Математические структуры и моделирование
2002, вып. 10, с. 192–197

УДК 621.316.5

СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА ДЛЯ ПОТОКОВ ДАННЫХ МАРШРУТИЗИРУЕМОЙ СЕТИ

Д.Н. Лавров

Scheme of division of secret for dataflows of network is offered.

Введение

Противодействие снифингу (перехвату и анализу сетевого трафика с целью получения служебной и/или конфиденциальной информации) может осуществляется в нескольких направлениях, одним из которых является использование схем разделения секрета. В качестве секрета выступает само передаваемое сообщение, а в качестве хранителей секрета — маршруты передачи. При использовании таких систем сниферу для перехвата сообщения требуется полный контроль узлов сети, задающих маршруты потоков, что трудно осуществить на практике.

По простейшей схеме [2] сообщение делится между двумя маршрутами. Алгоритм приема-передачи потока данных выглядит следующим образом.

(1) Отправляющая сторона генерирует строку случайных битов, F_1, такой же длины, что и сообщение, S.

(2) Выполнением «исключающее или» ($\oplus$) над S и R создается F_2,

$$R \oplus M = F_2.$$

(3) Далее по первому маршруту передается F_1, а по второму - F_2. Чтобы получить сообщение, принимающая сторона должна выполнить единственное действие:

$$F_1 \oplus F_2 = S.$$

Этот метод при правильном выполнении абсолютно безопасен. Никакие вычислительные средства не смогут восстановить сообщение только по одной его части [2].

Недостатком такой схемы является увеличение размера сообщения в два раза, что уменьшает производительность сети.

Идея разделенной передачи с использованием стека протоколов TCP/IP описана Р.Т. Файзуллиным и В.И. Ефимовым в статье настоящего журнала [1].

E-mail: lavrov@univer.omsk.su

Омский государственный университет

В предложенной реализации сообщение побитово делится на две части: первый поток образуется первой частью, второй — из сложенных побитово двух сообщений.

Особенностью такой схемы является передача по одному маршруту в открытом виде фактически половины сообщения.

В технической реализации требуется два промежуточных узла транслирующих IP-адреса. Система, таким образом, состоит из шести ключевых узлов: двух промежуточных пунктов, двух маршрутизаторов (проход которых определяет разделение или объединение маршрутов), передающей и приемной станций.

Предлагается модифицированная схема передачи данных по маршрутизируемой сети, в которой исходное сообщение разбивается на две части, подвергается воздействию двух необратимых по отдельности преобразований и последующей передачи по двум различным маршрутам к месту назначения. Как и в случае описанной в начале раздела системы, перехват одного из сообщений не приводит к вскрытию всей системы. В отличие от классической схемы в данной схеме используемые преобразования, которым подвергается текст, не имеют секретных ключей. Секретность основана в большей степени на отсутствии полной наблюдаемости, поэтому теоретически такая система может оказаться менее надежной. С другой стороны, такая система более эффективно использует оба маршрута, так же как и схема Ефимова-Файзуллина, а при надлежащей модификации может оказаться трудно вскрываемой. Надежность системы должна быть детально исследована.

1. Система с двумя маршрутами

Пусть $S = (s_1, s_2, \ldots, s_{2N})$, $S \in \mathbb{Z}_2^{2N} = \{0,1\}^{2N}$ — исходное сообщение, упорядоченный набор нулей и единиц, $|S| = 2N$ – длина сообщения.

Алгоритм приема-передачи сообщения состоит из 5 этапов.

1. Расщепление. Возможны несколько вариантов деления сообщения на две части. Используется в данной схеме побитовое расщепление, так что $S_1 = (s_1, s_3, \ldots, s_{2N-1})$ и $S_2 = (s_2, s_4, \ldots, s_{2N})$ — две части передаваемого сообщения.

2. Преобразования. Зададим две функции

$$F_1(S_1, S_2) = S_1 \oplus S_2,$$

$$F_2(S_1, S_2) = S_2 \oplus (S_1 \ggg 1),$$

где $\oplus$ – побитовая операция «исключающее ИЛИ»; $X \ggg 1$ – циклический битовый сдвиг X вправо на одну позицию.

3. Прием-передача сообщений. Последовательность F_1 передается по первому маршруту, а F_2 — по второму маршруту. Вариант технической реализации, не использующий промежуточных активных узлов, описан в разделе 4.

Принимающая сторона получает в свое распоряжение пару (F_1, F_2), по которой необходимо восстановить исходное сообщение S.

4. Восстановление частей сообщения. Пусть $P = F_1 \oplus F_2$. Вычисляем $F_1 \oplus F_2 = S_1 \oplus S_2 \oplus S_2 \oplus (S_1 \ggg 1) = S_1 \oplus (S_1 \ggg 1)$. Получаем уравнение

$$S_1 \oplus (S_1 \ggg 1) = P \tag{1}$$

относительно S_1. Как будет показано в следующем разделе, если данное уравнение имеет решение $\widehat{S_1}$ (а в нашем случае оно заведомо имеется в силу конструкции F_1 и F_2), то оно может принимать лишь два значения $\widehat{S_1} = S_1$ или $\widehat{S_1} = \neg S_1$, где $\neg X$ означает побитовую инверсию.

Найдем $\widehat{S_2}$ по формуле $\widehat{S_2} = F_1 \oplus \widehat{S_1}$. В зависимости от значений, которые может принимать $\widehat{S_1}$, получим либо $F_1 \oplus S_1 = S_1 \oplus S_2 \oplus S_1 = S_2$, либо $F_1 \oplus \neg S_1 = S_1 \oplus S_2 \oplus \neg S_1 = \neg S_2$.

5. Сборка. $\widehat{S}$ получается объединением $\widehat{S_1}$ и $\widehat{S_2}$ по правилу обратному расщеплению. В зависимости от того, какое из решений было выбрано на четвертом этапе, получаем либо $\widehat{S} = S$, либо $\widehat{S} = \neg S$. Исходное сообщение восстанавливается с точностью до побитовой инверсии.

2. Теоретическое обоснование

Теорема 1. *Пусть $X = (x_1, \ldots, x_n)$ и $P = (p_1, \ldots, p_n)$, $X, P \in \mathbb{Z}_2^n$, тогда уравнение*

$$X \oplus (X \ggg 1) = P \tag{2}$$

либо не имеет решений, либо имеет единственное решение с точностью до битовой инверсии.

Доказательство.

1. Пусть $A = (a_1, \ldots, a_n)$ – решение уравнения (2). Рассмотрим тождество $x \oplus y = \neg x \oplus \neg y \ \forall x, y \in \mathbb{Z}_2$. Если положить $x = a_i$ и $y = (A \ggg 1)_i$, $i = \overline{1, n}$ и воспользоваться тождеством, то в точности получим побитовое выполнение уравнения (2), но уже для элементов $\neg A$.

2. Решение будем искать по следующей схеме: положим $a_1 = 1$, тогда

$$\begin{aligned}
(A \ggg 1)_2 = a_1 \quad &\Rightarrow \quad a_2 = p_2 \oplus a_1, \\
(A \ggg 1)_3 = a_2 \quad &\Rightarrow \quad a_3 = p_3 \oplus a_2, \\
&\ldots \\
(A \ggg 1)_n = a_{n-1} \quad &\Rightarrow \quad a_n = p_n \oplus a_{n-1}.
\end{aligned}$$

Если $p_1 = a_n \oplus a_1$, то данная система рекуррентных соотношений дает нам решение, удовлетворяющее (2). Второе решение получается, если взять другое начальное условие $a_1 = 0$.

3. Докажем единственность решения. Пусть A – решение уравнения (2) и существует решение B, отличное от A и инверсии A, то есть $B \neq A$ и $B \neq \neg A$. Добавив к обеим частям соотношений A, видим, что $A \oplus B \neq O$ и $A \oplus B \neq E$, где O – последовательность, целиком состоящая из нулей, E – последовательность,

целиком состоящая из единиц. $B \oplus (B \ggg 1) = P$, $A \oplus (A \ggg 1) = P$. Сложим последние два уравнения:

$$B \oplus (B \ggg 1) \oplus A \oplus (A \ggg 1) = P \oplus P,$$

$$B \oplus A = (B \ggg 1) \oplus (A \ggg 1),$$

$$A \oplus B = (A \oplus B) \ggg 1.$$

Последнее соотношение возможно тогда и только тогда, когда $A \oplus B = O$ или $A \oplus B = E$. Полученное противоречие доказывает единственность решения.

Так как решение единственно с точностью до инверсии, то второе решение, получаемое из рекуррентных соотношений, будет инверсией первого.

Легко увидеть, что если $p_1 \neq a_n \oplus a_1$, то решения не существует вне зависимости от начальных условий рекурсии. ■

Рекурсивная процедура, приведенная в доказательстве дает нам алгоритм решения уравнений вида (1) и завершает построение схемы разделения первого раздела.

Для разрешения неоднозначности, связанной с инверсией, предлагается в начало первого сообщения S добавить 1, тогда в рекурсии для решения (1) можно в качестве стартового бита всегда выбирать бит, равный единице, $a_1 = 1$.

Следствие 1. *Пусть* $X = (x_1, \ldots, x_n)$ *и* $P = (p_1, \ldots, p_n)$, $X, P \in \mathbb{Z}_2^n$,

$$X \oplus (X \ggg k) = P \tag{3}$$

не имеет решений или имеет единственное решение с точностью до битовой инверсии, если $(k, n) = 1$, *то есть* k *и* n *взаимно просты.*

Доказательство. В этой перестановке x_1 переходит в x_{1+k}, x_{1+k} в x_{1+2k}, x_{1+2k} в x_{1+3k} и т.д. Из теории чисел известно, что tk, $t \in \mathbb{Z}$ пробегает полную систему вычетов по модулю n, тогда и только тогда, когда $(k, n) = 1$. Следовательно, в этом случае будет существовать ровно один цикл в разложении перестановки циклического сдвига $(X \ggg k)$. Таким образом, все доказательство будет идентично доказательству теоремы 1 с соответствующими изменениями в схеме поиска решения, где индексы будут пробегать полную систему вычетов:

$$(A \ggg k)_1 = a_{\tau^{-1}(1)} \quad \Rightarrow \quad a_{\tau^{-2}(1)} = p_1 \oplus a_{\tau^{-1}(1)},$$
$$(A \ggg k)_{\tau^{-1}(1)} = a_{\tau^{-2}(1)} \quad \Rightarrow \quad a_{\tau^{-3}(1)} = p_{\tau^{-1}(1)} \oplus a_{\tau^{-2}(1)},$$

и т.д,

где $\tau^{-1} \in \mathbb{S}_n$ – перестановка обратная к $(\cdot \ggg k)$, действующая на множестве индексов $\{1, 2, 3, \ldots, n\}$.

Единственность следует из теоремы 1. ■

В заключении раздела сформулируем еще одну теорему, являющуюся обобщением предыдущих результатов.

Теорема 2. *Пусть* $X = (x_1, \ldots, x_n)$ *и* $P = (p_1, \ldots, p_n)$, $X, P \in \mathbb{Z}_2^n$, $\pi \in \mathbb{S}_n$ — *элемент симметрической группы перестановок, действующий на упорядоченное множество* X, *тогда уравнение*

$$X \oplus \pi(X) = P \tag{4}$$

либо не имеет решений, либо имеет не более 2^d, *где* d – *число циклов в разложении перестановки* π. ■

Доказательство повторяет доказательство теоремы 1, но для каждого цикла перестановки π в отдельности.

В частности, если $\pi = (1)(2)(3)\ldots(n)$ – тождественная перестановка, то уравнение (4) превращается $X \oplus X = P$, имеющее 2^n решений только для $P = 0000\ldots0$, для остальных значений P решений не существует.

Теорема 2 фактически использует понятие ключа шифра простой перестановки — им является перестановка π.

3. Многомаршрутная схема

Используя результаты раздела 2, построим схему многомаршрутной системы передачи данных.

Пусть $S = (s_1, s_2, \ldots, s_N)$, $S \in \mathbb{Z}_2^N = \{0,1\}^N$ — исходное сообщение, упорядоченный набор нулей и единиц, $|S| = N$ – длина сообщения, n – число маршрутов. Будем считать, что $n|N$, в противном случае дополним сообщение S случайными битами, так чтобы n было делителем N.

1. В начало сообщения дописываем 1. Используем побитовое расщепление, так что $S_1 = (s_1, s_{1+n}, \ldots, s_{N-n+1})$, $S_2 = (s_2, s_{2+n}, \ldots, s_{N-n+2})$, $\ldots$, $S_n = (s_n, s_{n+n}, \ldots, s_N)$.
2. Зададим функции
$$F_1 = S_1 \oplus S_2, \quad F_2 = S_2 \oplus S_3, \quad \ldots, \quad F_n = S_n \oplus (S_1 \ggg 1).$$
3. F_1 передается по первому маршруту, а F_2 — по второму маршруту и т.д. Принимающая сторона получает в свое распоряжение набор $(F_1, F_2, \ldots, F_n)$, покоторому необходимо восстановить исходное сообщение S.
4. Пусть $P = \bigoplus_{i=1}^n F_i$. Легко проверить, что $P = S_1 \oplus (S_1 \ggg 1)$. Решаем полученное уравнение относительно S_1 (символ $\widehat{\cdot}$ опускаем, так как решение единственно: старший бит сообщения установлен в единицу).
Находим остальные части исходного сообщения
$$S_2 = F_1 \oplus S_1, \quad S_3 = F_2 \oplus S_2, \quad \ldots, \quad S_n = F_n \oplus S_n.$$
5. Собираем S из полученных частей.

4. Техническая реализация

Система передачи реализована [1] в сети с двумя маршрутами, организованной на основе стека протоколов TCP/IP. Предложенная в предыдущих пунктах схема разделения может быть применена к ней непосредственно.

Предлагаем следующую схему, состоящую всего из четырех узлов (1):

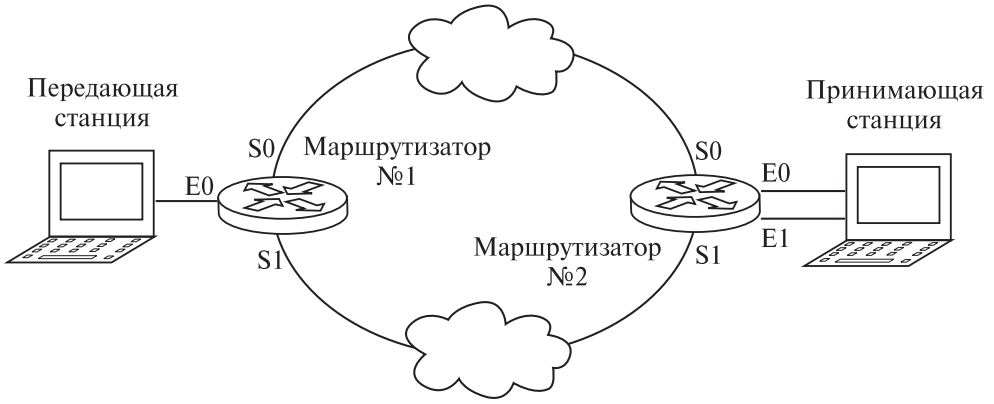

Рис. 1. Схема сети с двумя маршрутами.

1) передающая станция делит сообщение на две части, создает два соединения двумя сетевыми интерфейсами принимающей стороны. Пакеты первой части сообщения в IP-заголовке имеют адрес первого интерфейса, пакеты второй части – второго сетевого интерфейса;
2) маршрутизатор №1, статическая таблица маршрутизации настроена так, что пакеты на первый интерфейс принимающей стороны направляются через серийный порт S0, а на второй — через S1;
3) маршрутизатор №2 принимает пакеты и пересылает их принимающей станции;
4) принимающая станция собирает из пакетов два сообщения, а затем из них восстанавливает исходное сообщение. Станция должна иметь два сетевых интерфейса из различных подсетей.

5. Заключение

Стойкость схемы можно улучшить, если предварительно использовать один из оптимальных алгоритмов кодирования (например алгоритм Хаффмана), позволяющий выравнять статистические характеристики текста.

Вторая возможная модификация, повышающая стойкость к вскрытию, состоит в использовании циклических сдвигов как в F_2 так и в F_1,что при надлежащем выборе значений и отношению их к длине блока n может предотвратить возможность использовать для вскрытия значения корреляции между битами исходного сообщения.

Литература

1. Ефимов В.И. Файзуллин Р.Т. *Система мультиплексирования разнесенного TCP/IP трафика.* Математические структуры и моделирование. №10. 2002.
2. Шнаейр Б. *Прикладная криптография.* М.: Триумф. 2002. 816 с.