УДК [004.056+003.26] (075.8)

Студ. Д.В. Савельев
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий)

СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И ДЕТЕКТИРОВАНИЕ СКРЫТЫХ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Сетевые технологии определяют тренды в развитии многих направлений в ИТ [1]. Сейчас наблюдается бум по созданию так называемых систем «умного дома», которые раньше использовали Wi-Fiи Bluetoothдля подключения в общую сеть, а теперь используют специализированный протокол Zigbee.

Все беспроводные локальные сети используют и будут использовать широковещательную сети для связи. Беспроводные сети гораздо более подвержены искажению данных, чем проводные, поэтому использование помех и шумов в среде связи в работе системы представляется весьма привлекательным. Пакеты в беспроводных сетях довольно хорошо защищены, так как «имеют» слишком мало места для встраивания тайного сообщения: всего от 8 до 32 битов.

С созданием пирингового протокола BitTorrent [2] появилось множество сайтов с библиотеками торрентов. С помощью протокола BitTorrent обеспечивается децентрализация сети P2P. С ростом количества узлов росла и скорость загрузки, так как нагрузка распределялась между ними всеми. Распространенность данного протокола благоприятствует его использованию в стеганографических приложениях [1, 3].

В стеганографии принято оперировать такими понятиями как контейнер, сообщение, осаждение, извлечение и скрытый канал. Под контейнером понимают такие цифровые данные, использование избыточности которых позволяет передавать дополнительную информацию, не обнаруживая факта передачи. Совокупность методик и средств встраивания и извлечения дополнительной информации без обнаружения нарушения целостности контейнера позволяет говорить о формировании скрытого канала передачи информации. Стеганографической системой называют совокупность средств и методов передачи и приема пустого контейнера, функционирующих взаимосвязано со средствами и методами, используемыми для создания скрытого канала передачи информации [1, 3].

А теперь подробнее про механизм, который делает возможным реализовать соединение анализируемого протокола со стеганографией. Мы уже определили, что BitTorrent – это пиринговый протокол,

который использует узлы (пиры – peers) для загрузки файлов [2, 4]. В его терминологии узел (пир) – это компьютер, который участвует в загрузке общего ресурса. Для узлов, которые уже загрузили файл, есть свое название – сиды (seeds). Если общий ресурс еще не загружен полностью, то такие пиры называют личами (leech). Чтобы подключиться к BitTorrent-сети, пир загружает сид-файл, достает из него адрес трекера и запрашивает у него список всех пиров. Затем новый пир проводить трехстороннее рукопожатие, которое состоит из следующих этапов [5]:

– отправка рукопожатия;

– ответ на рукопожатие;

– обмен bitfield-сообщениями.

Далее они обмениваются переговорными сообщениями и затем начинается непосредственно передача фрагментов файлов. Ключевой момент в этой схеме – обмен bitfield-сообщениями, структура которых представлена на рис. 1. Bitfield-сообщение служит для информирования пирами друг друга о наличии у себя фрагментов файла общего ресурса. Данное сообщение имеет разную длину в зависимости от размеров загружаемого файла. Дело в том, что при создании торрента, выбирается размер фрагментов, которые будут считать минимальной единицей, которую можно отправлять по сети. Соответственно, количество таких фрагментов, из которых состоит целый файл и будет являться длиной Bitfield-поля. Таким образом, все фрагменты файла имеют свои индексы и если узел владеет каким-либо фрагментом, то по этому индексу в Bitfield-поле устанавливается единица, а в противном случае – 0.

Рисунок 1 – Структура bitfield-сообщения

Однако у способа, который описан выше есть один очень большой недостаток – низкая емкость – оценивается по объему файла, который нужно использовать для загрузки определенного текста. Для размещения сообщения «helloworld!» (в кодах ASCII) потребуется файл размером почти 25 Мб, если использовать размер фрагмента равный 256 КБ. Этот способ получил название одиночный режим. Также стоит учитывать, что внедренные в BitTorrent-сеть пиры не должны нарушать общую работу сети.

В представленном докладе исследуется возможность использования протокола BitTorrent для обмена скрытыми сообщениями между

компьютерами по беспроводной сетисо следующей функциональностью:

– возможность изменения bitfield-сообщения с целью передачи в нем секретной информации;

– выбор секретного сообщения;

– возможность получения и расшифровки секретного сообщения

Нами выбран одиночный режим из-за сложностей в создании большого количества пиров. Был реализован и модифицирован BitTorrent-клиент, который расшифровывает сид-файл, соединяется с трекером и пирами, а также отправляет скрытое сообщение в Bitfield-поле.

Для разработки BitTorrent-клиента, который сможет внедриться в сеть BitTorrentи не нарушить ее работу, использовались.NETи ASP.NETCore 6 версии. В результате разработано приложение, которое позволяет передавать другому компьютеру выбранное сообщение.

Использование BitTorrent-протокола для скрытой передачи информации является довольно интересным и удачным решением, которое обеспечивает достаточно высокую скрытность. Единственный серьезный недостаток – ограничение объема передаваемых данных. Одиночный режим позволяет отправлять, как правило, небольшую информацию, например, ключи и пароли.

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П. П. Урбанович, Д. М. Романенко. – Минск: БГТУ, 2022. – 608 с.

2. Why Google Made BitTorrent a Success [Электронный ресурс]. Режим доступа: https://torrentfreak.com/why-google-made-bittorrent-a-success-100321/. Дата доступа: 16.04.2023.

3. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

4. BitTorrent Turns 20: The File-Sharing Revolution Revisited [Электронный ресурс]. Режим доступа: https://torrentfreak.com/bittorrent-turns-20-the-file-sharing-revolution-revisited-210702/. Дата доступа: 17.04.2023.

5. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent [Электронный ресурс] – Режим доступа: https://www.hindawi.com/journals/scn/2020/8848315/ – Дата доступа: 18.04.2023.