000 RTP-пакетов.

Необнаружимость стеганоканала может быть оценена как качественно, так и количественно. Высокая качественная оценка необнаружимости канала связана с тем, что человеческие органы чувств не способны распознать потерю некоторого объема потерянных данных (RTP-пакетов) в много большем объеме передаваемых данных. Количественная оценка необнаружимости канала может быть сделана на основе анализа RTP-трафика, например, статистического. Измерение характеристик канала связи для автоматической настройки стеганосистемы и использование ГПСЧ при формировании намеренных потерь не нарушает статистику распределения полученных/потерянных пакетов, что подтверждено проверкой статистических критериев согласия для пустого потокового контейнера и заполненного (в котором имеются намеренные потери).

Робастность стеганоканала может быть оценена количественно. В локальной компьютерной сети, при отсутствии значительных внешних помех, стеганосообщение передавалось с потерями 0%. В сети Интернет, при естественном воздействии недетерминированных помех, в зависимости от начальных параметров стеганосистемы потери составляли 0–100% (см. табл. 2).

Заключение

В работе предлагается метод организации скрытого канала передачи информации на базе транспортного протокола реального времени RTP. Описана функциональная модель сетевой стеганосистемы, протокол скрытой связи, приведены характеристики стеганоканала, полученные с использованием разработанного программного прототипа.

Как показали эксперименты по организации стеганоканала в локальной вычислительной сети, предлагаемые метод скрытой передачи и стеганосистема реализуемы на практике. Оценочные характеристики носят вполне удовлетворительный характер. Однако эксперименты с использованием сети Интернет показали, что данное исследование требует дальнейшего развития. В частности, необходимо рас-

смотреть более эффективные методы помехоустойчивого кодирования в задачах реализации протоколов скрытой связи.

Полученные результаты исследований в данной области имеют две противоположные области применения. С одной стороны, методики детектирования нелегальных сетевых стеганоканалов могут быть предложены к использованию разработчикам DLP-систем, правоохранительным органам и оборонным ведомствам. С другой стороны, предлагаемый метод скрытой передачи информации может быть использован для организации телеметрического канала системы связи, например, спутниковой.

Литература

1. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications. 2017. V. 11. N 4. P. 71–84. doi: 10.14257/ijsia.2017.11.4.06
2. Karas M., Mazurczyk W., Szczypiorski K. SkyDe: a Skype-based steganographic method // International Journal of Computers, Communications & Control. 2014. V. 8. N 3. P. 432–443. doi: 10.15837/ijccc.2013.3.469
3. Janicki A., Karas M., Mazurczyk W., Szczypiorski K. YouSkyde: information hiding for Skype video traffic // Multimedia Tools and Applications. 2016. V. 75. N 21. P. 13521–13540. doi: 10.1007/s11042-015-2740-0
4. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. Wiley, 2016. 296 p.
5. Dyatlov A., Castro S. Exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the http protocol. Technical Report. Gray World, 2003. 8 p.
6. Rowland C.H. Covert channels in the TCP/IP protocol suite // First Monday. 1997. V. 2. N 5. 15 p. doi: 10.5210/fm.v2i5.528
7. Lewis S., Murdoch S.J. Embedding covert channels into TCP/IP // Lecture Notes in Computer Science. 2005. V. 3727. P. 247–261. doi: 10.1007/11558859_19
8. Berk V., Cybenko G., Giani A. Detection of covert channel encoding in network packet delays. Technical Report TR 2005-536. Dartmouth College, 2005. 11 p.
9. Gianvecchio S., Wang H., Wijesekera D., Jajodia S. Model-based covert timing channels: automated modeling and evasion // Lecture Notes in Computer Science. 2008. V. 5230. P. 211–230. doi: 10.1007/978-3-540-87403-4_12
10. Wendzel S., Mazurczyk W., Caviglione L., Meier M. Hidden and uncontrolled – on the emergence of network steganographic threats // Proc. ISSE 2014 Securing Electronic Business Processes. 2014. P. 123–133. doi: 10.1007/978-3-658-06708-3_9
11. Fridrich J. Applications of data hiding in digital images // Proc. 5th Int. Symposium on Signal Processing and its Applications. Brisbane, Australia, 1999. V. 1. 9 p. doi: 10.1109/isspa.1999.818099
12. Casner S., Frederick R., Jacobson V., Schulzrinne H. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. Network Working Group, 2003. 25 p.
13. Servetto S.D., Vetterli M. Communication using phantoms: covert channels in the Internet // Proc. IEEE Int. Symposium on Information Theory. Washington, 2001. doi: 10.1109/isit.2001.936092
14. Cabuk S., Brodley C., Shields C. IP covert timing channels: design and detection // Proc. 11th ACM Conference on Computer and Communications Security. New York, 2004. P. 178–187. doi: 10.1145/1030083.1030108
15. Houmansadr A., Borisov N. CoCo: coding-based covert timing channels for network flows // Lecture Notes in Computer Science. 2011. V. 6958. P. 314–328. doi: 10.1007/978-3-642-24178-9_22
16. Panneton F., L'Ecuyer P. On the Xorshift random number generators // ACM Transactions on Modeling and Computer Simulati. 2005. V. 15. N 4. P. 346–361. doi: 10.1145/1113316.1113319

References

1. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? *International Journal of Security and Its Applications*, 2017, vol. 11, no. 4, pp. 71–84. doi: 10.14257/ijsia.2017.11.4.06
2. Karas M., Mazurczyk W., Szczypiorski K. SkyDe: a Skype-based steganographic method. *International Journal of Computers, Communications & Control*, 2014, vol. 8, no. 3, pp. 432–443. doi: 10.15837/ijccc.2013.3.469
3. Janicki A., Karas M., Mazurczyk W., Szczypiorski K. YouSkyde: information hiding for Skype video traffic. *Multimedia Tools and Applications*, 2016, vol. 75, no. 21, pp. 13521–13540. doi: 10.1007/s11042-015-2740-0
4. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*. Wiley, 2016, 296 p.
5. Dyatlov A., Castro S. *Exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the http protocol*. Technical Report. Gray World, 2003, 8 p.
6. Rowland C.H. Covert channels in the TCP/IP protocol suite. *First Monday,* 1997, vol. 2, no. 5, 15 p. doi: 10.5210/fm.v2i5.528
7. Lewis S., Murdoch S.J. Embedding covert channels into TCP/IP. *Lecture Notes in Computer Science*, 2005, vol. 3727, pp. 247–261. doi: 10.1007/11558859_19
8. Berk V., Cybenko G., Giani A. Detection of covert channel encoding in network packet delays. *Technical Report TR 2005-536*. Dartmouth College, 2005, 11 p.
9. Gianvecchio S., Wang H., Wijesekera D., Jajodia S. Model-based covert timing channels: automated modeling and evasion. *Lecture Notes in Computer Science*, 2008, vol. 5230, pp. 211–230. doi: 10.1007/978-3-540-87403-4_12
10. Wendzel S., Mazurczyk W., Caviglione L., Meier M. Hidden and uncontrolled – on the emergence of network steganographic threats. *Proc. ISSE 2014 Securing Electronic Business Processes*, 2014, pp. 123–133. doi: 10.1007/978-3-658-06708-3_9
11. Fridrich J. Applications of data hiding in digital images. *Proc. 5th Int. Symposium on Signal Processing and its Applications*. Brisbane, Australia, 1999, vol. 1, 9 p. doi: 10.1109/isspa.1999.818099
12. Casner S., Frederick R., Jacobson V., Schulzrinne H. *RFC 3550. RTP: A Transport Protocol for Real-Time Applications*. Network Working Group, 2003, 25 p.
13. Servetto S.D., Vetterli M. Communication using phantoms: covert channels in the Internet. *Proc. IEEE Int. Symposium on Information Theory*. Washington, 2001. doi: 10.1109/isit.2001.936092
14. Cabuk S., Brodley C., Shields C. IP covert timing channels: design and detection. *Proc. 11th ACM Conference on Computer and Communications Security*. New York, 2004, pp. 178–187. doi: 10.1145/1030083.1030108
15. Houmansadr A., Borisov N. CoCo: coding-based covert timing channels for network flows. *Lecture Notes in Computer Science*, 2011, vol. 6958, pp. 314–328. doi: 10.1007/978-3-642-24178-9_22
16. Panneton F., L'Ecuyer P. On the Xorshift random number generators. *ACM Transactions on Modeling and Computer Simulati*, 2005, vol. 15, no. 4, pp. 346–361. doi: 10.1145/1113316.1113319

Авторы

Шипулин Павел Михайлович – инженер-программист, АО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва», г. Железногорск Красноярского края, 662972, Российская Федерация; аспирант, Сибирский федеральный университет, Красноярск, 660041, Российская Федерация, ORCID ID: 0000-0002-1211-078X, pshipulin@gmail.com

Козин Виталий Витальевич – студент, Сибирский федеральный университет, Красноярск, 660041, Российская Федерация, ORCID ID: 0000-0002-1063-4889, noxed@mail.ru

Шниперов Алексей Николаевич – кандидат технических наук, заведующий лабораторией, Сибирский федеральный университет, Красноярск, 660041, Российская Федерация, Scopus ID: 57193225757, ORCID ID: 0000-0003-4231-9805, ashniperov@sfu-kras.ru

Authors

Pavel M. Shipulin – software development engineer, Academician M.F. Reshetnev Information Satellite Systems, Zheleznogorsk, Krasnoyarsk region, 662972, Russian Federation; postgraduate, Siberian Federal University, Krasnoyarsk, 660041, Russian Federation, ORCID ID: 0000-0002-1211-078X, pshipulin@gmail.com

Vitaliy V. Kozin – student, Siberian Federal University, Krasnoyarsk, 660041, Russian Federation, ORCID ID: 0000-0002-1063-4889, noxed@mail.ru

Alexey N. Shniperov – PhD, Head of laboratory, Siberian Federal University, Krasnoyarsk, 660041, Russian Federation, Scopus ID: 57193225757, ORCID ID: 0000-0003-4231-9805, ashniperov@sfu-kras.ru