Технологии многопоточной передачи данных в информационных системах

А. А. Москвин, email: tema.kg9012@gmail.com [1]

[1]Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, Краснодар, Россия

Аннотация. *В статье рассматриваются основные этапы реализации протокола транспортного уровня SCTP, имеющим функции управления информационными потоками при многопоточной передачи данных, а также сделаны выводы о применимости данной технологии в синтезе с существующими методами проактивной защиты вычислительных сетей. Цель стати - постановка задачи по разработке алгоритма динамического управления информационными потоками с применением маскирующего трафика, а также разработке модели функционирования сети передачи данных с применением технологии многопоточной передачи данных для организации маскирующего обмена с соблюдением требований к своевременности информационного обмена конструктивными сообщениями.*

Ключевые слова: *проактивная защита, вычислительная сеть, многоадресность, многопоточность, компьютерная атака, сетевые соединения, протокол, сетевая разведка.*

Введение

В информационных системах (далее - ИС) в качестве основного протокола гарантированной передачи данных транспортного уровня применяется TCP (Transmission Control Protocol, RFC 703). Однако, указанный протокол имеет существенные недостатки, которые могут влиять на качество информационного обмена:

протокол TCP достаточно слабо защищён от DOS-атак;

протокол TCP формирует задержки в получении данных при возникновении нарушения порядка доставки пакетов в сети, в том числе для приложений вышестоящего уровня, где требуется лишь гарантированная доставка.

Формулируя требования по защите информации, регуляторы предписывают необходимость в управлении информационными потоками между информационными системами, в том числе в контроле сетевых соединений (приказ ФСТЭК от 15.02.2017 г. № 27), что сводит

к минимуму применение транспортного протокола UDP (User Datagram Protocol, RFC 768).

Данные ограничения снимаются при применении протокола транспортного уровня SCTP (Stream Control Transmission Protocol — «протокол передачи с управлением потоком», RFC 4960).

В данной статье рассмотрено функциональное представление протокола SCTP, а также сделаны выводы о его применимости по формированию и управлению маскирующего обмена между корреспондентами ИС с точки зрения обеспечения своевременности информационного обмена в условиях применения злоумышленником средств технической компьютерной разведки.

Функциональное представление протокола SCTP

Протокол SCTP обеспечивает корреспондентам следующие типы сервиса:

передача пользовательских данных с корректировкой ошибок, подтверждением доставки и отсутствием дубликатов;

фрагментирование данных в соответствии с определенным для пути значением MTU (Maximum Transmission Unit; максимальная единица передачи);

упорядоченная доставка пользовательских сообщений внутри множества потоков

с возможностью управления порядком доставки отдельных пользовательских сообщений;

возможность группировки пользовательских сообщений в один пакет SCTP;

устойчивость к отказам на сетевом уровне за счёт поддержки многоадресных корреспондентов на обеих сторонах соединения.

Структура протокола SCTP, а также формирующие ее функции представлены на Рисунке.

Основными являются следующие этапы реализации протокола:

1. Создание (завершение) ассоциации. Ассоциация SCTP определяет протокольные отношения между корреспондентами SCTP. В процессе создания ассоциации задается число применяемых потоков (S), формируется список транспортных адресов (номер порта SCTP в комбинации с множеством адресов IP, формирующих сокет SCTP), которые корреспондент может использовать для связи и откуда она будет получать пакеты SCTP. Это обеспечивает устойчивость к отказам на сетевом уровне в случае поддержки многоадресности корреспондентами ассоциации.

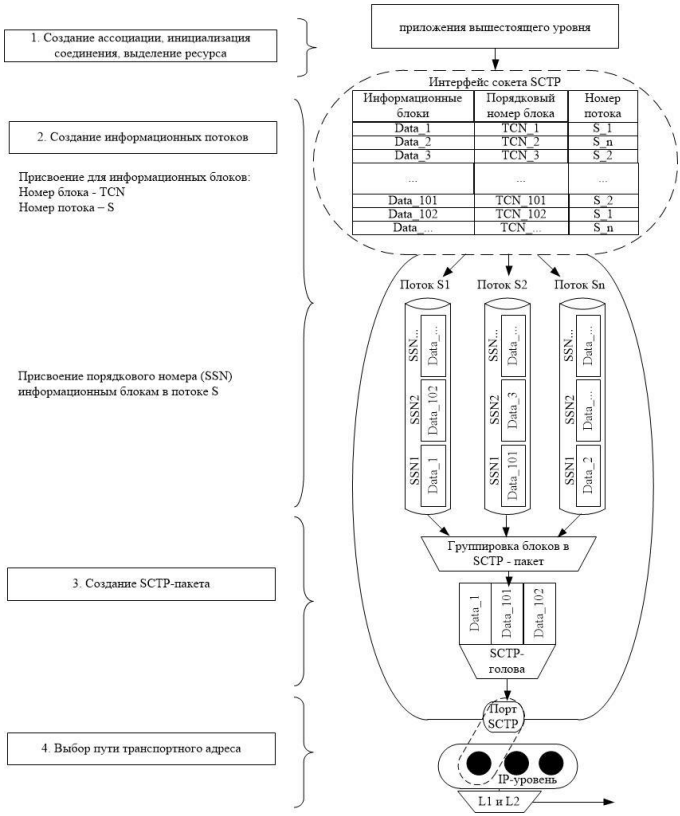

Рисунок.

Многоадресное обращение к единому SCTP-сокету позволяет использовать вырабатываемый ресурс приложений вышестоящего уровня без разрыва сетевого соединения (ассоциации).

Это отличает SCTP-сокет от TCP-сокета, который каждый раз создается между парой взаимодействующих корреспондентов при создании новых процессов.

При создании ассоциации применяется четырехэтапный механизм согласования сетевого соединения («four-way handshake») со встроенными процедурами проверки служебной информации, что позволяет избежать компьютерных атак на синхронизацию соединения.

Протокол SCTP не поддерживает полуоткрытых состояний (как в TCP), когда одна сторона может передавать данные после того, как другая сторона уже закрыла соединение.

2. Создание информационных потоков. Единицей информации, передаваемой между корреспондентами ассоциации SCTP, является блок (chunk). Тип блока зависит от передаваемой в нем информации, и может подразделятся на блоки с пользовательскими данными (тип блока DATA), и служебные блоки для обеспечения корректной работоспособности протокола SCTP (блоки типа INIT, SACK, ABORT).

Каждому блоку пользовательских данных, поступающих из приложений вышестоящего уровня, присваиваются следующие порядковые номера:

порядковый номер при передаче (TSN, имеет значение от 0 до 232-1), применяется для управления передачей сообщений и выявления их потери;

номер используемого потока (S);

порядковый номер в потоке S (SSN, имеет значение от 0 до 65535), используется для управления порядком доставки конечным точкам полученных данных.

Указанные механизмы нумерации являются независимыми, что позволяет доставлять на вышележащий уровень пользовательские данные даже при наличии пропусков в порядковых номерах TSN (т.е. пропущенный блок DATA относится к другому потоку). Блокировка одного потока, вызванного потерей SCTP-пакета (и как следствие вызова процедур повторного запроса на передачу в форме служебного блока SACK), никак не влияет на функционирование других потоков, что предоставляет возможность приложениям вышестоящего уровня, где порядок доставки сообщений не является критичным, своевременно обрабатывать полученные сообщения.

По запросу приложения вышестоящего уровня, блоки пользовательских данных могут быть отправлены в обход механизма упорядочивания и незамедлительно доставлены

на вышестоящий уровень. Как правило, такие данные помещаются в начале очереди

на отправку.

3. Формирование SCTP-пакета. Элементом данных, передаваемый от SCTP в нижележащий уровень, является SCTP-пакет. Он состоит из общего заголовка и одного или нескольких сгруппированных блоков, поступающих из различных потоков. Запрет на группировку информационных блоков может быть осуществлен по запросам приложений вышестоящего уровня.

В одном пакете SCTP может содержаться множество блоков, пока размер пакета не превысит значение MTU. Поскольку передаваемые блоки пользовательских данных определяются приложениями

вышестоящего уровня и имеют переменный размер, то, в целях формирования пакетов с соответствующим MTU, SCTP применяет механизмы фрагментации блоков пользовательских сообщений. При этом каждому фрагменту присваивается уникальный номер TSN, но одинаковый номера SSN.

Протокол SCTP имеет функции контроля насыщения для обеспечения доставки данных за приемлемое время в условиях внешних воздействий на сеть, проявляющихся, например,

в качестве неожиданных всплесков трафика. Контроль насыщения работает в SCTP на уровне ассоциаций, а не отдельных потоков в ассоциации.

Применение этих функций позволяет управлять скоростью передачи SCTP-пакетов, воздействуя на следующие переменные:

размер окна приема (rwnd, в байтах), устанавливаемый получателем данных;

окно контроля насыщения (cwnd, в байтах), устанавливаемый отправителем данных;

порог замедленного старта (ssthresh, в байтах), используемый отправителем для выбора алгоритма контроля насыщения.

Известны способы удержания в двустороннем порядке сетевого соединения TCP посредством воздействия на окно приема, а также эмуляции наличия помех в канале связи [1]. Такие способы возможны и для SCTP.

4. Многоадресность. Корреспондент SCTP рассматривается как многоадресный, если может использовать множество транспортных адресов для отправки SCTP-пакета. При этом выбор основного пути определяется приложениями вышестоящего уровня.

SCTP использует процедуру выбора альтернативного адреса назначения (из множества транспортных адресов созданной ассоциации) в случае недоступности основного (например,

в случае его отказа).

Данный механизм позволяет поддерживать в активном состоянии критические сетевые соединения, например в условиях динамического управления сетевым адресным пространством [2-5], ввиду чего механизм «многоадресности» SCTP может быть рассмотрен как один из способов маскирования структуры информационной системы.

Описанные 4 этапа реализации протокола обуславливают возможность применения технологии многопоточной передачи данных для обеспечения своевременности информационного обмена при применении методов проактивной защиты [6-16] вычислительных сетей.

Учитывая поддержку многоточности в протоколе SCTP, имея возможность воздействовать на определение потоков для поступающих блоков данных, группировки потоков в один SCTP-пакеты, а также способности влиять на скорость передачи пакетов, SCTP применим для модернизации известных способов защиты вычислительных сетей [17-24].

Учитывая поддержу многоадресности в протоколе SCTP, имея возможность воздействия на выбор основного пути (в том числе в автоматическом режиме), SCTP применим в качестве маскирования адресного пространства ИС при динамическом конфигурировании структурно-функциональных характеристик клиент-серверной вычислительной сети в условиях ведения технической компьютерной разведки.

Заключение

Рассмотренные функциональные возможности протокола транспортного уровня SCTP компенсируют ограничения протоколов TCP и UDP, которые непосредственно влияют на своевременность доставки сообщений получателю. Это достигается посредством применения механизмов «многопточности» и «многоадресности».

Указанные механизмы применимы в синтезе с существующими способами маскирования сетевых адресов корреспондентов и способами формирования маскирующего обмена между информационными системами. Вместе с этим возникает задача по созданию алгоритмов динамического управления потоками, реализуемым в протоколе транспортного уровня.

Маскирующий обмен формируется случайным образом, зависит от количества информационных потоков и количества транспортных адресов между корреспондентами, что добавляет избыточность в среду передачи данных. Ввиду этого возникает задача по разработке модели функционирования сети передачи данных с применением технологии многопоточной передачи данных для организации маскирующего обмена с соблюдением требований к своевременности информационного обмена конструктивными сообщениями.

Список литературы

1. Максимов, Р. В. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки / Р. В. Максимов, Д.Н. Орехов, С. П. Соколовский // Системы управления, связи и безопасности. – 2019. – № 4. – С. 50-86.

2. Ворончихин, И. С. Маскирование структуры распределенных информационных систем в киберпространстве / И. С. Ворончихин, Р. В. Максимов Р.В. , С. П. Соколовский // Вопросы кибербезопасности. – 2019. – № 6(34), – С. 92-99.

3. Максимов, Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Информатика и автоматизация. – 2020. – № 19 (5). – С. 1018-1044.

4. Иванов, И. И. Модель функционирования распределенных информационных систем при использовании маскированных каналов связи / И. И. Иванов // Системы управления, связи и безопасности. – 2020. – № 1. – С. 198-230.

5. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения : Материалы XXIII Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева (Красноярск, 11–15 ноября 2019 г.). – Красноярск, 2019. – С. 447-448.

6. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 166-173.

7. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2009. – № 1(72). – С. 181-187.

8. Максимов, Р. В. Модель случайных помех интегрированным системам ведомственной связи / Р. В. Максимов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 151-155.

9. Максимов, Р.В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды

всеармейской научно-практической конференции (Санкт-Петербург, 11–12 октября 2017 г.). – Санкт-Петербург, 2017. – С. 138-147.

10. Максимов, Р.В. Этюды технологии маскирования функционально-логической структуры информационных систем / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции (Санкт-Петербург, 11–12 октября 2017 г.). – Санкт-Петербург, 2017. – С. 147-154.

11. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н.Е. Жуковского : сб. тр. участников VIII Междунар. научно-практической конф. "Научные чтения имени профессора Н. Е. Жуковского" (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2018. – С. 47–52.

12. Соколовский, С. П. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию / С. П. Соколовский, Н. А. Усов // Информатика: проблемы, методология, технологии : материалы XVI Международной научно-методической конференции (Воронеж, 11-12 февраля 2016 г.). – Воронеж, 2016. – С. 259-264.

13. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов [и др.] // Технические и технологические системы : материалы девятой Международной научной конференции «ТТС-17» (Краснодар, 22-24 ноября 2017 г.). – Краснодар, 2017. – С. 117–121.

14. Душкин, А. В. Особенности оценки времени противодействия несанкционированным воздействиям на информационные телекоммуникационные системы / А. В. Душкин, М. Ю. Петшауэр, С. П. Соколовский // Информация и безопасность. – 2009. – № 2. – С. 305-308.

15. Соколовский, С. П. Модель конфликта в информационной сфере / С. П. Соколовский, С. Р. Шарифуллин, Е. С. Маленков // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-ой годовщине полета Ю.А. Гагарина в космос : Сборник научных статей, Краснодар, 12–13 апреля 2018 года / КВВАУЛ им. А.К. Серова. – Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг", 2018. – С. 299-304.

16. Катунцев С. Л. Моделирование способа обфускации идентификаторов сетевых устройств в интересах минимизации компрометирующих признаков средств проактивной защиты вычислительных сетей / С. Л. Катунцев, Д. Н. Орехов,

С. П. Соколовский // Научные труды Кубанского государственного технологического университета. – 2018. – № 3. – С. 239-248.

17. Устройство поиска информации [Текст] : пат. 2219577 Российская Федерация : МПК G 06 F 17/40 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военный университет связи. – № 2002111059/09 ; заявл. 24.04.2002 ; опубл. 20.12.2003, Бюл. № 1. – 27 с.

18. Способ выбора безопасного маршрута в сети связи (варианты) : пат. 2331158 Российская Федерация : МПК H 04 L 12/28 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2007103774/09 ; заявл. 31.01.2007 ; опубл. 10.08.2008, Бюл. № 22. – 34 с.

19. Способ сравнительной оценки структур информационно-вычислительной сети : пат. 2408928 Российская Федерация : МПК G 06 F 21/20 H 04 L 12/28 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2009129726/08 ; заявл. 03.08.2009 ; опубл. 10.01.2011, Бюл. № 1 – 16 с.

20. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети : пат. 2306599 Российская Федерация : МПК G 06 F 21/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2006114272/09 ; заявл. 26.04.2006 ; опубл. 20.09.2007, Бюл. № 26 – 56 с.

21. Способ мониторинга безопасности автоматизированных систем : пат. 2355024 Российская Федерация : МПК G 06 F 15/00 G 06 F 17/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2007105319/09 ; заявл. 12.02.2007 ; опубл. 10.05.2009, Бюл. № 13 – 15 с.

22. Способ защиты вычислительных сетей : пат. 2649789 Российская Федерация : МПК H 04 L 12/801 H 04 L 29/06 H 04 L 9/32 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2017125677 ; заявл. 17.07.2017 ; опубл. 04.04.2018, Бюл. № 10 – 25 с.

23. Способ защиты вычислительных сетей : пат. 2696330 Российская Федерация : МПК G 06 F 21/50 G 06 F 21/60 H 04 L 09/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2018128075 ; заявл. 31.07.2018 ; опубл. 01.08.2019, Бюл. № 22 – 30 с.

24. Душкин, А. В. Способ распознавания вредоносных воздействий на информационную систему / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Телекоммуникации. – 2011. – № 10. – С. 25-28.