УДК 004.056

Мустафаева Э.А.

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ ОТ ХАРАКТЕРИСТИК СКРЫВАЕМОЙ ИНФОРМАЦИИ

Институт систем управления НАН Азербайджана

mustafayevaesmira@yahoo.com

Введение

Стеганографические системы строятся путем использования таких компонентов, как конфиденциальная информация, контейнеры, алгоритмы внедрения и скрытые каналы передачи. Естественно, эффективность стеганографической системы зависит от характеристик этих компонентов, поэтому при их построении необходимо учитывать ряд важных факторов.

Прежде всего отметим, что для того, чтобы обеспечить скрытую передачу конфиденциальной информации по открытому (например, по интернет и по обычной почте) каналу с помощью стеганографической системы требуется выбрать соответствующий контейнер и алгоритм сокрытия. Выбранный алгоритм должен предоставить возможность сокрытия конфиденциальной информации в контейнере таким образом, чтобы внесенные при этом изменения в контейнере не были заметными (хотя бы были незаметными с большой вероятностью) для посторонних лиц.

При выборе контейнера необходимо учитывать объем, формат и форму представления и т.д. скрываемой информации. Далее определяется соответствующий алгоритм сокрытия в зависимости от характеристик скрываемой информации и выбранного контейнера. После того, как информация была внедрена в контейнер, определяется канал (например, социальная сеть, электронная почта, облако и т.д.) для скрытой доставки стего-контейнера в адрес назначения.

С учетом вышеизложенного, в настоящей статье исследуется зависимость эффективности стеганографических систем от таких характеристик скрываемой (конфиденциальной) информации и контейнера, как объем, формат, форма представления и назначение, а также каналов передачи стегоконтейнера. В статье также рассматриваются проблемы правильного выбора контейнеров, алгоритмов внедрения информации и каналов скрытой передачи в зависимости от характеристик скрываемой конфиденциальной информации.

Стеганографическая система и предъявляемые к ней требования

Набор методов и средств, используемых для создания канала скрытой передачи информации, называется стеганографической системой (стегосистемой), а такой канал называют стеганографическим каналом (стегоканалом).

Цель стеганосистемы – не только ограничить доступ к контейнеру, в котором скрыта информация, но и предоставить значительную гарантию того, что информация, скрытая в контейнере, будет доставлена по адресу без повреждений, без подделки и с возможностью восстановления.

В целом стеганографическая система – это комплекс, состоящий из следующих элементов: конфиденциальная информация, контейнер для ее сокрытия, алгоритмы скрытия информации в контейнере и извлечения ее оттуда, стеганографический ключ и стегоканалы для их передачи (рис.1).

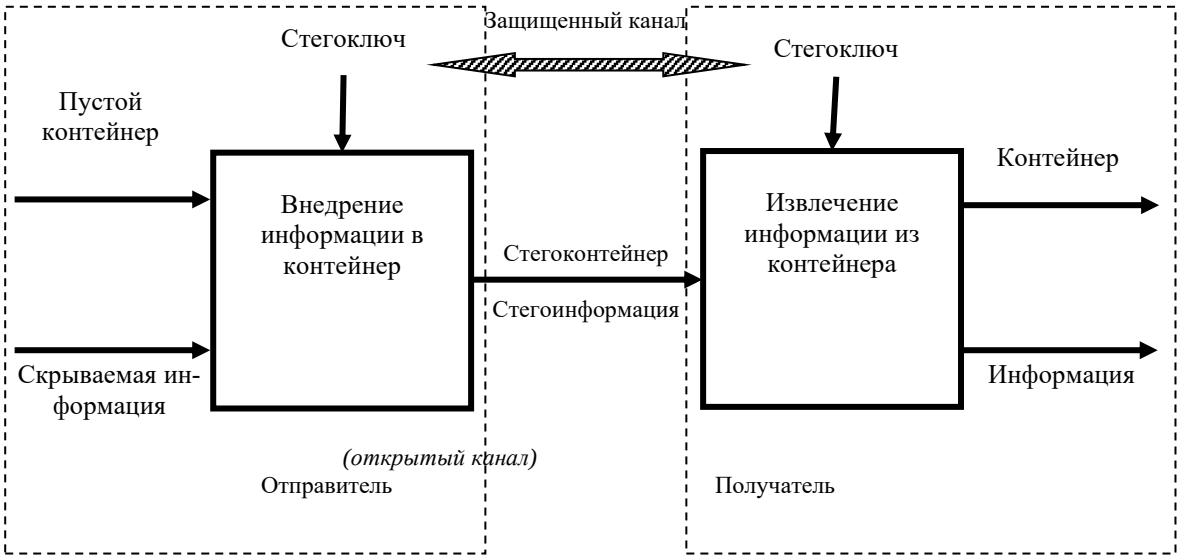

Рис. 1. Концептуальная модель стеганографической системы

Одним из основных требований к стеганографическим системам, занимающимся скрытой передачей конфиденциальной информации и безопасной доставкой по адресу, является вопрос надежности. Как правило, к стеганографическим системам предъявляются следующие требования:

- надежное размещение конфиденциальной информации в контейнере;
- возможность внедрения в контейнер конфиденциальной информации любого типа, независимо от формата и формы представления;
- устойчивость к изменению стегоконтейнера, содержащего конфиденциальную информацию;
- скрываемая в стегоконтейнера информация не должна быть потеряна и искажена при передаче;
- минимизация возможности обнаружения и захвата стегоконтейнера;
- невозможность извлечения конфиденциальной информации при захвате стегоконтейнера;
- возможность использовать стеганографический ключ;
- возможность реализации надежного канала передачи и неосуществление прямой передачи стегоконтейнера по адресу назначения.

Список требований к стеганографическим системам можно продолжить. Это говорит о том, что стеганографические системы должны обладать свойствами, способными отвечать тем или иным подобным требованиям. В связи с этим надежность стеганографических систем напрямую зависит от принципов ее построения.

Зависимость стегосистемы от характеристик скрываемой информации

Под характеристиками скрываемой информации понимаются ее объем, формат, форма представления, назначение и т.д. Для большинства современных стеганографических методов существует прямая зависимость между надежностью системы и объемом скрываемой информации (рис.2). По мере увеличения объема скрываемой информации надежность сокрытия значительно снижается.

Можно принять оптимальное решение при выборе между размером (объемом) скрываемой информации и степенью стойкостью стегоконтейнера к возможным стеганографическим анализам. При стеганографическом анализе контейнера путем ограничения степени снижения качества стегоконтейнера, который может быть обнаружен злоумышленником, можно достичь либо увеличения объема вводимой информации, либо повышения ее стойкости к стеганографическим анализам. Однако, невозможно обеспечить высокие

значения обоих этих показателей одновременно. Так как увеличение одного показателя приводит к абсолютному уменьшению другого [1,2].

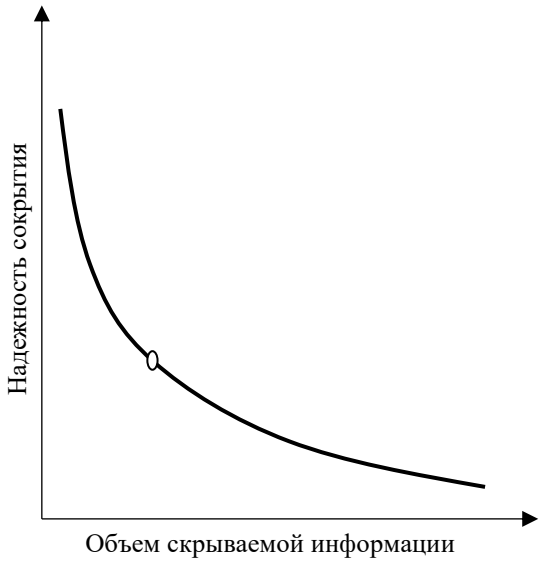

Рис. 2. Зависимость надежности скрываемой информации от ее объема

Под форматом конфиденциальной информации понимается представление ее в виде текста, графики, аудио или видео. Такая информация может быть помещена в контейнер в виде соответствующего файла или короткого сообщения.

Назначение конфиденциальной информации также играет важную роль при создании стеганографических систем. Так как, конфиденциальная информация может выступать в качестве цифровых водяных знаков для защиты авторских прав, идентификационных номеров для защиты интеллектуальной собственности, скрытой в заголовках с целью защиты конфиденциальности, или конфиденциальной информации, передаваемой тайно по открытому каналу. Это зависит от сферы применения стеганографии:

- с целью защиты авторского права над электронными продуктами, предотвращения несанкционированного копирования и использования интеллектуальной собственности эффективно используется скрытая (стего) информация в виде невидимых знаков, то есть цифровых водяных знаков (digital watermarking). Стегоинформация может принадлежать владельцу в виде нескольких аутентичных кодов или носителем управляющей информации в качестве как цифровых водяных знаков.
- с целью предотвращения незаконного тиражирования и контроля за каждым законным экземпляром электронной продукции можно использовать стегоинформацию в качестве цифровых отпечатков пальцев, то есть идентификационных номеров (digital fingerprinting). В отличие от цифровых водяных знаков, идентификационные номера уникальны для каждого номера продукта. Стегоинформация в качестве идентификационного номера позволяет производителю отслеживать свою деятельность в будущем, т.е. производитель может получить информацию о том, занимается ли какой-либо покупатель незаконным оборотом. В случае незаконной деятельности, «цифровые отпечатки пальцев» позволяют определить нарушителя.
- стегоинформация также может быть использовано в качестве заголовков, чтобы сохранить данных, представленных в разных форматах, в единой базе. Например, в больших электронных хранилищах (библиотеках) он используется для разметки цифровых изображений, аудио и видео файлов (подпись медицинских записей, нанесения легенды на карту и т.д.).
- стегосистема в основном используется для скрытой передачи конфиденциальной информации. Конфиденциальная информация помещается внутри любого другого объекта (информации, носителя информации и т.д.) для скрытого (тайного) хранения и передачи [3].
- Как известно, при построении стеганографических систем предъявляются определенные требования. К требованиям, предъявляемым при размещении конфиденциальной информации в контейнер, можно отнести следующие:
- скрываемая информация должна быть устойчива к возможным помехам, сжатиям с потерями, фильтрациям, модификациям, аналого-цифровым и цифро-аналоговым преобразованиям;
- изменения в контейнере при внедрении конфиденциальной информации не

должны достигать той степени, при которой человеческие органы чувств (глаза, уши и т. д.) могут чувствовать (воспринимать) эти изменения;

- попытки удаления (уничтожения) скрываемой информации должны привести к серьезному повреждению контейнера;
- скрываемая информация не должна привести к значительным изменениям статистических параметров контейнера.

Выбор контейнера в зависимости от характеристик конфиденциальной сообщении

В компьютерной стеганографии в качестве контейнеров могут быть использованы различные цифровые объекты, такие как изображения, аудио-видео записи, цифровые носители, а также текстовые файлы и другие электронные документы.

Подавляющее большинство современных стеганографических систем используют в качестве контейнеров растровые графические изображения различных форматов. Очевидно, что лучшим контейнером считается тот, который не вызывает подозрений в процессе передачи. Поэтому при выборе формата на графических изображениях, представленных в качестве контейнеров, недостаточно требовать, чтобы стеганографические системы были устойчивы только к атакам. При этом, чтобы не вызывать сомнений, форматы, используемые в качестве контейнеров, должны быть широко применяемыми на практике и достаточно распространенными. В последнее время наиболее распространенным форматом является формат JPEG. Практически все современные цифровые фото- и видеоустройства хранят изображения в таком формате. Именно в этом формате и находится большинство графических изображений в сети Интернет.

С точки зрения построения стеганографических систем можно отметить следующие отличительные особенности форматов современных графических контейнеров [4]:

- существование изображения в сжатом виде;
- возможность сжатия изображения без потери;
- возможность использования цветовой палитры.

Если формат хранения растровых изображений использует сжатие данных, то разработка стеганографических систем значительно усложняется. Во-первых, усложняется анализ графического формата, а во-вторых, изменения, вносимые в данные изображения стеганографической системой, приводят к нежелательному ухудшению эффективности сжатия. Когда формат графических изображений использует сжатие данных с потерями, классические методы сокрытия информации на графических изображениях, как правило, малоэффективны. Такая потеря может привести к уничтожению скрытой информации. В этом случае сначала следует искать подходящий алгоритм сжатия для сокрытия, а затем адаптировать его к классическим методам или провести детальный анализ разработки новых методов.

Использование форматов графических изображений без сохранения цветовой палитры затрудняет применение классических методов стеганографического сокрытия. В качестве примера можно привести метод сокрытия информации в наименее значимых битах (LSB). Под сокрытием в наименее значимых битах понимается сокрытие информации не в малых битах данных графического изображения, сформированных из элементов палитры, а в малых битах элементов самой палитры, размер которых не превышает 256 цветов. В этом случае, для сокрытия в младших битах элементы палитра должны быть близки к интенсивности цветовых составляющих, что не всегда возможно сделать. В литературе также встречается множество модификаций метода LSB, отличающихся надежностью и стойкостью.

Стеганографические методы сокрытия в возможных областях изображений не устойчивы к большинству типов искажений. Например, использование сжатия с

потерями приводит к частичному или полному разрушению дополнительной информации. Более устойчивыми к различным искажениям, а также сжатию при сокрытии информации являются методы, использующие для сокрытия информации не пространственную область контейнера, а частотную [1].

Другими методами являются методы сокрытия информации в сетевых протоколах, которые относятся к сетевой стеганографии. В этих методах в качестве контейнеров используются такие протоколы Интернета, как TCP, IP, VoIP, SCTP и ICMP. В методах, использующих протоколы TCP/IP в качестве контейнера, выступают пакеты, и информация скрывается в неиспользуемых полях заголовка пакета. Преимущество этого метода заключается в том, что информацию можно передать от отправителя к получателю без изменений и данный метод прост в реализации. А недостаток заключается в ограниченном объема информации, которая может быть вставлена в пакет, а также в том, что передаваемая информация передается открыто и может легко обнаруживаться нарушителем [5,6].

Пакеты VoIP, обеспечивающие голосовую и видеосвязь через интернет, используются в качестве контейнеров для сокрытия данных за счет сжатия полезной нагрузки пакета за счет перекодирования. В качестве недостатка данного метода можно указать сложность его реализации.

Из перечисленных выше методов большой интерес представляют стеганографические методы, использующие возможности протокола SCTP (Stream Control Transmission Protocol). Такой стеганографический метод, основанный на транспортном протоколе управления пакетами, применяется в многопоточной передаче и в режиме множества интерфейсов. Стеганографические методы типа SCTP делятся на 3 вида – скрытая скрытая передача информации основана на изменение содержания пакетов, изменение последовательности передачи пакетов, а также на совместном использовании этих методов. Передача, которая позволяет использовать переменные настройки, а также изменять адреса отправителя и получателя, делает его удобным для стеганографических приложений.

Выбор алгоритма внедрения в зависимости от характеристик скрываемой информации

Следующие алгоритмы внедрения конфиденциальной информации широко используются в стеганографических приложениях [7]:

- сокрытие информации с использованием различных битовых полей;
- сокрытие с использованием структур графических файлов;
- сокрытие в голограммах – голографический подход (цифровые водяные знаки);
- сокрытие в заголовках различного типа файлов;
- сокрытие в наименее важных битах в изображениях (LSB).

На основе известных стеганографических алгоритмов возможно создать усовершенствованных алгоритмов, устойчивых к достаточно разнообразным преобразованиям и визуальному стегоанализу.

При совершенствовании существующих и разработки новых стеганографических алгоритмов необходимо учитывать вышеотмеченные требования. Наиболее важным из них этих требований является стойкость алгоритмов к различным атакам. К таким воздействиям относятся, в частности, наложение различных шумов на стегаданные, сжатие с потерями, фильтрация и др. [8].

Выбор скрытых каналов (стегоканалов) в зависимости от характеристик скрытой информации

Известно, что канал передачи данных состоит из трех составных частей – передатчик (источник сигнала), приемник (получатель сигнала) и канал связи. Естественно, это остается в силе и при создании скрытых каналов в стеганографии.

При этом каналы связи могут быть открытыми или защищенными. Секретный канал можно организовать через существующие открытые или защищенные каналы. Для этого, помимо открытого или защищенного канала, требуется наличие контейнера, который может нести конфиденциальную информацию внутри себя. Как мы уже упоминали выше, в качестве контейнера может выступать обычный текстовой или другой файл, рисунок, графическое изображение, аудио-видео данные, сообщения электронной почты, SMS сообщение, веб-страница, профили пользователей, фрагменты текста и т. д. [1,3,9-12].

В качестве секретного канала передачи (стегоканала) может выступать любая информационная служба и протокол Интернета. Так, на практике для реализации стегоканала часто используют электронную почту, веб, чат, Skype, социальные сети, облака, протоколы TCP/IP, VOIP, HTTP, SCTP.

Были проведены эксперименты и получены положительные результаты по созданию стегоканалов через Facebook, Twitter, Google+, Instagram и другие социальные сети, а также WhatsApp [13].

Как отметили выше, для создания скрытого канала передачи информации можно использовать цифровые объекты (файл, изображение, графическое изображение, аудио, видео, веб-страницу, текст и т.д.) и услуги, позволяющие передать их через Интернет.

Выбор стегоканала прежде всего зависит от характеристик скрываемой информации. Например, если объем скрываемой информации небольшая, то можно использовать стегоканалы онлайн служб – сетевых протоколов интернета, чат, Skype и т.д. Если объем передаваемой информации большая или необходимо передать какой-то файл (текст, рисунок, изображение, таблицу и т.д.), то можно реализовать стегоканал через электронную почту, веб, социальные сети, облачные технологии с использованием стегоалгоритмов на основе текстовых, графических, аудио-видео файлов. Аналогичный выбор стегоканалов можно осуществить согласно форматам, формам представления скрываемой информации.

Далее следует отметить, что одним из важнейших задач при реализации стегоканалов является оценка их пропускной способности. Пропускная способность стегоканалов вычисляется методами теории информации. Пропускная способность скрытых каналов в основном измеряется отношением количества скрываемой информации к количеству информации, легально маскирующей скрытую передачу в контейнере или процессе. Оценка пропускной способности носит асимптотический характер и подход, связанный с ограничением пропускной способности, может оказаться неэффективным в реальных приложениях. Следует отметить, что хотя канал может иметь асимптотическую нулевую пропускную способность, однако через него можно передавать конфиденциальную информацию небольшой длины [11,14].

Заключение

В ходе исследований зависимости между объемом скрываемой информации и степени устойчивости стегоконтейнера к возможному стеганографическому анализу выяснилось, что увеличение одного из них приводит к абсолютному уменьшению другого.

Использование сжатия с потерями в изображениях приводит к частичному или полному уничтожению конфиденциальной информации. Чтобы этого избежать, предлагается реализовать методы, использующие не фазовые поля контейнера, а их частотные поля, которые более устойчивы к различным искажениям, а также к сжатию.

Несмотря на то, что при использовании протоколов TCP, IP, VoIP, SGTP и ICMP в качестве контейнеров является предпочтительным из-за возможности передачи без модификации и простой реализации, однако ограниченность объема скрываемой информации, которая может быть помещена в пакет, а также простота

обнаружения передаваемой информации могут создавать проблемы.

Преимущество использования изображений в качестве контейнеров заключается в том, что они имеют меньшую вычислительную сложность в процессе внедрения и декодирования дополнительной информации в их пространственные части, что приводит к меньшему количеству вычислительных ошибок.

Литература

1. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

2. *Bender W., Gruhl D., Morimoto N., Lu A.* Techniques for Data Hiding, IBM Systems Journal. – 1996. – Vol. 35. – P. 313-336.

3. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

4. *Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.* Стеганография, цифровые водяные знаки и стеганоанализ. – М.: Вузовская книга, 2009. – 220 с.

5. *Qasımov V., Hüseynova G.* Internet protokollarında gizli informasiya ötürmə kanallarının yaradılması imkanları. Journal of Qafqaz University Mathematics and Computer Science. – 2015. – Vol. 3. – № 1. – P. 50-56.

6. *Qasımov V.Ə., Mustafayeva E.Ə.* İnter-netdə informasiyanın gizli ötürülmə kanallarının yaradılması üsulları // "Milli təhlükəsizlik və hərb elmləri" elmi-praktik jurnalı. Azərbaycan Respublikası Silahlı Qüvvələrinin Hərbi Akademiyası. Bakı. – 2016. – №3. – Səh. 122-128.

7. *Горелкина Д.А., Дорошенко Н.С., Осипов Д.Л.* Применение методов цифровой стеганографии для внедрения конфиденциальной информации в растровые изображения. Вестник Ставропольского государственного университета – Технические науки. – 75/2011. – С. 73-77.

8. *Кобозева А.А., Лебедева Е.Ю., Костырка О.В.* Стеганопреобразование пространственной области изображения контейнера, устойчивое к атакам против встроенного сообщения // Problemele energeticii regionale. – 2014. – № 1. – С. 57-65.

9. *Shannon C.E.* A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Т. 27. – С. 379-423, 623-656.

10. *Ahsan K., Kundur D.* Practical Data Hiding in TCP/IP // Proc. ACM Wksp. Multimedia Security. – 2002. – 8 p.

11. *Тимонина, Е.Е.* Скрытые каналы (обзор) // Jet info. – 2002. – № 11. – 20 с.

12. *Johnson N.F., Jajodia S.* "Steganalysis: The investigation of Hidden Information", IEEE Infonnation Technology Conference, Syracuse, NY, USA, 1-3 September 1998. – 4 p.

13. *Gasimov V., Mustafayeva E., Huseynova G.* Implementing covert channels to transfer hidden information over whatsapp on mobile phones. International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661. – February 2019. – Vol. 6. – Iss. 2. – P. 32-35.

14. *Moscowitz I.S., Kang M.H.* Covert Channels Here to Stay?// Information Technology Division Naval Research Laboratory, Washington, DC 20375, 1995. – 21 p.

Мустафаева Э.А.

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ ОТ ХАРАКТЕРИСТИК СКРЫВАЕМОЙ ИНФОРМАЦИИ

Для построения совершенных стеганографических систем необходимо учитывать множество параметров, в том числе их зависимость от характеристик скрываемой информации и канала связи, используемая для секретной передачи. В связи с этим в статье исследуется зависимость стеганографических систем от таких характеристик, как объем, формат, форма представления, назначение скрываемой информации. Предлагаются подходы правильного выбора контейнера, алгоритма внедрения, каналов

скрытой передачи в зависимости от этих характеристик. В ходе исследований зависимости между объемом скрываемой информации и степени устойчивости стегоконтейнера к возможному стеганографическому анализу выяснилось, что улучшение одного из этих показателей приводит к абсолютному ухудшению другого. Кроме того, в статье исследуется устойчивость контейнера и скрываемой в нем информации различным шумам, сжатиям с потерями, фильтрацию, модификацию, аналого-цифровым и цифро-аналоговым преобразованиям для построения совершенных стеганографических систем. Были изложены преимущества и недостатки использования изображений, протоколов TCP, IP, VoIP, SCTP и ICMP, а также пакетов VoIP в качестве контейнера.

Mustafayeva E.A.

RESEARCH OF THE DEPENDENCE OF STEGANOGRAPHIC SYSTEMS ON THE CHARACTERISTICS OF HIDDEN INFORMATION

To build perfect steganographic systems, it is necessary to take into account many paraeters, including their dependence on the characteristics of the hidden information and the communication channel used for secret transmission. In this regard, the article examines the dependence of steganographic systems on characteristics such as volume, format, form of presentation, purpose of hidden information. Approaches are proposed for the correct choice of the container, the implementation algorithm, covert transmission channels, depending on these characteristics. In the course of studies of the relationship between the amount of hidden information and the degree of stegocontainer's resistance to possible steganographic analysis, it was found that an improvement in one of these indicators leads to an absolute deterioration in the other. In addition, the article examines the resistance of the container and the information hidden in it to various noises, lossy compression, filtering, modification, analog-to-digital and digital-to-analog conversions to build perfect steganographic systems. The advantages and disadvantages of using images, TCP, IP, VoIP, SCTP and ICMP protocols, and VoIP packets as a container were outlined.