УДК 004.724.4(045)

КУЛАКОВ Ю.А.
МАКСИМЕНКО Е.В.,
РУЩАК О.А.

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В МОБИЛЬНЫХ СЕТЯХ

Рассмотрены вопросы повышения уровня безопасности в мобильных сетях. Предложен способ оптимального разбиения сообщения на отдельные блоки данных. Предложен алгоритм многопутевой маршрутизации для повышения безопасности передачи данных.

Questions of rise of level of safety in transportable networks are considered. The way of optimal splitting of the message on separate bulks is offered. The algorithm of multipath routeing for rise of safety of data transfer is offered.

Введение

В связи с расширением области применения мобильных компьютерных сетей, а также интеграции их в глобальные компьютерные сети, особую актуальность приобретает обеспечение безопасности передачи информации в сетях данного типа. Использование беспроводных каналов передачи, а также динамически изменяющаяся топология мобильных сетей не позволяют в полной мере использовать способы защиты информации, применяемые в сетях с проводными каналами связи и фиксированной структурой. Большинство существующих схем защиты информации для мобильных сетей ориентировано на обеспечение корректности маршрутной информации. В работах [1,2,3] предложены различные схемы защиты на уровне протоколов маршрутизации. Как правило, эти схемы предназначены для обеспечения корректности маршрутизации в мобильных сетях. Некоторые из них также включают решение проблемы некорректного поведения узла и способы обнаружения вторжения. В то же время практически ни одна из схем не рассматривает вопросы обеспечения безопасности самих передаваемых данных.

В данной работе предлагается передавать предварительно разбитое сообщение по нескольким путям.

На первом этапе производится разбиение сообщения на оптимальное количество частей. Для получения частей исходного сообщения используется пороговый алгоритм разделения секрета [4]. Пороговый алгоритм разделения секрета делит секретное сообщение на N частей, называемых *долями (share* или *shadow)* . При этом, имея в своем распоряжении любое число частей, меньшее T, нельзя получить никаких данных о секретном сообщении. В то же время при использовании

соответствующего алгоритма можно восстановить секретное сообщение из любого числа T (или больше) частей. Такой подход называют пороговой схемой разделения секрета (T, N) (threshold secret sharing). Таким образом, при использовании пороговой схемы разделения (T, N), секретное сообщение может быть разделено на N частей, при чем для того, чтобы перехватить сообщение, противник должен перехватить как минимум T частей. При перехвате числа частей меньше порогового, T, противник не может получить никаких данных о сообщении и фактически шансы его восстановить сообщение не больше, чем у того, кто вообще ничего не знает о сообщении. В рамках данной работы будет использована пороговая схема Шамира с использованием интерполяционных многочленов Лагранжа.

На втором этапе происходит выбор набора путей, соответствующих значений (T, N), и распределение частей на каждый из выбранных путей для достижения максимальной безопасности. Фундаментальная цель состоит в том, чтобы максимизировать безопасность путем распределения частей таким образом, чтобы противнику пришлось перехватить все пути, чтобы восстановить сообщение.

Формулировка проблемы

Предположим, что пороговый алгоритм разделения (T, N) применен к сообщению, которое нужно защитить, в исходном узле. Пусть на сетевом уровне есть всего M непересекающихся путей, путь *1*, путь *2*, …, путь M, доступных от источника до адресата. Для обозначения характеристик безопасности путей используется вектор $\underline{p} = [p_1, p_2, \ldots, p_M]$, где $pi(i= 1,2,\ldots,M)$ – это вероятность, что путь i скомпроментирован. Не отходя от обобщения, далее принимается $p_1 \le p_2 \le \ldots \le p_M$, что означает, что пути упорядочиваются от более безопасного до менее безопасного. При этом информация о безопасности пути p доступна в источнике из протоколов маршрутизации. Предполагается, что, если узел перехвачен, все части сообщения, проходящие через этот узел, перехвачены. Следовательно, путь скомпрометирован тогда, когда один или более любых узлов по пути скомпрометированы. Для каждого пути, предполагается, что, если он скомпрометирован, то все части сообщения, направленные по этому пути скомпрометированы. Поскольку используются непересекающиеся пути, то вероятность компроментации отдельного пути независима от вероятности компроментации других путей. Вероятности pi не включают вероятности того, что источник или адресат скомпрометированы, то есть, предполагается, что и источник, и адресат надежны.

Схема распределения используется, чтобы распределить N частей на M доступных путей. Обозначим распределение частей как $\underline{n} = [n_1, n_2, \ldots, n_M]$, где n_i – число частей, распределенных по пути i, n_i – целое число, $n_i \ge 0$,

$$\sum_{i=1}^{M} ni = N \qquad (1)$$

В соответствии с алгоритмом разделения, вероятность, что сообщение скомпрометировано, равняется вероятности, что *T* или больше частей скомпрометированы. Обозначим вероятность, что сообщение скомпрометировано как $P_{msg}(n)$. Тогда, распределение частей может быть сформулировано в виде проблемы оптимизации:

минимизировать $P_{msg}(n)$ при $\sum_{i=1}^{M} ni = N$,

n_i – целое число, $n_i \geq 0$.

Достижение максимальной безопасности без избыточности

Определим

$$r = 1 - \frac{T}{N} \qquad (2)$$

как коэффициент избыточности схемы разделения (*T, N*). Безизбыточной является схема с *r=0*, то есть *N = T*. При наличии *M* доступных путей и соответствующих характеристик безопасности, $\underline{p} = [p_1, p_2, \ldots, p_M]$, безизбыточная (*N, N*) (*N≥M*), схема разделения сообщения обеспечивает максимальную защиту, то есть, минимальную вероятность перехвата сообщения, когда не менее одной и не более *T-1* частей распределены по каждому из доступных путей, то есть

$$\begin{cases} 1 \leq n_i \leq T-1, \ i = 1, \ldots m \\ \sum_{i=1}^{m} n_i = N \end{cases} \qquad (3)$$

Это распределение вынуждает противника перехватывать все пути, чтобы перехватить сообщение. Вероятность перехвата равняется вероятности, что все пути скомпрометированы, т.е.

$$P_{msg}(\underline{n}) = \prod_{i=1}^{M} p_i \qquad (4)$$

Заметим, что максимальная безопасность зависит только от выбранных путей. Так как *pi* – вероятность, удовлетворяющая условию $0 \leq pi \leq 1$, то чем больше путей используется для распределения ресурсов, тем меньше вероятность, и тем более безопасна доставка сообщения. Таким образом, если требуемый уровень защиты γ_{Pn} , схема должна выбрать для доставки сообщения первые m путей, путь *1*, путь *2*, …, путь *m*, которые удовлетворяют условию

$$P_{msg}(\underline{n}) = \prod_{i=1}^{m} p_i \le \gamma_{Pn} \quad (5)$$

Для достижения максимальной безопасности с избыточностью, общее количество частей, распределенных по любым *m-1* или меньшему количеству путей, должно быть меньше чем *T*. Опять-таки, это распределение частей вынуждает противника перехватить все *m* путей, чтобы перехватить сообщение. Это также необходимое и достаточное условие для достижения максимальной безопасности.

Способ многопутевой маршрутизации

Рассмотрим алгоритм нахождения максимального количества путей, используемый для оптимизации набора путей для системы. Алгоритм использует частичное представление топологии сети, которое может быть предоставлено любым основным протоколом маршрутизации.

Предположим, что q_i – вероятность того, что узел перехвачен. Тогда вероятность того, что путь (s, t), состоящий из узлов *s*, n_1, n_2, …,n_l, скомпроментирован, равна

$$p = 1 - (1 - q_1) \cdot (1 - q_2) \cdot \cdots \cdot (1 - q_l) \quad (6)$$

Так как рассматривается безопасность сообщений во время передачи по сети, то предполагается, что источник и адресат надежны *qs=qd=0*. Вероятность *qi* показывает уровень защиты узла *i* и может быть оценена при помощи некоторого контролирующего программного обеспечения с обратной связью и/или аппаратных средств типа файерволов и устройств обнаружения вторжения. Вероятность также может быть назначена вручную администраторами на основании уровня физической защиты узлов, расположения или ранжирования узлов, и т. д. Например, штаб в тыле имеет самый высокий уровень защиты (наиболее низкое значение q_i), в то время как отдельные узлы, проникающие в зону неприятеля, будут иметь более низкий уровень защиты (высокое значение q_i).

В сети необходимо найти оптимальный набор путей, такой, чтобы вероятность P_{msg} была минимизирована. Вероятность перехвата сообщения

$$P_{msg}(\underline{n}) = \prod_{i=1}^{M} p_i$$

P_i – вероятность, которая всегда меньше чем 1. Чем больше частей p_i, тем меньше вероятность, и лучше защита. Таким образом, цель алгоритма поиска путей состоит в том, чтобы найти как можно больше путей, которые в то же время будут как можно более безопасными.

Алгоритм нахождения максимального количества путей, используемый для схемы распределения, является модификацией алгоритма алгоритма Дейкстры. Модифицированный алгоритм Дейкстры отличается от классического алгоритма тем, что позволяет помеченному узлу

вернуться к временной метке в случае нахождения к этому узлу пути с меньшей стоимостью. Для того, чтобы использовать модифицированный алгоритм нахождения кратчайшего пути во взвешенном графе, необходимо преобразовать характеристики безопасности отдельных узлов в совокупную функцию стоимости связи

Функция стоимости связи между узлами n_i и n_j определяется как:

$$c_{ij} = -\log\sqrt{(1-q_i)(1-q_j)} \tag{7}$$

Тогда, стоимость пути (s, t) при применении алгоритма поиска кратчайшего пути определяется как

$$\cos t(s,t) = c_{s1} + c_{12} + \ldots + c_{l-1,l} + c_{lt}.$$

учитывая, что источник и приемник надежны, т.е. $q_s = q_t = 0$

тогда

$$\cos t(s,t) = -\log\sqrt{(1-q_1)^2(1-q_2)^2\ldots(1-q_l)^2} =$$
$$= -\log((1-q_1)(1-q_2)\cdots(1-q_l))$$

значение $\cos t(s,t)$ будет минимально при минимальном значении f

$$f = -\log((1-q_1)(1-q_2)\cdots(1-q_l)),$$

которое минимально при максимальном значении произведения

$$(1-q_1)(1-q_2)\cdots(1-q_l)$$

Алгоритм поиска максимального числа заключается в следующем.

При поиске набора путей сначала находится первый самый безопасный путь при помощи модифицированного алгоритма Дейкстры. После этого выполняется преобразование графа следующим образом:

1. Для каждого выбранного пути связи, используемые в пути, заменяются направленными дугами - дуге, которая направлена к источнику, присваивается ее исходная стоимость со знаком «-»; дуге, направленной к адресату, присваивается бесконечная стоимость (таким образом дуга фактически удаляется, поскольку критерием выбора является минимальная стоимость дуги).

2. Каждый узел на выбранных путях (кроме источника и адресата) разбивается на два разнесенных подузла, соединенных дугой нулевой стоимости, направленный к узлу-источнику.

3. Каждая внешняя связь, соединенная с узлом на выбранном пути, заменяется двумя составными дугами со стоимостью, равной стоимости связи - одна дуга заканчиваться на одном подузле, а другая выходит от другого подузла таким образом, что вместе с дугой нулевой стоимости, не получается замкнутый цикл.

4. С помощью модифицированного алгоритма Дейкстры, нахождение самого безопасного пути в преобразованном графе.

5. Если больше не может быть найдено ни одного пути, то заканчиваем моделирование с сохраненным набором путей.

6. Выполняется преобразование графа к первоначальному виду; при этом удаляются чередующиеся ребра (ребра, соединяющие два узла и направленные в противоположные стороны); остающиеся ребра группируются для формирования нового набора путей.

7. Вычисляется общая безопасность нового набора путей, она сравнивается с безопасностью набора путей, полученного на предыдущей итерации.

8. Если новый набор путей не обеспечивает лучшую безопасность, чем предыдущий, то поиск заканчивается с сохраненным набором путей, в противном случае сохраняется найденный набор путей и осуществляется переход к первоначальной трансформации графа.

На рис. 1(а) показана первая итерация работы алгоритма, показан первый найденный путь. На рис. 1(б) изображена трансформация графа – каждый узел, кроме источника и адресата, заменяется двумя подузлами, соединенными дугой нулевой стоимости, направленной к источнику; каждая внешняя связь, соединенная с узлом на выбранном пути, заменяется двумя составными дугами со стоимостью, равной стоимости связи - одна дуга заканчивается на одном подузле, а другая выходит из другого подузла. На рис. 1(в) показана вторая итерация работы алгоритма, найден еще один путь. Рис. 1(г) иллюстрирует трансформацию графа уже для этого набора путей, и применение модифицированного алгоритма Дейкстры. На рис. 1(д) показана перегруппировка ребер и формирование окончательного набора путей. Рис. 1(е) иллюстрирует результирующий набор путей.

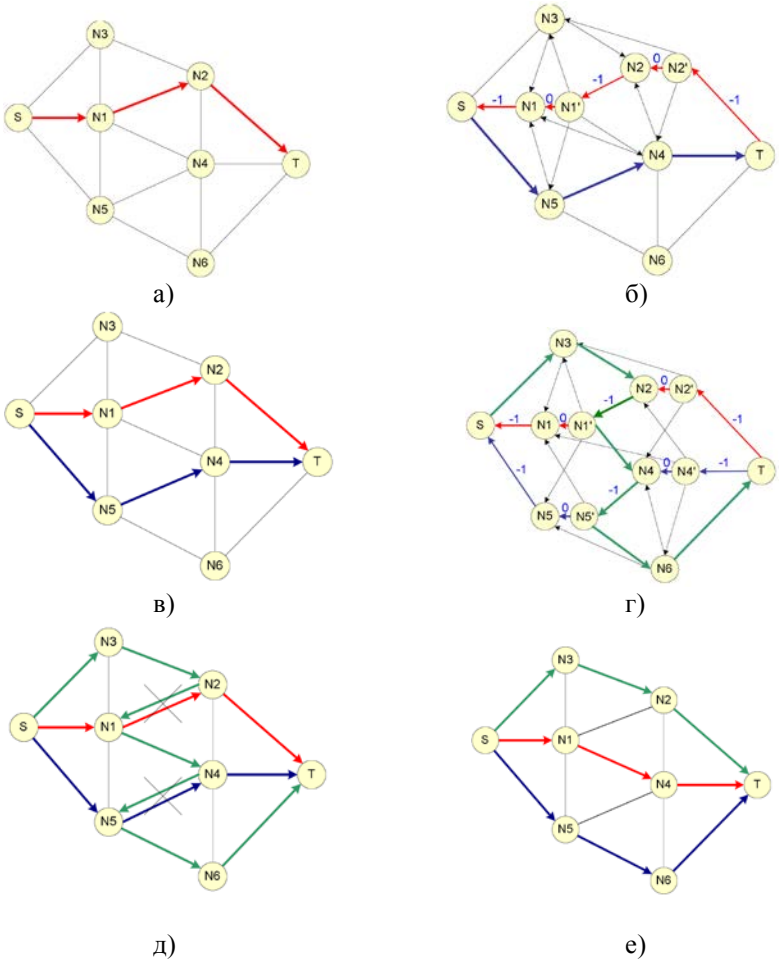

Рис.1

Использование многопутевой маршрутизации позволяет повысить защищенность информации при передаче ее по сети. Эффективность предложенного подхода зависит от топологии мобильной сети и степени ее узлов. При высокой степени узлов сети (порядка 15 и выше) передача информации по нескольким непересекающимся путям позволяет снизить вероятность перехвата передаваемой по сети информации, по сравнению с отправкой по одному пути, в среднем на 30%. При степени узлов от 6 до 12 выигрыш составляет порядка 20%. При степени узлов сети, меньшей 6, применение многопутевой маршрутизации дает те же самые результаты, что и применение однопутевой маршрутизации. Это объясняется тем, что

при этом слишком низка вероятность нахождения набора независимых путей.

Эффективность предложенного подхода также зависит от средней вероятности перехвата узлов. Как показали исследования, при средней вероятности перехвата узлов 0,3 на исследуемом диапазоне степеней (от 6 до 12) применение предложенного подхода дает выигрыш по безопасности порядка 12%.

Исследование вероятности того, что противник подслушает сообщение при передаче его по сети, также показало эффективность предложенного подхода. Применение многопутевой маршрутизации позволяет значительно снизить вероятность подслушивания сообщения (в среднем на 30%). Это снижение фактически зависит от количества используемых для доставки информации путей. Данная вероятность имеет некоторую нижнюю границу, что связано с тем, что противник, находясь в пределах зоны покрытия узла-источника или узла-приемника, может подслушать все части передаваемого сообщения.

Заключение

Предложен и разработан алгоритм нахождения приемлемого с точки зрения безопасности набора независимых путей для доставки сообщения.

Предложен и обоснован способ разделения передаваемого сообщения в исходном узле, и распределения полученных частей сообщения на выбранные пути позволяющий повысить безопасность передачи информации, и обеспечить в то же время определенный уровень надежности доставки информации путем введения некоторой избыточности.

Список использованных источников

1. Hu Y.-C., Johnson D. B., Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks // Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002) – 2002.- Calicoon(NY,USA)- P.3-13.
2. Papadimitratos P., Haas Z.J. Secure routing for mobile ad hoc networks // SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002) – San Antonio(TX, USA) - 2002
3. Venkatraman L., Agrawal D.P. Strategies for enhancing routing security in protocols for mobile ad hoc networks // Journal of Parallel and Distributed Computing – 2003-Vol.63, №2,P.214 – 227
4. Marti S., Giuli T., Lai K., Baker M. Mitigating routing misbehavior in mobile ad hoc networks // the 6th annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobi-Com'OO) - 2000 - Boston(MA, USA) - P.255-265