

ИССЛЕДОВАНИЕ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ ИЗМЕНЕНИЯ ДАННЫХ В ПОЛЯХ ПОЛЕЗНОЙ НАГРУЗКИ ПАКЕТОВ

Смирнова Галина Андреевна

студентка

Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А.Бонч-Бруевича, г.Санкт-Петербург

Аннотация. В статье приведена классификация существующих методов сетевой стеганографии. Наиболее подробно проанализированы методы сетевой стеганографии на основе изменения данных в полях полезной нагрузки пакетов. Приводится сравнительная характеристика рассматриваемых методов.

Ключевые слова: сетевая стеганография, TranSteg, RSTEG.

Ввиду бурного развития сетевых коммуникаций возрастает и количество передаваемой при их помощи информации, поэтому все большее внимание уделяется обеспечению конфиденциальности данных, которые передаются по сети. Подобного рода задачи решаются при помощи достижений криптографии и стеганографии. Криптография скрывает содержимое сообщения, при этом сохраняет возможность обнаружить факт ее использования, а стеганография скрывает этот факт. Принимая во внимание то, что зашифрованное не скрытое сообщение привлекает к себе повышенное внимание, применение стеганографии имеет явное преимущество.

Задачу скрытой передачи данных по сетям связи в режиме реального времени успешно решают методы сетевой стеганографии, при которой сообщения скрываются непосредственно в сетевых потоках, в качестве носителей секретной информации использует сетевые протоколы эталонной модели OSI.

Основной целью данной статьи является рассмотрение существующей классификации методов сетевой стеганографии. Наиболее подробно проанализировать методы сетевой стеганографии на основе изменения данных в полях полезной нагрузки пакетов. Сравнительные характеристики рассматриваемых методов.

Методы сетевой стеганографии можно разделить на три группы:

1. Методы стеганографии, суть которых в изменении данных в полях заголовков сетевых протоколах и в полях полезной нагрузки пакетов;

2. Методы стеганографии, в которых изменяется структура передачи пакетов, например, изменяются очередности передачи пакетов или преднамеренное введение потерь пакетов при их передаче;
3. Смешанные (гибридные) методы стеганографии – при их применении изменяются содержимое пакетов, сроки доставки пакетов и порядок их передачи.

Каждый из этих методов делится еще на несколько групп; например, методы модификации пакетов включают в себя три разных метода:

1. Методы, изменяющие данные в полях заголовков протокола: они основаны на модификации полей сетевых заголовков IP, TCP, SCTP и так далее;
2. Методы, которые изменяют данные в полях полезной нагрузки пакета; в этом случае могут применяться алгоритмы водяных знаков, речевых кодеков и прочих стеганографических техник по скрытию данных;
3. Методы, объединяющие два предыдущих пункта.

Методы модификации структуры передачи пакетов включают в себя три направления:

1. Методы, в которых изменяется порядок следования пакетов;
2. Методы, изменяющие задержку следования пакетов;
3. Методы, суть которых заключается во введении преднамеренной потери пакетов путем пропуска порядковых номеров у отправителя.

Смешанные (гибридные) методы стеганографии изменяют как содержимое пакетов, так сроки доставки пакетов и порядок их передачи. При этом используют два подхода: методы потери аудио пакетов (LACK) и ретрансляция пакетов (RSTEG). [1]

Метод TranSteg

В наше время очень популярны программы, которые обеспечивают голосовую и видеосвязь через сеть Интернет. Из-за этого метод Transcoding Steganography (TranSteg) пользуется большим успехом. Он может использоваться как в IP-телефонии, так и в других приложениях, где существует возможность сжатия открытых данных. TranSteg производит транскодирование исходных данных с потерями для освобождения места под стеганограмму.

Как правило, транскодирование работает следующим образом. RTP пакеты просматриваются и анализируются. Кодек, первоначально используемый для кодирования речи (здесь называемый открытым), определяется путем проверки поля PT (Payload Type) в заголовке RTP. TranSteg выбирает так называемый скрытый кодек. Его применение обеспечивает сопоставимое качество голоса и меньший размер голосовой нагрузки. Голосовой поток транскодируется (при использовании скрытого кодека) в меньший размер и помещается в исходное поле полезной нагрузки, при этом первоначальный размер и индикатор типа кодека

(поле PT) остается без изменений. Оставшееся свободное пространство заполняется стеганограммой.

Метод RSTEG

RSTEG использует механизм повторной передачи. Естественно отправитель и получатель знают о стеганографической процедуре. В некоторый момент времени после успешного приема пакета получатель преднамеренно не выдает подтверждающее сообщение. В обычной ситуации отправитель обязан повторно передать потерянный пакет, когда истекает период времени, в течение которого должно было быть получено подтверждение пакета. В контексте RSTEG отправитель заменяет исходную полезную нагрузку стеганограммой вместо повторной отправки того же пакета. Когда повторно переданный пакет достигает приемника, извлекается скрытая информация. При следующем срабатывании данного механизма посылается оригинальный пакет без скрытых вложений, на который приходит пакет с подтверждением об удачном получении.

В статье «Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи» [2] приведено сравнение методов по их основным характеристикам и реализации. В рамках данной статьи количество методов было сокращено до двух исследуемых и их сравнение приведено в табл.1. Чем выше отображен метод в таблице, тем больше показатели его характеристик. В поле Реализация рассматривается простота организации данного метода. Чем меньше времени и усилий требует реализация данного метода, тем выше его позиция данным заголовком. [2]

Таблица 1. Сравнение методов TranSteg и RSTEG

№	Пропускная способность	Сложность обнаружения	Стоимость стеганографии	Реализация
1	TranSteg	TranSteg	RSTEG	TranSteg
2	RSTEG	RSTEG	TranSteg	RSTEG

Анализируя данные из таблицы, можно сделать вывод о прямой зависимости основных характеристик друг от друга.

В заключении хотелось отметить, что каким бы ни был метод, скрытая информация может быть потенциально обнаружена. Как правило, чем больше скрытой информации вставляется в поток данных, тем выше вероятность того, что она будет обнаружена.

Список литературы:

1. Белкина Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности // Молодой ученый. — 2018. — №11. — С. 36-44. — URL <https://moluch.ru/archive/197/48821/> (дата обращения: 10.05.2019).

2. О. Ю. Пескова, Ю. Г. Халабурда. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия Южного федерального университета. Технические науки. — 2012. —С. 172