УДК 004.724.4(045)

Кулаков Ю.А., д-р техн. наук
Деревянчук А.О.

АЛГОРИТМЫ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ ДЛЯ МОБИЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Национальный технический университет Украины «КПИ»

Приведен краткий обзор безопасных протоколов маршрутизации для мобильных беспроводных Ad hoc сетей, а так же приведено новое решение задачи безопасной маршрутизации. Данная задача решается посредством выбора оптимального набора путей, обеспечивающего максимальную безопасность передачи сообщения

Введение

Проблема защиты информации крайне актуальна для мобильных *Ad hoc* сетей. Из-за особенностей *MANET* (*Mobile Ad hoc Networking*) для них не подходят многие схемы защиты, эффективные для проводных сетей. В работах [1-3], предложены различные схемы защиты на уровне протоколов маршрутизации. Как правило, эти схемы предназначены для обеспечения корректности маршрутизации в *Ad hoc* сетях. Некоторые их них также включают проблемы некорректного поведения узла [4-6], и способы обнаружение вторжения [7]. В то же время практически ни одна их схем не рассматривает вопросы обеспечения безопасности самих передаваемых данных.

Особенности маршрутизации в мобильных сетях

Маршрутизация в мобильных *Ad hoc* сетях сталкивается с дополнительными проблемами и сложностями по сравнению с маршрутизацией в традиционных проводных сетях с постоянной инфраструктурой. Проблема маршрутизации в такой среде усложняется за счет следующих факторов: быстрое изменение топологии, высокая потребляемая мощность, низкая полоса пропускания и высокая частота появления ошибок [8]. Большая часть существующих протоколов маршрутизации базируется на одном их двух различных подходов – табличном (*table-driven*) или на подходе "от источника по запросу" (*source-initiated on demand*).

Сравнение протоколов маршрутизации

Протоколы маршрутизации решают проблемы безопасности в *Ad hoc* сетях, основываясь на определенных предположениях, а так же выдвигают различные требования. В таблице 1 приведены результаты сравнения различных протоколов. Можно сделать вывод, что большинство протоколов требуют наличия третьего *online*-сервера. Он участвует в подтверждении прав доступа, служит для облегчения сбора, проверки подлинности открытых ключей. Под эту категорию попадают следующие протоколы: *ARAN, SAD, SEAD, SAODV*, в протоколах *TIARA* и защищенном протоколе маршрутизации по запросу *Resilient to Byzantine Failures* разработаны и детально описаны множество правил, а *IPsec* базируется на созданном наборе методов защиты. Кроме того, защищенный протокол маршрутизации по запросу *Resilient to Byzantine Failures* требует наличия закрытых ключей на всех вершинах пути от вершины-отправителя до вершины-премника. Каждая промежуточная вершина используется для подтверждения приема принимаемых пакетов. Как альтернатива, применяются протоколы *SAR* и *IPsec*, которые используют заранее рассчитанные данные, скрываемые каждым узлом, для обмена сообщениями между каждой парой вершин. Функциональные требования к *SRP* похожи, поскольку требуют заранее подготовленное защищенное соединение между источником и узлом-назначением.

Таблица 1.

Предложенное решение	Описание
ARAN	Доверительная *online* сертификация полномочий. Каждый узел знает открытый ключ CA.
SAR	Распределение ключей или использование секретного распределительного механизма.
SRP	Существование защищенной связи между каждый из приемников и отправителей. Вершины, которые используют злоумышленники, не используются уже после первого шага работы протокола.
SEAD	Синхронизация по времени либо защищенный секрет между каждой парой узлов.
Ariadne	Синхронизация по времени и защищенный секрет между каждой парой узлов. Для каждой вершины ключ аутентификации *TESLA*, правило поиска аутентификации для каждой из цепочки вершин, используемых при маршрутизации. *TESLA* ключи передаются участвующим узлам через online центр распределения ключей в криптографии.
SAODV	*Online* схема распределения ключей для сбора и проверки открытых ключей.
TIARA	*Online* инфраструктура открытых ключей.
Resilient to Byzantine Failures (защищенный протокол маршрутизации по запросу)	*Online* инфраструктура открытых ключей и скрытые симметричные ключи между источником и промежуточными вершинами.
SLSP	Узлы должны иметь открытые ключи, сертифицированные *TTP*. Отсутствие коллизий между узлами, используемыми злоумышленниками.
BISS	Узел-назначение найденного маршрута должен разделять все секретные ключи с промежуточными узлами. Доверительная *offline* аутентификация сертифицирует все открытые ключи промежуточных узлов.
Watchdog and Pathrater	Отсутствие коллизий между узлами, используемыми злоумышленниками.
CONFIDANT	Узлы не могут менять свой идентификатор, чтобы изменить свой приоритет. Предопределен список дружественных вершин.
Сдерживание пакетов: временное	Чрезвычайно точная синхронизация по времени.
Сдерживание пакетов: географическое	Информация о географической позиции, и не жесткая синхронизация по времени.
IPSec	Заранее подготовленная секретная информация между каждой парой вершин, или доверительный *online* сервер.

Функциональные требования к *SRP* похожи, поскольку требуют заранее подготовленное защищенное соединение между источником и узлом-назначением. Протокол *SEAD* требует, чтобы была схема распространения ключей для опознавания каждого элемента цепочки хеширования между двумя узлами. Может быть реализовано с помощью механизма подтверждения подлинности на основе широковещательной рассылки такого как *TESLA*, который требует, чтобы вершины сети имели часы для синхронизации. *Ariadne* требует наличия как закрытых ключей на обеих вершинах для подтверждения подлинности при *point-to-point* передаче сообщений, так и синхронизацию по времени, идентичную механизму *TESLA*, для аутентификации широковещательных сообщений. И, наконец, для расширенного протокола *Watchdog and Pathrater* необходимо, чтобы никакие две или больше вершин не были захвачены злоумышленниками для предотвращения возможных сетевых атак.

Предлагаемое решение

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 [1-3]. 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. Для 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.

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 p_i (i=1,2,…,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 p_i 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, $n_i \ge 0$,

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

В соответствии с алгоритмом разделения, вероятность, что сообщение скомпрометировано, равняется вероятности, что T или больше частей скомпрометированы. Обозначим вероятность, что сообщение скомпрометиро-

вано как $P_{msg}(n)$. Тогда, распределение частей может быть сформулировано в виде проблемы оптимизации: минимизировать $P_{msg}(n)$ при $\sum_{i=1}^{M} n_i = N$, 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) ($N \geq M$), 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 p_i – вероятность, удовлетворяющая условию $0 \leq p_i \leq 1$, 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

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

Достижение максимальной безопасности с избыточностью

Для достижения максимальной безопасности, 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. Это условие может быть упрощено и представлено в виде

$$\begin{cases} N - n_i < T, \ \forall i \in (1,2,\ldots m) \\ n_1 + n_2 + n_3 + \ldots + n_m = N \end{cases}. \qquad (6)$$

Т.е. $\begin{cases} n_i > N - T, \ \forall i \in (1,2,\ldots m) \\ n_1 + n_2 + n_3 + \ldots + n_m = N \end{cases}$,

$$\begin{cases} \sum_{i=1}^{m} n_i > \sum_{i=1}^{m} (N-T) \\ n_1 + n_2 + n_3 + \ldots + n_m = N \end{cases} \Rightarrow$$

$$N > m(N-T);$$

разделим обе части уравнения на N

$$1 > \frac{m \cdot (1-T)}{N} \Rightarrow$$

$$1 > m \cdot (1 - \frac{T}{N})$$

С учетом формулы (1),

$$1 - \frac{T}{N} < \frac{1}{m}$$

Таким образом, мы получаем необходимое условие достижения максимальной безопасности

$$r < \frac{1}{m}, \ (m \geq 2). \qquad (7)$$

Это условие определяет максимальную избыточность, которую можно добавить к схеме, не жертвуя безопасностью. Оно показывает, что для обеспечения максимальной безопасности,

максимальная избыточность, которую можно добавить к алгоритму разделения, ограничена условием $r < \frac{1}{m}$, где m – число выбранных путей ($m \geq 2$). Другими словами, можно утверждать, что для r-избыточной схемы распределения максимальная безопасность может быть достигнута, только если избыточность удовлетворяет условию $r < \frac{1}{m}$, ($m \geq 2$). Тогда, выбирая соответствующие значения (T, N), удовлетворяющие условию

$$T \geq N \cdot \frac{m-1}{m} + 1 \quad (m \geq 2) \qquad (8)$$

можно разработать оптимальную схему разделения, с помощью которой будет обеспечена и максимальная безопасность, и некоторая избыточность r. Любое распределение, удовлетворяющее ограничениям

$$\begin{cases} N - T + 1 \leq n_i \leq T - 1, \ i = 1, \ldots m \\ \sum_{i=1}^{m} n_i = N \end{cases} \qquad (9)$$

является оптимальным с точки зрения безопасности. Использование оптимального распределения вынуждает противника перехватить все пути, чтобы перехватить сообщение, и при этом допускается потеря во время передачи некоторого числа $(N\text{-}T)$ частей.

Заключение

Предложен способ повышения безопасности передачи сообщений в беспроводной сети – передача частей сообщения по некоторому набору независимых путей. Оговорен способ разбиения сообщения на части. Также представлены не только теоретические выкладки по достижению максимальной безопасности, но и учтена реальная составляющая процесса радиообмена, требующая введения некоторой избыточности. Таким образом выведен коэффициент избыточности и определен его диапазон, при котором безопасность будет на максимальном уровне.

Список литературы

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 Computting. – 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 (MobiCom'OO). – 2000. – Boston(MA, USA). – P. 255–265.

5. *Corner M.D., Noble B.D.* Zero-interaction authentication // The 8th ACM International Conference on Mobile Computing and Networking (MobiCom'02). – Atlanta(GA,USA). – 2002. – P. 1–11.

6. *Sanzgiri K., Dahill B., Levine B. N., Shields C., Belding-Royer E.* A secure routing protocol for ad hoc networks //in Proc. 10th Int. Conf. Network Protocols (ICNP'02). – Paris(France). – 2002. – P. 78–89.

7. *Zhang Y. and Lee W.* Intrusion detection in wireless ad hoc networks // Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom'OO). – 2000. – Boston(MA,USA). – P. 275–283.

8. *E.M. Royer, and C.-K. Toh.* "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," IEEE Personal Communications, vol. 2. nov. 6, April 1999. – P. 46–55.