УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

Моделирование с использованием сетей Петри защищенной передачи данных в пиринговых сетях

Аннотация. В данной работе рассматривается подход к моделированию защищенной передачи данных на основе сетей Петри в пиринговых сетях. Описан традиционный подход к передаче данных и его модификации с целью шифрования передаваемой информации. Приведены общая сеть Петри для получения и передачи данных, установления соединения и обмена данными.

Ключевые слова: информационная безопасность; организационно-распорядительная документация; защита информации; сети Петри.

Введение

В настоящее время многие крупные организации и предприятия бывают разделены территориально, в связи с чем, остро встает потребность в передаче большого объема информации между филиалами. Для того чтобы распределить нагрузку с центрального сервера, можно использовать пиринговые сети.

Несмотря на многообразие различных Torrent-клиентов, невозможно найти продукт, выполняющий передачу данных с одновременным шифрованием, что может привести к возможности получения конфиденциальной информации третьими лицами.

В данной работе с помощью сетей Петри[1,2] моделируется процесс функционирования Torrent-клиента и передача данных по torrent протоколу в пиринговых сетях.

Описание протокола и его модификации

Протокол непосредственной передачи данных состоит из подтверждения установления связи («рукопожатия»), за которым следует непрерывающий поток сообщений, каждому из которых соответствует длина сообщения. В стандартной реализации протокола определено девять типов сообщений.

- keepalive ([0]) – это сообщение нулевой длины, которое передается каждые две минуты и служат для поддержания состояния соединения для клиентов;
- choke ([1] [0]) – это сообщение, длиной 1 байт, которое указывает на то, что клиент заблокирован и не будет передавать данные;
- unchoke ([1] [1]) – это сообщение, длиной 1 байт, которое указывает на то, что клиент разблокирован и готов передавать данные;
- interested ([1] [2]) – это сообщение, длиной 1 байт, которое указывает на то, что клиент заинтересован в получении данных от других клиентов;
- not interested ([1] [3]) – это сообщение, длиной 1 байт, которое указывает на то, что клиент не будет получать данные;
- have ([5] [4] [данные]) – это сообщение, длиной 5 байт, которое содержит индекс фрагмента и отправляется всем подключенным клиентам после успешной загрузки и проверки хэша фрагмента;
- bitfield ([1 + длина данных] [5] [данные]) – это сообщение переменной длины, отправляемое в самом начале загрузки и содержащее сведения о имеющихся и отсутствующих фрагментах;
- request ([13] [6] [индекс] [начало] [длина]) – это сообщение фиксированной длины, которое служит для запроса данных от других клиентов;
- piece ([9 + длина данных] [7] [индекс] [начало] [данные]) – это сообщение переменной длины с фрагментом запрошенных данных.

Для передачи зашифрованных данных предлагается ввести два новых типа сообщений:

- enrequest ([13] [8] [индекс] [начало] [длина]) – сообщение фиксированной длины, аналогичное сообщению piece(передача данных), но имеющее системный номер 8;

- enpiece ([13 + длина данных] [9] [индекс] [начало] [длина данных] [данные]) – это сообщение переменной длины с фрагментом запрошенных данных в зашифрованном виде. По сравнению с сообщением piece, было добавлено указание длины данных, т.к. из-за особенностей процесса шифрования, размер зашифрованных данных может отличаться от размера запрошенных.

Моделирование

Для моделирования функционирования системы загрузки данных в пиринговых сетях в данной работе применяются сети Петри.

На рисунке 1 изображена сеть Петри, моделирующая работу всей системы загрузки и передачи и координации работы клиентов, в целом. Эта сеть предназначена для более общего рассмотрения процессов, происходящих при работе системы получения и передачи данных в пиринговых сетях.

Сеть сочетает в себе клиентскую и серверную часть. Ее работа начинается с перехода *Запуск приложения*. Сразу после запуска выполняется *чтение настроек* из соответствующего файла, затем *открывается порт* для прослушивания новых подключений и *запускается поток таймера*. Таймер выполняет определенные функции через заданные интервалы времени. К этим функциям относятся:

- отображение всплывающих информационных окон при начале, завершении загрузки, проверке хэша, ошибках;
- обработка очереди сообщений к трекеру – выполняет отсчет до следующего времени отправки сообщения к трекеру и отправляет его;
- запись загруженных фрагментов на диск – проверяет загрузку фрагмента данных, и в случае, если все блоки фрагмента были загружены, выполняет проверку хэш-суммы и последующую запись данных на диск.

Параллельно с запуском потока таймера, открывается порт для прослушивания подключений новых клиентов. В случае установления новой связи, запускается цикл обмена сообщениями.

После запуска приложения, когда были прочитаны настройки и открыт порт, можно добавить новый торрент-файл. В этом случае сначала выполняется проверка хэш-сумм имеющихся файлов, отправляется сообщение о начале загрузки трекеру. Трекер, в свою очередь, получив такое сообщение, извлекает из него необходимые параметры, после чего формирует список активных клиентов и отправляет его запросившему клиенту. После того, как клиент получит ответ от трекера, он пытается установить новые подключения.

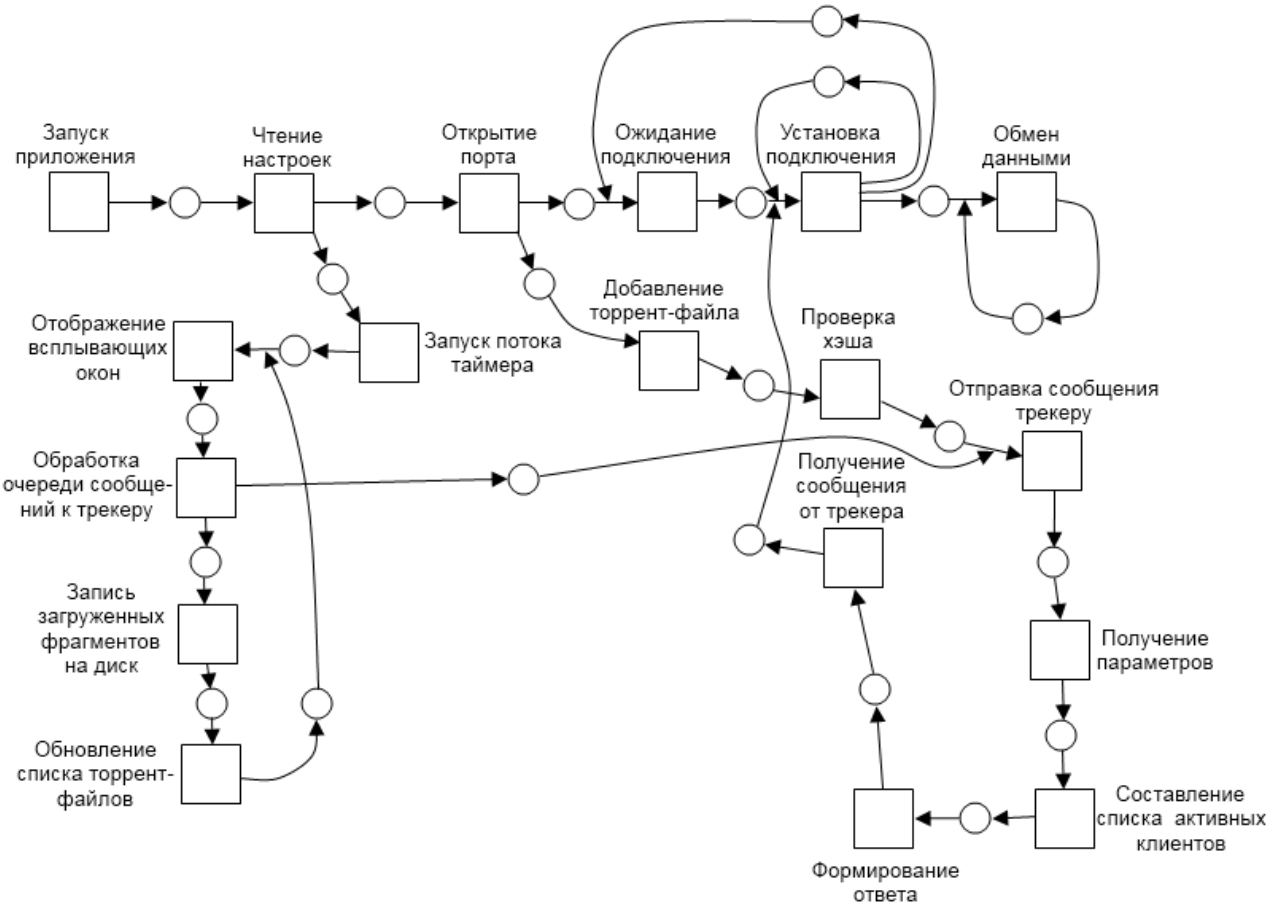

Рис. 1. *Сеть Петри системы получения и передачи данных в пиринговых сетях*

Установление подключения. После приема нового соединения и до передачи данных, клиентам необходимо подтвердить установление нового подключения путем обмена «Рукопожатиями» (Handshake-сообщениями). Сеть Петри, моделирующая этот процесс, представлена на рисунке 2.

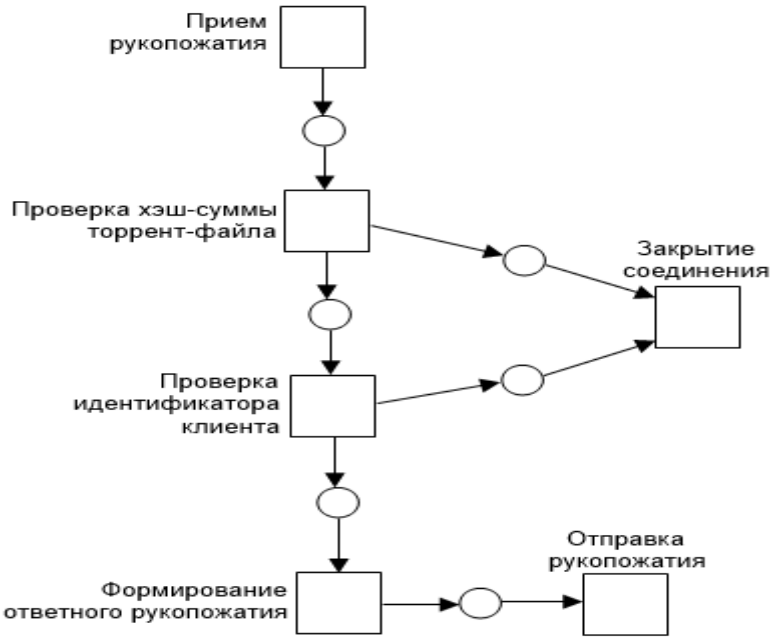

Рис. 2. *Сеть Петри для установления подключения*

Обмен данными с клиентами. На рисунке 3 представлена сеть Петри, моделирующая процесс обмена данными с клиентами.

Получив сообщение, необходимо узнать его тип. После этого можно проверить, правильной ли длины это сообщение. Если его размер не соответствует ожидаемому, тогда это сообщение игнорируется.

В зависимости от типа сообщения, выполняются различные действия. Например, при получении сообщения типа «Choke», клиент, от которого было получено это сообщение, помечается как «заблокированный», т.е. он не будет передавать фрагменты файлов.

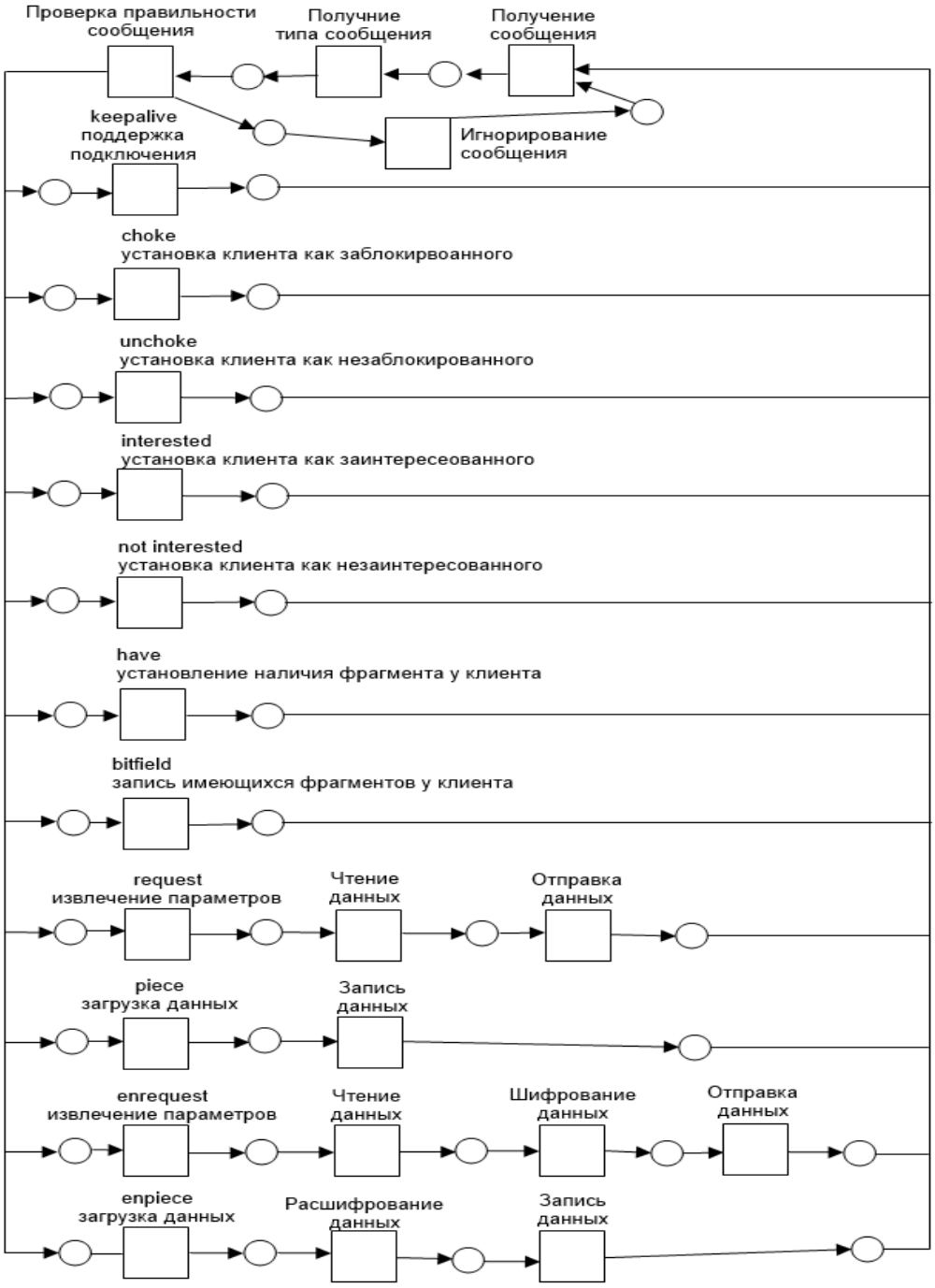

Рис. 3. *Сеть Петри для обмена данными*

При получении сообщения типа «Request», запрашиваемые данные считываются с диска и отправляются запрашиваемому клиенту. Аналогичные действия, за исключением шифрования отправляемых данных, программа выполняет при получении сообщения типа «EnRequest». Сообщения «Piece» и «EnPiece» так же похожи. При получении сообщения «EnPiece», приложение получает данные из сообщения, затем производит их расшифрование и записывает результат, в то время как при получении сообщения «Piece», приложение выполняет те же действия, но без расшифрования данных.

Заключение

В работе описан протокол для обмена данными в пиринговых сетях и его модификация для использования криптографических протоколов с целью обеспечения конфиденциальности передаваемой информации. Построены сети Петри учитывающие особенности предлагаемых модификаций процесса обмена сообщениями в torrent-сетях.

ЛИТЕРАТУРА

1. Iorsache, M. V. Supervisory Control of Concurrent Systems. A Petri Net Structural Approach / M. V. Iordache, P. J. Antsaklis. – Boston : Birkhauser, 2006. – 281 p.
2. Котов, В. Е. Сети Петри / В. Е. Котов. – М. : Наука. Главная редакция физико-математической литературы, 1984. – 160 с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

Modeling using Petri nets secure data transmission in peer-to-peer networks

Abstract. This paper describes an approach to modeling the secure transmission of data based on Petri nets in peer to peer networks. Described traditional approach to data transmission and modifications to encrypt information transmitted. Given the general Petri net for receiving and transmitting data, establish a connection and exchange data.

Keywords: information security; organizational and administrative documentation; data protection; Petri networks.

REFERENCES

1. Iorsache, M. V. Supervisory Control of Concurrent Systems. A Petri Net Structural Approach / M. V. Iordache, P. J. Antsaklis. – Boston : Birkhauser, 2006. – 281 p.
2. Kotov, V. E. Seti Petri / V. E. Kotov. – M. : Nauka. Glavnaja redakcija fiziko-matematicheskoj literatury, 1984. – 160 s.