Математические структуры и моделирование 2018. № 4(48). С. 139–146

УДК 004.052.32:004.722
DOI: 10.25513/2222-8772.2018.4.139-146

ПРИНЦИПЫ ПОСТРОЕНИЯ ПРОТОКОЛА ГАРАНТИРОВАННОЙ ДОСТАВКИ СООБЩЕНИЙ

Д.Н. Лавров
к.т.н., доцент, e-mail: lavrov@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Как правило, в компьютерных сетях информационная безопасность рассматривается с точки зрения трёх свойств: конфиденциальность, целостность и доступность. В настоящее время актуально рассматривать и такое свойство информации, как анонимность. Для обеспечения последнего используется такое средство, как TOR. Сеть TOR даёт нам иллюзию анонимности в сети Интернет и усыпляет бдительность конечного пользователя. Но на выходном узле TOR-сети трафик расшифровывается, и его содержимое может стать известно владельцу этого выходного узла. Если владельцем узла или серии узлов являются авторитарное правительство или иностранный агент, то он может не только узнать содержимое передаваемого сообщения, но и попытаться модифицировать его или вовсе прервать канал связи. Конфиденциальность сообщения можно защитить с помощью шифрования, но остаётся лишь надеяться, что оно надёжно. Доступность и целостность остаются под угрозой. Здесь под доступностью понимается гарантия доставки целостного сообщения до места назначения. В статье рассматриваются принципы, которые должны быть положены в основу протокола передачи данных с гарантированной доставкой. Идея протокола основана на существовании в сети нескольких независимых маршрутов доставки и использовании криптографических (k, n)–пороговых схем разделения секрета в n сетевых потоках разных маршрутов. Это позволит не только дополнительно анонимизировать трафик, но и в случае контроля авторитарным правительством выходных узлов (меньших порога k) предоставит дополнительную защиту конфиденциальностит трафика.
Исследование выполнено в рамках научного проекта НИОКТР № 01-06/683.

Ключевые слова: разделение секрета, маршрутизируемая сеть, анонимность, доступность.

Введение

В компьютерных сетях информационная безопасность рассматривается с точки зрения трёх свойств: конфиденциальность, целостность и доступность. В настоящее время рассматривается и такое свойство информации, как аноним-

ность. Для обеспечения последнего используются различные инструменты анонимайзеры. Одно из таких средств — это технология TOR (The Onion Routing). Сеть TOR даёт пользователю иллюзию безопасности в сети Интернет. Так ли это на самом деле?

Кратко опишем суть технологии [1, 2]. Сеть TOR состоит из компьютеров добровольцев. По умолчанию маршрут до адресата формируется через три узла TOR-сети: guard (сторожевой) или entry (входной, в более ранней версии), middle (промежуточный) и exit (выходной). Все три узла могут находиться в разных странах и под разной юрисдикцией. Исходный трафик вместе с заголовками многократно шифруется. Так, первый узел шифрует трафик и направляет его на входной узел, тот в свою очередь шифрует вместе с заголовком, содержащим адрес отправителя, и передаёт его промежуточному узлу. Далее полученный трафик ещё раз шифруется и направляется на выходной узел. Получается вложенное туннелирование, так что промежуточный узел не знает, кому и от кого отправлено сообщение. Выходной узел извлекает исходные данные и отправляет их адресату.

Итак, на выходном узле TOR-сети трафик расшифровывается и его содержимое может стать известно владельцу этого выходного узла. Если владельцем узла или серии узлов является злоумышленник, авторитарное правительство или иностранный агент, то они могут не только узнать содержимое передаваемого сообщения, но и попытаться модифицировать его или вовсе прервать канал связи. Конфиденциальность сообщения можно защитить с помощью шифрования (использование https), но остаётся лишь надеяться, что оно надёжно. Имеется информация, что «выходные узлы TOR могут прослушивать коммуникации и осуществлять атаки посредника (MiTM), даже при использовании HTTPS» [3].

Кто разработчики? Технология TOR создана в «Центре высокопроизводительных вычислительных систем» Исследовательской лаборатории Военно-морских сил США совместно с DARPA по федеральному заказу (1999 год). В дальнейшем исходный код был опубликован под свободной лицензией (2003 год).

Кто контролирует выходные узлы? Теоретически проект заявляет, что это делается добровольцами. Имеется информация о контроле выходных узлов спецслужбами иностранных государств [4].

Анализ всех представленных данных показывает, что доступность и целостность находятся под угрозой в TOR-сетях. Под доступностью понимается гарантия доставки целостного сообщения до места назначения.

Таким образом, необходимо разработать принципы, которые могут быть положены в основу протокола передачи данных с гарантированной доставкой. Такой протокол может работать в любой маршрутизируемой сети с несколькими маршрутами доставки до адресата.

1. Модель злоумышленника

Злоумышленник может быть пассивным и только просматривать трафик и активным — может вмешиваться: модифицировать или даже уничтожать сооб-

щения.

Вне зависимости от типа злоумышленник может контролировать менее k-каналов.

2. Существующие подходы

В работе В.И. Ефимова и Р.Т. Файзуллина [6] предложена простая двухканальная схема маскирования трафика.

Пусть M — исходное сообщение. С помощью демультиплексора поток разделяется на два байтовых потока чётных M_0 и нечётных байт M_1. По первому каналу передаётся $M_0 \oplus M_1$, по второму — только M_1 передаётся как есть. У адресата на мультиплексор поступает $M_0 := (M_0 \oplus M_1) \oplus M_1$ и поток M_1, приходящий по второму каналу. Мультиплексор объединяет эти два потока в поток M.

С точки зрения экономии схема не порождает лишнего трафика, но с точки зрения безопасности протокол подвержен атаке восстановления сообщения по словарю. Для восстановления сообщения необходимо наблюдать все каналы.

Ещё одна схема разделения секрета, которую можно использовать для маскирования трафика в системе из нескольких каналов, — это n-канальная схема, описанная у Б. Шнайера [5, п. 3.6].

Пусть M — исходное сообщение. Отправитель генерирует $n-1$ случайных битовых последовательностей по длине равных длине сообщения K_i, $i = 1, \ldots, n-1$. Далее по первому каналу отправляется $M \oplus \bigoplus\limits_{i=1}^{n-1} K_i$, по второму — K_1, по третьему — K_2, ..., по n-ому — K_{n-1}. На принимающей стороне все фрагменты складываются, и исходное сообщение восстанавливается $M := (M \oplus \bigoplus\limits_{i=1}^{n-1} K_i) \oplus K_1 \oplus \ldots \oplus K_{n-1}$.

Достоинством протокола является высокая безопасность (при условии правильного выбора случайных одноразовых ключей K_i, $i = 1, \ldots, n-1$). Первый недостаток в том, что каждый фрагмент по объёму равен всему сообщению. Второй недостаток в том, что при повреждении хотя бы одного фрагмента становится невозможным восстановить всё сообщение.

В работах [7, 8] предлагается оригинальный алгоритм на основе побитового мултиплексирования с битовыми сдвигами или перестановками, осуществляемыми над фрагментами. Сами фрагменты после сдвигов и перестановок становятся автоключом для соседнего канала.

Избыточность алгоритма — низкая, надёжность с точки зрения безопасности — приемлемая [8]. Недостатком подхода является то, что повреждение фрагмента секрета приведёт к невозможности восстановления всего сообщения.

В основу протокола может быть положен и любой из известных алгоритмов разделения секрета. Например, схема Шамира. К сожалению, избыточность алгоритма будет высокой потому, что размер фрагмента секрета (тени) равен в большинстве случаев размеру самого сообщения.

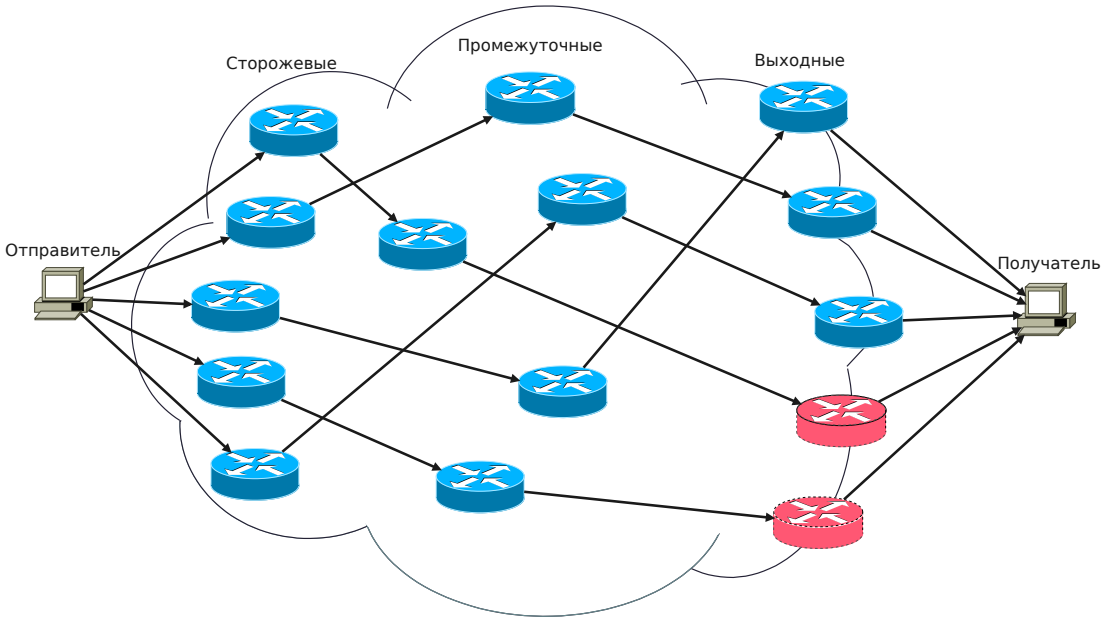

Рис. 1. Схема маршрутизируемой сети с несколькими маршрутами до адресата. Облако обозначает часть маршрутизируемой сети (например, TOR-сеть). Красным выделены выходные маршрутизаторы, находящиеся под управлением злоумышленника

3. Принцип гарантированной доставки

В работе [9] описаны несколько подходов к реализации протокола гарантированной доставки, в частности одним из подходов является использование схемы разделения секрета. Первые три подхода, описанные в предыдущем разделе, также являются видом (n, n)-пороговой схемы.

Идея протокола основана на существовании в сети нескольких независимых маршрутов доставки и использовании криптографических (k, n)-пороговых схем разделения секрета в n сетевых потоках разных маршрутов. Это позволит не только дополнительно анонимизировать трафик, но и в случае контроля злоумышленником выходных узлов (меньших порога k) позволит предоставить дополнительную защиту конфиденциальности трафика.

Рассмотрим схему сети, представленную на рис. 1. Два последних маршрутизатора находятся под контролем злоумышленника. В таблице. 1 представлены сводные результаты возможности восстановления секрета пассивным наблюдателем (конфиденциальность) и возможность повредить сообщение без возможности восстановления (доступность). Из таблицы видно, что в указанной ситуации добиться одновременной доступности и конфиденциальности (без непосредственного шифрования) можно при схеме $(3, 5)$. Гарантию доставки (доступность) можно добиться при пороге $k \leqslant 3$.

Таблица 1. Защищённость многоканального соединения

Схема	**Конфиденциальность**	**Доступность**
(1,5)	–	+
(2,5)	–	+
(3,5)	**+**	**+**
(4,5)	+	–
(5,5)	+	–

4. Восстановление сообщения

Возможны два подхода. *Первый* — комбинаторный. Необходимым условием корректности восстановления является совпадение восстановленного сообщения на нескольких пороговых комбинациях.

Рассмотрим его на примере. Пусть имеется сообщение M, разделённое на пять фрагментов M_1, M_2, M_3, M_4, M_5. Для определённости пусть повреждена пятая тень. Используется пороговая схема $(3, 5)$. Из 5 теней можно скомбинировать $C_5^3 = 10$ комбинаций:

$M_1,\ M_2,\ M_3$; <– $M_2,\ M_3,\ M_4$; <–
$M_1,\ M_2,\ M_4$; <– $M_2,\ M_3,\ \mathbf{M}_5$;
$M_1,\ M_2,\ \mathbf{M}_5$; $M_3,\ M_4,\ \mathbf{M}_5$;
$M_1,\ M_4,\ M_3$; <– $M_1,\ M_4,\ \mathbf{M}_5$;
$M_1,\ \mathbf{M}_5,\ M_3$; $M_1,\ \mathbf{M}_5,\ M_4$.

Из четырёх комбинаций, помеченных "<–", однозначно восстанавливается сообщение. И по ним же мы можем проверить необходимое условие совпадения результата восстановления.

При повреждении двух фрагментов, пусть это будут для определённости M_4 и M_5, только одна комбинация M_1, M_2, M_3 позволяет восстановить сообщение, но что именно по этой комбинации возможно восстановление определить нельзя.

Недостатки подхода: 1) имеется лишь необходимое условие корректности восстановления (достаточное условие неизвестно); 2) при повреждённых фрагментах на единицу меньших порога нет возможности установить, какое из восстановленных сообщений верно; 3) при росте каналов растёт трудоёмкость, как C_n^k.

Второй подход заключается в использовании алгоритма HMAC [10]. Для этого на этапе согласования параметров необходимо сгенерировать общий ключ K, например, с помощью алгоритма Диффи–Хеллмана [11], который в дальнейшем и будет использоваться для алгоритма HMAC.

Каждый фрагмент «подписывается» алгоритмом HMAC на ключе K и передаётся вместе с фрагментом секрета.

5. Описание протокола гарантированной доставки

Первый этап протокола гарантированной доставки — это согласование параметров передачи. На этом этапе осуществляется обмен сообщениями одновременно по всем каналам («лавинная» рассылка). На данном этапе необходимо согласовать следующие параметры:

- тип схемы разделения секрета и её параметры;
- число каналов n;
- порог схемы k;
- модуль схемы разделения секрета p;
- алгоритм HMAC и его параметры;
- ключ K для алгоритма HMAC;
- алгоритм генерации общего ключа и его параметры.

На втором этапе происходит передача данных. Сообщение M разбивается на блоки $B_i < p$, $i = 1, \ldots, N$, p — согласованный ранее параметр, простое число, модуль конечного поля. Каждое B_i разбивается на n фрагментов секрета (теней):

$$M_{1,i}, M_{2,i}, \ldots, M_{n,i}.$$

К каждой тени применяется HMAC:

$$h_{1,i} = HMAC(M_{i,1}|i), \ldots, h_{n,i} = HMAC(M_{n,i}|i).$$

По каналам отправляются пары:

$$(M_{1,i}, h_{1,i}, i);\ (M_{2,i}, h_{2,i}, i), \ldots, (M_{n,i}, h_{n,i}, i).$$

По j-ому каналу передаётся тройка $(M_{j,i}, h_{j,i}, i)$. Третий параметр, номер блока, необходим для отслеживания правильного порядка в сетях с коммутацией пакетов при использовании транспорта без установления соединения.

На принимающей стороне проверяется целостность теней, из неповреждённых фрагментов секрета восстанавливаются блоки B_i исходного сообщения M и затем само сообщение.

Заключение

В работе рассмотрены основные принципы построения протокола гарантированной доставки. В настоящее время идёт разработка расширяемых программных модулей, осуществляющих реализацию подходов, описанных в данной статье.

Благодарности

Выражаю огромную признательность Гуссу Святославу Владимировичу, Бречке Денису Михайловичу, Черкашину Антону Васильевичу за обсуждение принципов архитектуры протокола и конструктивную критику. Часть результатов данной статьи озвучена в докладе на конференции «Современное программирование» (2018 г. [12]).

Исследование выполнено в рамках научного проекта НИОКТР №01-06/683.

Литература

1. Dingledine R., Mathewson N., Syverson P. Tor: The Second-Generation Onion Router. [Электронный ресурс]. 2004. URL: `https://svn.torproject.org/svn/projects/design-paper/tor-design.html` (дата обращения: 15.11.2018).
2. Dingledine R., Mathewson N. Tor Protocol Specification. [Электронный ресурс]. URL: `https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt` (дата обращения: 15.11.2018).
3. Анонимность в TOR: что нельзя делать / псевдоним автора : m1rko // Хабр [Электронный ресурс]. 2017. URL: `https://habr.com/post/329756/` (дата обращения: 15.11.2018).
4. Ализар А. ФБР контролирует выходные узлы TOR? URL: `https://xakep.ru/2014/11/11/fbi-tor/` (дата обращения: 15.11.2018).
5. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. Переводчик: Дубнова Н. 2-е издание. М. : Диалектика, 2003. 610 с.
6. Ефимов В.И., Файзуллин Р.Т. Система мультиплексирования разнесённого TCP/IP трафика // Математические структуры и моделирование. 2002. Вып. 10. С. 170-172
7. Д.Н. Лавров. Схема разделения секрета для потоков данных маршрутизируемой сети // Математические структуры и моделирование. 2002. Вып. 10. С. 192–197.
8. Дулькейт В.И., Лавров Д.Н., Михайлов П.И., Свенч А.А. Анализ надёжности алгоритма разделения секрета в сетевых потоках // Математические структуры и моделирование. 2003. Вып. 12. С. 146–154.
9. Гусс С.В., Лавров Д.Н. Подходы к реализации сетевого протокола обеспечения гарантированной доставки при мультимаршрутной передаче данных // Математические структуры и моделирование. 2018. № 2(46). С. 95–101.
10. Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-hashing for message authentication. // IETF. Febrary, 1997. URL: `https://tools.ietf.org/html/rfc2104` (дата обращения: 15.11.2018).
11. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Trans. Inf. Theory / F. Kschischang — IEEE. 1976. V. 22, No. 6. P. 644–654.
12. Лавров Д.Н., Черкашин А.В. Гарантированная доставка на основе разделения секрета в сети с несколькими маршрутами // I Международная научно-практическая конференция «Современное программирование» // Нижневартовск : Изд-во Нижневарт. гос. ун-та, 2018.

PRINCIPLES OF BUILDING A PROTOCOL FOR GUARANTEED MESSAGE DELIVERY

D.N. Lavrov
Ph.D.(Eng.), Associate Professor, e-mail: lavrov@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. As a rule, in computer networks information security is considered from the point of view of three properties: confidentiality, integrity and availability. Currently, it is important to consider such property of information as anonymity. To ensure the latter, a tool such as TOR is used. The TOR network gives us the illusion of anonymity on the Internet and lulls the vigilance of the end user. But at the output node of the TOR network, the traffic is decrypted and its contents may become known to the owner of this output node. If the owner of a node or a series of nodes is an authoritarian government, or a foreign agent, then he can not only know the contents of the message being transmitted, but also try to modify it or completely interrupt the communication channel. Confidentiality of the message can be protected by encryption, but one can only hope that it is secure. Accessibility and integrity remain at risk. Here, availability means a guarantee of delivering a complete message to a destination. The article discusses the principles that should be the basis of the data transfer protocol with guaranteed delivery. The idea of the protocol is based on the existence in the network of several independent delivery routes and the use of cryptographic (k, n)—threshold secret separation schemes in the n network flows of different routes. This will allow not only to further anonymize traffic, but also in the case of control by the authoritarian government of the output nodes (lower than k threshold) will provide additional protection for the confidentiality of traffic.
This research was done as part of a research project NIOKTR number 01-06/683.

Keywords: secret sharing, routed network, anonymity, availability.

Дата поступления в редакцию: 21.11.2018