УДК 004.056.53
DOI: 10.22213/2410-9304-2024-3-78-84

Способы организации и выявления стеганографических каналов в IP-сетях

А. А. Каринцев, студент, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия
Д. В. Ардашев, кандидат технических наук, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия

Статья посвящена обзору методов сетевой стеганографии, которые могут быть использованы для построения скрытых каналов передачи сообщений в IP-сетях, а также методов, направленных на выявление таких скрытых каналов. В статье дано понятие стегоконтейнера, приведена классификация методов сетевой стеганографии. В статье рассматриваются следующие методы организации скрытых каналов: метод изменения содержимого заголовков сетевых пакетов, метод Transcoding Steganography (TranSteg), метод модуляции задержкой, метод Lost Audio Packet Steganography (LACK), метод Retransmission Steganography (RSTEG). В обзоре метода изменения содержимого заголовков сетевых пакетов рассмотрен принцип реализации изменений значений в некоторых служебных полях заголовков пакетов протоколов IP (Internet Protocol) и TCP (Transmission Control Protocol), которые не приводят к сбою в передаче данных. В обзоре метода TranSteg рассмотрен принцип перекодировки содержимого сетевых пакетов, доставляющих realtime трафик, с целью освобождения пространства в пакете, которое будет использоваться для передачи скрытой информации. В обзоре метода модуляции задержкой рассмотрены принципы скрытого кодирования сообщений, которое осуществляется с помощью изменения величины задержки отправки пакетов в сети. В обзоре метода LACK рассмотрен механизм преднамеренного удержания RTP-пакетов со встроенным стеганографическим сообщением. В обзоре метода RSTEG рассмотрен принцип осуществления обмена TCP-сегментами, обеспечивающий возможность передачи стеганограммы. Приведен ряд параметров, по которым можно сделать вывод о наличии в сети скрытого канала. Рассмотрена применимость статистических методов и методов с классификатором для обнаружения скрытых каналов в IP-сетях. Обозначена целесообразность реализации статистических методов и методов с классификатором в интеграции с системами захвата и анализа сетевого трафика.

Ключевые слова: стеганография, сетевая, протокол, модификация, анализ, статистический, вектор, опорный.

Введение

Актуальным направлением развития систем защиты информации является разработка средств поиска и блокирования скрытых каналов передачи информации, реализуемых с помощью различных стегоконтейнеров – объектов, используемых для скрытого внедрения информационных сообщений, например графических файлов [1]. Своевременное обнаружение каналов передачи скрытых сообщений является важным фактором эффективности систем предотвращения утечки информации.

Одним из способов организации скрытой передачи информации является сетевая стеганография [2]. Методы сетевой стеганографии эксплуатируют особенности функционирования протоколов передачи данных, используемых в компьютерных сетях. В качестве стегоконтейнера, используемого для скрытой передачи информации, могут выступать различные поля пакетов протоколов передачи данных.

Методы сетевой стеганографии можно классифицировать по трем группам:

- методы, которые модифицируют содержимое пакетов сетевых протоколов (содержимое полей заголовков и данных);
- методы, которые модифицируют структуру передачи пакетов сетевых протоколов, например влияя на порядок передачи пакетов, изменяя временную задержку передачи или создавая преднамеренные потери пакетов;
- гибридные методы, которые комбинируют вышеперечисленные методы.

Учитывая тот факт, что межсетевой протокол IP (Internet Protocol) является сегодня основным протоколом сетевого уровня в современных сетях передачи данных, целями написания настоящей статьи являются: обобщение информации об основных способах организации сетевых стеганографических каналов, которые применимы к протоколам передачи данных в IP-сетях; обзор методов обнаружения сетевых стеганографических каналов в IP-сетях.

Обзор методов сетевой стеганографии

Разберем некоторые из реализаций методов стеганографии в IP-сетях.

1. **Метод изменения содержимого заголовков сетевых пакетов –** это метод, основанный на возможности изменения значений в некоторых служебных полях заголовков протоколов IP и TCP (Transmission Control Protocol), которые не приводят к сбою в передаче данных.

Вначале рассмотрим структуру заголовка IP-пакета, используемую в версии 4 протокола IP (рис. 1).

Структура заголовка IPv4-пакета описана в технической спецификации RFC 791 (Internet Protocol. URL: https://www.ietf.org/rfc/rfc791.txt, дата обращения 03.02.2024).

Поле Identification обладает одним свойством: ему присваивается некоторое уникальное (для отправителя пакета) значение. Поскольку данное поле необходимо только для того, чтобы правильно собрать фрагменты дейтаграммы, то можно предположить, что для нефрагментированного пакета оно может быть каким угодно (в пределах установленной длины – 16 бит).

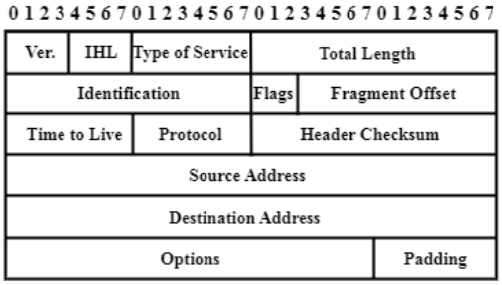

Рис. 1. Структура заголовка IPv4-пакета

Fig. 1. IPv4 packet header structure

Пересчет контрольной суммы заголовка тоже не представляет технических проблем.

Теперь рассмотрим заголовок сегмента транспортного протокола TCP (рис. 2). Информацию о его структуре можно найти в технической спецификации RFC 793 (Transmission Control Protocol. URL: https://www.ietf.org/rfc/rfc793.txt, дата обращения 03.02.2024).

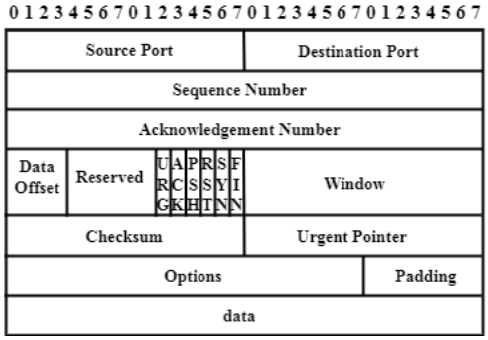

Рис. 2. Структура заголовка TCP-сегмента

Fig. 2. TCP segment header structure

Начальное значение поля Sequence Number (32 бита) устанавливается исходя из значения Initial Sequence Number (ISN), которое генерируется заново каждый раз, когда устанавливается новое соединение по протоколу TCP. Таким образом, при установлении соединения поле Sequence Number не привязано к конкретным значениям и может быть использовано для кодирования символов передаваемого скрытого сообщения.

На рис. 3 представлена схема, описывающая метод создания стеганографического канала, построенного на базе протоколов TCP и IP.

Данный метод использует для внедрения скрытого сообщения служебное поле Identification (IP-пакет) и служебное поле Sequence Number (TCP-сегмент).

Следует отметить, что поле Identification можно использовать только в том случае, если IP-пакет не будет фрагментирован. Поэтому, используя данный метод стеганографии, необходимо либо запрещать фрагментирование пакета, что может привести к его потере, либо подбирать размер IP-пакета таким образом, чтобы его размер был в пределах некоторого максимального значения, которое будет пропускаться параметром MTU (Maximum Transmission Unit) большинства наиболее распространенных сетевых интерфейсов.

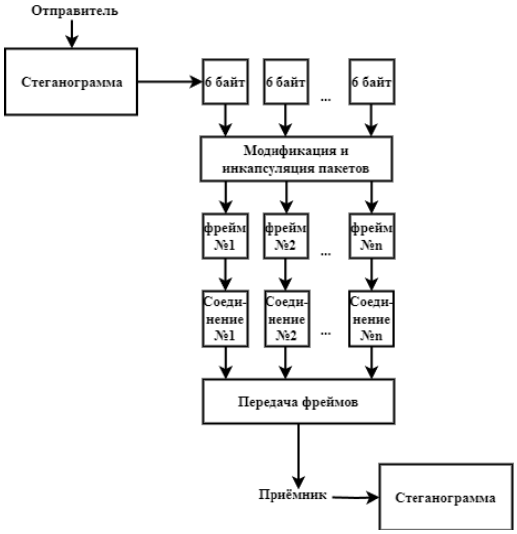

Рис. 3. Схема метода на основе изменения служебных полей TCP/IP

Fig. 3. Diagram of the method based on changing TCP/IP service fields

Принимающая сторона может извлечь значения из нужных полей IP-пакета с помощью программных средств, например, большинством анализаторов сетевого трафика.

В случае применения на сетевом уровне протокола IP версии 6 (рис. 4) в заголовке отсутствует поле Identification, но присутствует 20-битное поле Flow Label (метка потока), которое может использоваться отправителем для маркировки последовательностей IP-пакетов, для которых он запрашивает специальные условия пересылки и обработки. Например, различные сервисы «реального времени» могут использовать различные метки потока.

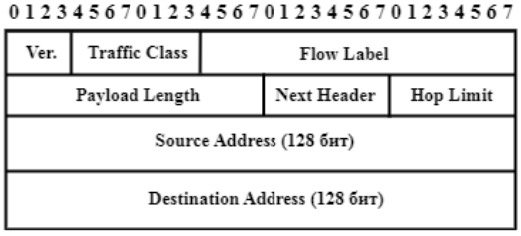

Рис. 4. Структура заголовка IPv6-пакета

Fig. 4. IPv6 packet header structure

Узлы сети (хосты или маршрутизаторы), которые не поддерживают обработку поля метки потока, согласно технической спецификации RFC 2460 (Internet Protocol, Version 6 (IPv6) Specification. URL: https://www.ietf.org/rfc/rfc2460.txt, дата обращения 12.03.2024), должны:

- в своих IP-пакетах устанавливать нулевое значение в это поле;
- в пересылаемых IP-пакетах оставлять это поле неизменным;
- в получаемых IP-пакетах игнорировать это поле.

Исходя из особенностей использования поля «Flow Label», целесообразно предположить, что в протоколе IP версии 6 можно использовать это поле (по аналогии

с полем Identification в протоколе IP версии 4) для размещения стеганографической информации.

Кроме того, в качестве стегоконтейнера могут быть использованы опции IP-пакета, например опция Timestamp [3].

2. **Метод TranSteg (Transcoding Steganography)** – это метод модификации сетевых пакетов, применяющийся для построения стеганографического канала в сетях с использованием протокола RTP (Real-time Transport Protocol) и в других сетевых протоколах, где возможно сжатие данных с потерями.

Метод TranSteg использует возможность перекодировки информации с потерями, чтобы уменьшить размер исходных (легальных) данных и освободить место для стеганограммы. В случае протокола RTP при использовании метода TranSteg анализируется поле PT (Payload Type) RTP-пакета и определяется кодек (далее – codec1), используемый для кодирования передаваемых, например, аудиоданных. Затем выбирается новый кодек (далее – codec2), который должен обеспечить приемлемый уровень качества воспроизведения аудиоданных при распаковке на принимающей стороне и обеспечить более высокую степень сжатия передаваемых данных. Далее данные в RTP-пакете перекодируются с использованием codec2, а на освободившееся место записывается стеганограмма (рис. 5) [4–6].

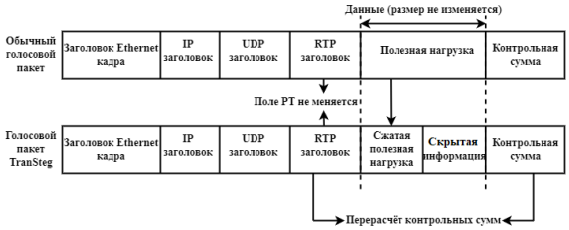

Рис. 5. Изменение кадра TranSteg

Fig. 5. Changing the TranSteg frame

Когда модифицированный RTP-пакет доходит до принимающей стороны, из сообщения извлекается стеганограмма (рис. 6) и производится распаковка сжатых данных с помощью codec2.

Таким образом, принимающая сторона извлекает из поля данных RTP-пакета скрытое сообщение, реализуя стеганографический канал и не нарушая основной процесс передачи данных.

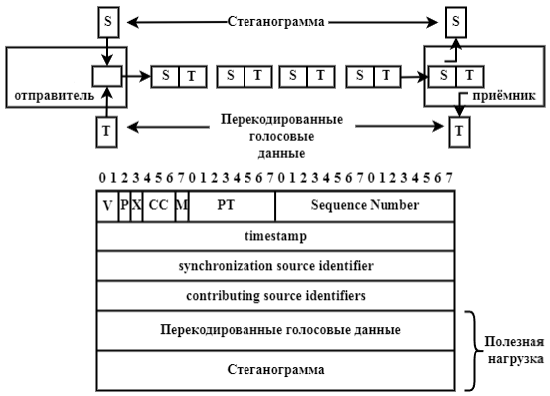

Рис. 6. Сценарий использования TranSteg

Fig. 6. TranSteg Usage Scenario

3. Метод модуляции задержкой – это метод, основанный на возможности изменения времени ожидания между передачей последовательных сетевых пакетов. Например, для реализации передачи двоичного кода можно ввести следующие условия, что короткая временная задержка между двумя последовательными пакетами кодирует двоичный ноль, а более длительная временная задержка кодирует двоичную единицу или наоборот.

Для расширения набора передаваемых символов или чисел стороны должны иметь согласованную таблицу кодировок этих символов, т. е. какой временной задержкой кодируется тот или иной символ (рис. 7) [7].

Особенность данного метода заключается в том, что на практике каналы передачи данных не являются идеальными. Сторонам обмена придётся выбрать систему кодировки, наиболее подходящую для конкретных условий передачи, которая минимизирует количество возможных ошибок и обеспечит приемлемую скорость передачи данных.

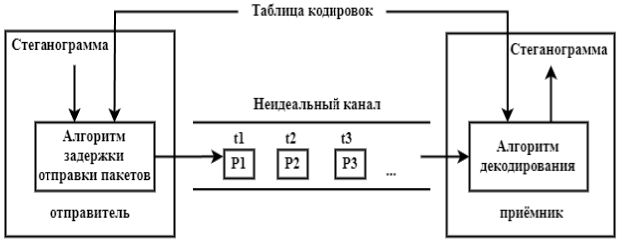

Рис. 7. Схема скрытого канала, работающего на межпакетных задержках

Fig. 7. Diagram of a hidden channel operating on inter-packet delays

4. Метод LACK (Lost Audio Packet Steganography) – это метод, основанный на использовании особенности протокола RTP [8].

Протокол RTP обеспечивает передачу трафика реального времени, и, если доставка RTP-пакета осуществляется дольше, чем это предусмотрено протоколом, данный пакет отбрасывается принимающей стороной. Таким образом, потеря RTP-пакетов может не вызвать подозрений при анализе сетевого трафика, если уровень потерь будет укладываться в норму (<1 % от общего RTP-трафика) [9].

Метод LACK использует механизм преднамеренного удержания RTP-пакетов со встроенным стеганографическим сообщением (рис. 8).

На принимающей стороне такой пакет будет обработан по одному из двух сценариев:

- если принимающая сторона не знает о скрытом сообщении, пакет будет отброшен;
- если принимающая сторона знает о скрытом сообщении, из пакета будет извлечено это сообщение.

Поскольку модифицированный пакет не учитывается в общем потоке, его полезная нагрузка может быть полностью заменена скрытым сообщением. Это повышает пропускную способность скрытого канала по сравнению с аналогичным, строящимся на основе метода TranSteg.

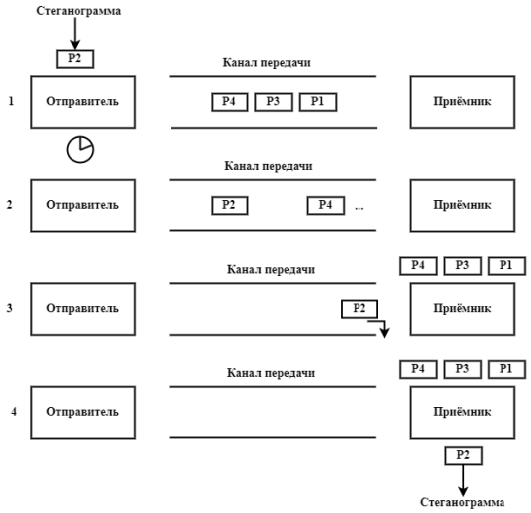

Рис. 8. Принцип работы метода LACK

Fig. 8. The principle of operation of the LACK method

5. **Метод RSTEG (Retransmission Steganography)** – это метод, который использует особенность протокола TCP, он заключается в том, что принимающая сторона должна подтвердить отправителю, что TCP-сегмент был получен. Если передающая сторона в течение определенного времени не получит подтверждение от принимающей стороны, то отправителем будет выполнена повторная отправка потерянного или искаженного TCP-сегмента (рис. 9) [10].

При использовании RSTEG между отправителем и получателем внешне происходит стандартный обмен TCP-сегментами. Но если принимающая сторона готова принять скрытое сообщение, то отправитель (после передачи очередного сегмента) не получает подтверждение ACK. По истечении времени, установленного протоколом TCP, на стороне отправителя начинается процесс повторной передачи последнего отправленного сегмента, но полезная нагрузка будет заменена байтами стеганограммы. Принимающая сторона получает данный пакет, извлекает из него скрытое сообщение и отправляет подтверждение отправителю.

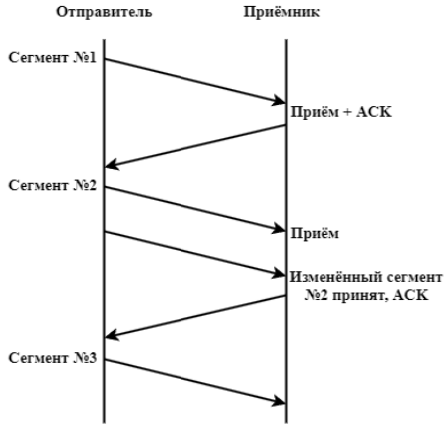

Рис. 9. Принцип работы метода RSTEG

Fig. 9. The principle of operation of the RSTEG method

Так как повторная отправка TCP-сегментов чаще всего связана с загруженностью сети, то количество повторных TCP-сегментов, отправленных в рамках реализации метода RSTEG, не должно значительно увеличивать среднестатистический показатель числа ошибок, возникающих при передаче TCP-сегментов в конкретной сети, чтобы не затруднить работу протокола TCP, снижение размера TCP-окна [11] и не вызвать подозрений у стороннего наблюдателя.

Также необходимо отметить, что реализация методов сетевой стеганографии зависит от скоростных характеристик используемой версии протокола IP. Так, протокол IP версии 6 в некоторых случаях имеет худшие скоростные показатели, чем протокол IP версии 4 [12].

Обзор методов обнаружения скрытых каналов

Сетевая стеганография может использоваться злоумышленниками для организации канала утечки конфиденциальной информации во внешнюю сеть, который будет незаметен для систем безопасности, так как будет восприниматься как совокупность легитимных действий пользователя.

Следовательно, существует необходимость в применении методов обнаружения стеганографических каналов, которые можно разделить на две группы методов: статистические методы и методы с классификатором. Далее рассмотрим принципы реализаций этих методов.

Статистические методы – это методы, использующие статистический анализ и опирающиеся на массив данных о пакетах, передаваемых в сети. Есть ряд параметров, по которым можно сделать вывод о наличии в сети скрытого канала:

- количество повторных отправок пакетов;
- распределение задержек пакетов;
- количество отброшенных пакетов;
- энтропия значений полей сетевых пакетов.

В случае энтропии речь идет о вероятности появления определенных значений при генерации случайных данных в полях заголовков (нормальная ситуация) и встраивании стеганограммы (есть скрытый канал).

Метод реализует сравнение двух дампов: первый (контрольный) со случайными значениями полей Sequence Number и Identification заголовков TCP/IP и второй (подозрительный). Для этих дампов рассчитывается энтропия по Шеннону, по приведенной ниже формуле:

$$H(x) = \sum_{i=1}^{n} p_i \log_2 p_i,$$

где $H(x)$ – мера информационной энтропии по Шеннону, n – количество значений поля; p_i – вероятность появления i-го значения.

Далее происходит сравнение двух значений. Как правило, при передаче стеганограммы информационная энтропия по Шеннону уменьшается [13].

Стеганографический канал, реализуемый с помощью метода модуляции задержкой передаваемых пакетов, можно выявить при помощи анализа статистики задержек пакетов в сети.

В сетях передачи данных, в силу особенностей их функционирования, задержки между передачей пакетов являются случайными величинами, т.е. значение времени задержки Δt должно имеет нормальное распределение (рис. 10) [14].

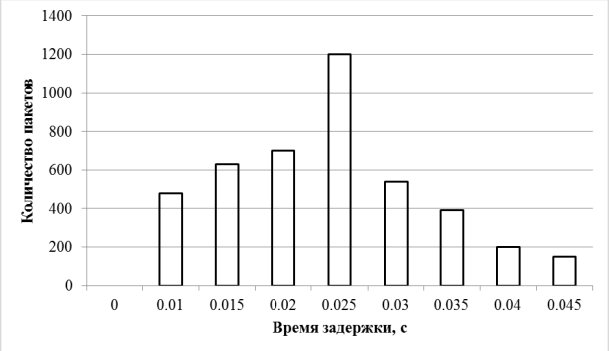

Рис. 10. Нормальное распределение пакетных задержек в сети

Fig. 10. Normal distribution of packet delays in the network

Отклонение Δt от нормального распределения (рис. 11) может свидетельствовать о наличии в сети скрытого канала, так как временные задержки будут сосредоточены вокруг определенной группы различных значений, размер группы значений будет зависеть от размера закодированного алфавита.

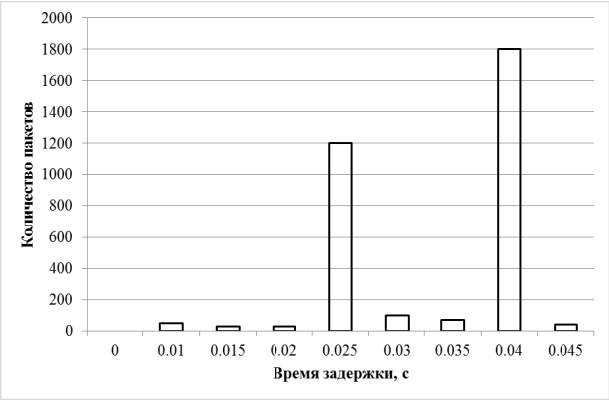

Рис. 11. Отклонение задержек от нормального распределения

Fig. 11. Deviation of delays from the normal distribution

Метод LACK также должен поддаваться статистическому анализу, который должен проводиться по признаку наличия отброшенных или потерянных пакетов. Для проведения статистического анализа можно установить некоторый «нормальный» процент потери пакетов в сети, который должен, как правило, быть меньше 1 %. Если будет замечено, что количество «отброшенных» RTP-пакетов в сети выше установленного процента, то можно предположить, что есть вероятность наличия скрытого канала (см. обзор метода LACK).

Аналогичным образом может производиться анализ метода RSTEG. В качестве наблюдаемого параметра можно рассматривать количество повторно отправленных пакетов (см. обзор метода RSTEG).

Применение статистических методов обнаружения стеганографических каналов предполагает проведение статистического. При проведении статистического анализа, объектом исследования являются статистические данные полученные в том числе в результате наблюдений за трафиком в защищаемой сети. Следовательно, реализацию статистических методов целесообразно выполнять в интеграции с системами захвата и анализа сетевого трафика [15].

Методы с классификатором – это методы, применяющие технологии машинного обучения для классификации пакетов в сети.

Как видно из рис. 12, для классификации пакетов по их характерным признакам (например, поля заголовка) применяется алгоритм машинного обучения – классификатор. В качестве такого алгоритма, например, может быть рассмотрен метод опорных векторов Support Vector Machine (SVM) [16].

Рис. 12. Поиск скрытого канала с использованием классификатора

Fig. 12. Searching for a hidden channel using a classifier

Суть применения метода заключается в том, чтобы максимально точно разбить входящие пакеты на два класса: обычные пакеты и пакеты, которые применяются для передачи стеганограммы.

Применение методов обнаружения стеганографических каналов с классификатором предполагает наличие подготовленных наборов данных (обучающая, тестовая, проверочная выборки). Как и в случае со статистическими методами, подготовка наборов данных может осуществляться на основе информации, полученной в том числе в результате наблюдений за трафиком в защищаемой сети. Следовательно, реализацию и этих методов целесообразно выполнять в интеграции с системами захвата и анализа сетевого трафика.

Выводы

По результатам написания настоящей статьи были сформулированы следующие выводы:

1) методы статистического анализа позволяют обнаружить варианты реализации скрытых каналов в IP-сетях, которые формируют характерные статистические отклонения;

2) методы, опирающиеся на алгоритмы машинного обучения, можно использовать для выявления нехарактерного содержимого сетевых пакетов, классифицировав их по заданному признаку.

3) корректная работа перечисленных методов обнаружения скрытых каналов передачи данных зависит от количества собранных исходных данных, в том числе и в защищаемой сети, поэтому реализацию методов обнаружения скрытых каналов передачи дан-

ных целесообразно выполнять в интеграции с системами захвата и анализа сетевого трафика.

Библиографические ссылки

1. *Гвоздева И. Г., Громов А. С., Гвоздева О. М.* Разработка и реализация метода цифровой стеганографии на основе встраивания псевдоинформации // Труды Института системного программирования РАН. 2023. Т. 35, № 3. С. 63–70. DOI 10.15514/ISPRAS-2023-35(3)-4.

2. *Mazurczyk W., Smolarczyk M., Szczypiorski K.* Retransmission steganography and its detection // Soft Computing. 2011. vol. 15, no 3. pp. 505–515. DOI 10.1007/s00500-009-0530-1.

3. *Punam Bedi, Arti Dua.* Network steganography using the overflow field of timestamp option in an IPv4 packet // Procedia Computer Science. 2020. vol. 171. pp. 1810-1818. DOI 10.1016/j.procs.2020.04.194.

4. *Mazurczyk W., Szaga P., Szczypiorski K.* Using transcoding for hidden communication in IP telephony // Multimedia Tools and Application. 2014. vol. 70, no. 3, pp. 2139-2165. DOI 10.1007/s11042-012-1224-8.

5. *Kheddar H., Megías D.* High capacity speech steganography for the G723.1 coder based on quantised line spectral pairs interpolation and CNN auto-encoding // Applied Intelligence. 2022. vol. 52, pp. 9441–9459. DOI 10.1007/s10489-021-02938-7.

6. *Su Z., Li W., Zhang G. et al.* A steganographic method based on gain quantization for iLBC speech streams // Multimedia Systems. 2020. vol. 26. pp. 223–233. DOI 10.1007/
s00530-019-00624-w.

7. *Коромыслов К. Е.* Исследование способов обнаружения метода сетевой стеганографии, основанного на преднамеренных временных задержках // НИЦ «Л-Журнал». 2021. № 70. С. 38–42. DOI 10.18411/lj-02-2021-09.

8. *Mazurczyk W., Lubacz J.* LACK - a VoIP steganographic method // Telecommunication Systems. 2010. Vol. 45, no. 2-3. Pp. 153-163. DOI 10.1007/s11235-009-9245-y.

9. *Макаренко С. И., Черницкая Т. Е.* Аспекты совместимости сетевых протоколов, интерфейсов и требований по качеству обслуживания в рамках оценки интероперабельности сетецентрических информационно-управляющих систем // Журнал радиоэлектроники. 2020. № 10. DOI 10.30898/1684-1719.2020.10.4.

10. *Artur M. Brodzki, Jedrzej Bieniasz* Yet Another Network Steganography Technique Basedon TCP Retransmissions // ICFSP 2019: 5th International Conference on Frontiers of Signal Processing. 2019. DOI: 10.1109/ICFSP48124. 2019.8938085.

11. *Wojciech Mazurczyk, Miłosz Smolarczyk, Krzysztof Szczypiorski* Retransmission Steganography Applied // 2010 International Conference on Multimedia Information Networking and Security. 2010. DOI: 10.1109/MINES.2010.179.

12. *Бачило В. В., Дравица В. И., Листопад Н. И.* Сравнительный анализ возможностей протоколов IPv6 и IPv4 для обеспечения заданного качества обслуживания // Доклады БГУИР. 2022. Т. 20, № 8. С. 75–83. DOI 10.35596/1729-7648-2022-20-8-75-83.

13. *Красов А. В.* Метод обнаружения сетевой стеганографии на основе статистического распределения полей сетевых пакетов // Издательство «Научные технологии». 2022. № 4. С. 84–91.

14. *Коромыслов К. Е.* Исследование способов обнаружения метода сетевой стеганографии, основанного на преднамеренных временных задержках // НИЦ «Л-Журнал». 2021. № 70. С. 38–42. DOI 10.18411/lj-02-2021-09.

15. *Tomasz Koziak, Katarzyna Wasielewska, Artur Janicki* How to Make an Intrusion Detection System Aware of Steganographic Transmission // EICC '21: Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference. 2021. Pp. 77–82. DOI 10.1145/3487405.3487421.

16. *Гетьман А. И., Иконникова М. К.* Обзор методов классификации сетевого трафика с использованием машинного обучения // Труды ИСП РАН. 2020. Т. 32, № 6. С. 137–154. DOI 10.15514/ISPRAS-2020-32(6)-11.

References

1. Gvozdeva I.G., Gromov A.S., Gvozdeva O.M. [Development and implementation of the digital steganography method based on the embedding of pseudoinformation]. *Trudy Instituta sistemnogo programmirovaniya RAN,* 2023, vol. 35, no. 3, pp. 63-70 (in Russ.). DOI 10.15514/ISPRAS-2023-35(3)-4.

2. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection. *Soft Computing,* 2011, vol. 15, no 3, pp. 505-515. DOI 10.1007/s00500-009-0530-1.

3. Punam Bedi, Arti Dua. Network steganography using the overflow field of timestamp option in an IPv4 packet. *Procedia Computer Science,* 2020, vol. 171, pp. 1810-1818. DOI 10.1016/j.procs.2020.04.194.

4. Mazurczyk W., Szaga P., Szczypiorski K. Using transcoding for hidden communication in IP telephony. *Multimedia Tools and Application,* 2014, vol. 70, no. 3, pp. 2139-2165. DOI 10.1007/s11042-012-1224-8.

5. Kheddar H., Megías D. High capacity speech steganography for the G723.1 coder based on quantised line spectral pairs interpolation and CNN auto-encoding. *Applied Intelligence,* 2022, vol. 52, pp. 9441–9459. DOI 10.1007/s10489-021-02938-7.

6. Su Z., Li W., Zhang G. et al. A steganographic method based on gain quantization for iLBC speech streams. *Multimedia Systems,* 2020, vol. 26, pp. 223–233. DOI 10.1007/s00530-019-00624-w.

7. Koromyslov K.E. [Investigation of ways to detect a network steganography method based on deliberate time delays]. *NITs «L-Zhurnal»*, 2021, no 70, pp. 38-42 (in Russ.). DOI 10.18411/lj-02-2021-09.

8. Mazurczyk W., Lubacz J. LACK—a VoIP steganographic method. *Telecommunication Systems,* 2010, vol. 45, no. 2-3, pp. 153-163. DOI 10.1007/s11235-009-9245-y.

9. Makarenko S.I., Chernitskaya T.E. [Aspects of compatibility of network protocols, interfaces and quality of service requirements in the framework of assessing the interoperability of network-centric information management systems]. *Zhurnal radioelektroniki*, 2020, no. 10 (in Russ.). DOI 10.30898/1684-1719.2020.10.4.

10. Artur M. Brodzki, Jedrzej Bieniasz Yet Another Network Steganography Technique Basedon TCP Retransmissions. *ICFSP 2019: 5th International Conference on Frontiers of Signal Processing,* 2019. DOI: 10.1109/ ICFSP48124.2019.8938085.

11. Wojciech Mazurczyk, Miłosz Smolarczyk, Krzysztof Szczypiorski Retransmission Steganography Applied. *2010 International Conference on Multimedia Information Networking and Security,* 2010. DOI: 10.1109/MINES.2010.179.

12. Bachilo V.V., Dravitsa V.I., Listopad N.I. [Comparative analysis of the capabilities of IPv6 and IPv4 protocols to ensure a given quality of service]. *Doklady BGUIR,* 2022, vol. 20, no. 8, pp. 75-83 (in Russ.). DOI 10.35596/1729-7648-2022-20-8-75-83.

13. *Krasov A.V.* [A method for detecting network steganography based on the statistical distribution of network

packet fields]. *Izdatel'stvo «Nauchnye tekhnologii»*, 2022, no 4, pp. 84-91 (in Russ.).

14. Koromyslov K.E. [Investigation of ways to detect...]. *NITs «L-Zhurnal»*, 2021, no 70, p. 40 (in Russ.).

15. Tomasz Koziak, Katarzyna Wasielewska, Artur Janicki How to Make an Intrusion Detection System Aware of Steganographic Transmission. *EICC '21: Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference,* 2021, pp. 77–82. DOI 10.1145/3487405.3487421.

16. Get'man A.I., Ikonnikova M.K. [An overview of methods for classifying network traffic using machine learning]. *Trudy ISP RAN,* 2020, vol. 32, no. 6, pp. 137-154 (in Russ.). DOI 10.15514/ISPRAS-2020-32(6)-11.

* * *

Ways to Organize and Identify Steganographic Channels in IP Networks

A. A. Karintsev, Student, Kalashnikov Izhevsk State Technical University, Izhevsk, Russia
D. V. Ardashev, PhD in Engineering, Kalashnikov Izhevsk State Technical University, Izhevsk, Russia

The article is devoted to an overview of network steganography methods that can be used to build hidden message transmission channels in IP networks, as well as methods aimed at identifying such hidden channels. The article gives the concept of a stegocontainer, and provides classification of network steganography methods. The article discusses the following methods of organizing hidden channels: the method of changing the contents of network packet headers, the Transcoding Steganography (TranSteg) method, the delay modulation method, the Lost Audio Packet Steganography (LACK) method, the Retransmission Steganography (RSTEG) method. In the review of the method of changing the contents of network packet headers, the principle of implementing changes in values in some service fields of IP (Internet Protocol) and TCP (Transmission Control Protocol) packet headers, which do not lead to data transmission failure, are considered. In the overview of the TranSteg method, the principle of transcoding the contents of network packets delivering real-time traffic is considered in order to free up space in the packet, which will be used to transmit hidden information. In the review of the delay modulation method, the principles of hidden message encoding are considered, which is carried out by changing the delay value of sending packets in the network. In the review of the LACK method, the mechanism of deliberate retention of RTP packets with an embedded steganographic message is considered. In the review of the RSTEG method, the principle of TCP segment exchange is considered, which provides the possibility of transmitting a steganogram. A number of parameters are given by which it is possible to conclude that there is a hidden channel in the network. The applicability of statistical methods and the methods with a classifier for detecting hidden channels in IP networks is considered. The expediency of implementing statistical methods and methods with a classifier in integration with systems for capturing and analyzing network traffic is indicated.

Keywords: steganography, network, protocol, modification, analysis, statistical, vector, support.

Получено: 26.04.24

Образец цитирования

Каринцев А. А., *Ардашев Д. В.* Способы организации и выявления стеганографических каналов в IP-сетях // Интеллектуальные системы в производстве. 2024. Т. 22, № 3. С. 78–84. DOI: 10.22213/2410-9304-2024-3-78-84.

For Citation

Karintsev A.A., Ardashev D.V. [Ways to organize and identify steganographic channels in ip networks]. *Intellektual'nye sistemy v proizvodstve.* 2024, vol. 22, no. 3, pp. 78-84. DOI: 10.22213/2410-9304-2024-3-78-84.