Transaction of Azerbaijan National Academy of Sciences, Series of Physical-Technical and Mathematical Sciences: Informatics and Control Problems, Vol. XXXIV, No.3, 2014
www.icp.az/2014/3-05.pdf

УДК 004.724

Ю.А. КУЛАКОВ, В.В. ЛУКАШЕНКО, А.В. КОГАН

СПОСОБ И СРЕДСТВА КОНСТРУИРОВАНИЯ ТРАФИКА НА ОСНОВЕ БЕЗОПАСНОЙ МНОГОПУТЕВОЙ МАРШРУТИЗАЦИИ В МОБИЛЬНЫХ СЕТЯХ

Рассмотрены вопросы конструирования трафика на основе многопутевой безопасной маршрутизации в мобильных сетях. Предложен способ формирования запасных маршрутов, максимально близких к основному пути передачи информации. Представлен алгоритм обхода узлов, скомпрометированных или исключенных из маршрута, с минимальной сквозной задержкой передачи. Приведен пример реализации данного алгоритма в рамках технологии GMPLS (Generalized Multi - Protocol Label Switching).

Ключевые слова: мобильные сети, многопутевой маршрут, вычислительный алгоритм

1. Введение. Мобильные одноранговые (adhoc) сети имеют самоорганизующуюся сетевую архитектуру, где набор мобильных узлов с беспроводными сетевыми интерфейсами могут образовывать временную сеть. Топология беспроводной сети может меняться быстро и непредсказуемо.

Характерной особенностью adhoc сети является ее динамичная топология, не стабильная инфраструктура, ограниченная мощность сигнала все это порождает ряд серьезных проблем при конструировании трафика в сетях данного типа. Ограниченная пропускная способность, ограничения энергопотребления, и безопасность являются серьезными проблемами в этих типах сетей.

Беспроводные технологии имеют принципиальный недостаток с точки зрения безопасности - доступ к беспроводной среде передачи данных не составляет особого труда. Передача информации по беспроводным каналам, используя один маршрут, позволяет злоумышленникам легко и без особых усилий получить доступ к передаваемой информации. В свою очередь, использование многопутевой маршрутизации [1] позволяет повысить уровень конфиденциальности, потому что данный способ маршрутизации существенным образом усложняет перехват всех частей сообщения, разделенных и отправленных через несколько путей между отправителем и получателем информации.

2. Обзор и анализ существующих решений. Существующие подходы по обеспечению безопасности adhoc сетей можно отнести к следующим категориям:

- Distributed Trust Models – модели распределённого доверия;
- Key Management Models – модели управления ключами;
- Intrusion Detection Systems – системы определения вторжения;
- Secure routing protocol Models – модели протокола безопасной маршрутизации;
- Multipath protocols – многопутевые протоколы.

Следует отметить, что большинство известных методов повышения безопасности в основном ориентированы на сети с фиксированной структурой. В частности, использование трудоемких решений по обеспечению безопасности, таких как инфраструктуры открытых ключей [2], не является эффективным из-за ограничения ресурсов в adhoc сетях. Также не эффективными являются методы, основанные на анализе топологии сети. В связи с этим одним из важнейших аспектов безопасности мобильных сетей является безопасная маршрутизация[3,4].

Сформулируем основные требования к *QoS* (Quality of Service) для маршрутизации в беспроводных сетях:

- минимальная загрузка сети служебной информацией;
- отсутствие зацикливания маршрутов;

- быстрая сходимость;
- построение маршрута (при необходимости) заданного качества;
- эффективное использование емкости батарей;
- поддержка однонаправленных каналов;
- отсутствие потери информационных пакетов.

Наиболее полно этим требованиям отвечает технология GMPLS (Generalized Multi – Protocol Label Switching).

Цель многопутевой маршрутизации – найти не один, а несколько путей от отправителя к получателю. Большинство известных методов многопутевой маршрутизации в мобильных компьютерных сетях в основном направлены на повышения качества передачи информации и обеспечения равномерной загрузки компьютерной сети и, как правило, не обеспечивают требуемого уровня безопасности передаваемой информации.

При использовании многопутевой маршрутизации целесообразно разбить исходящее сообщение на оптимальное количество частей с точки зрения безопасности передаваемой информации. С этой целью в работе [5] предлагается использовать пороговый алгоритм разделения сообщения. Он делит секретное сообщение на N частей, которые называются долями (*share* или *shadow*). При этом, при наличии любого числа частей, меньше чем T, невозможно получить никаких данных о секретном сообщении. В то же время, при использовании соответствующего алгоритма, можно восстановить сообщение из любого числа равного или больше T. Такой подход называют пороговой схемой разделения сообщения (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. Другая причина использования порогового разделения состоит в том, что генерация частей сообщения и реконструкция сообщения являются линейными операциями (схема Шамира с использованием интерполяционных многочленов Лагранжа) [6].

В работе [7] предложен способ безопасной многопутевой маршрутизации, который позволяет обеспечит максимально безопасную передачу информационных сообщений и равномерно загрузит все каналы связи. На рис.1 представлен пример множества непересекающихся путей, сформированных в соответствие с алгоритмом, предложенным в работе[8].

На сетевом уровне множество непересекающихся путей может быть представлено совокупностью виртуальных путей, например, с помощью технологии GMPLS-VPN (Generalized Multi – Protocol Label Switching –Virtual Private Network) [9].

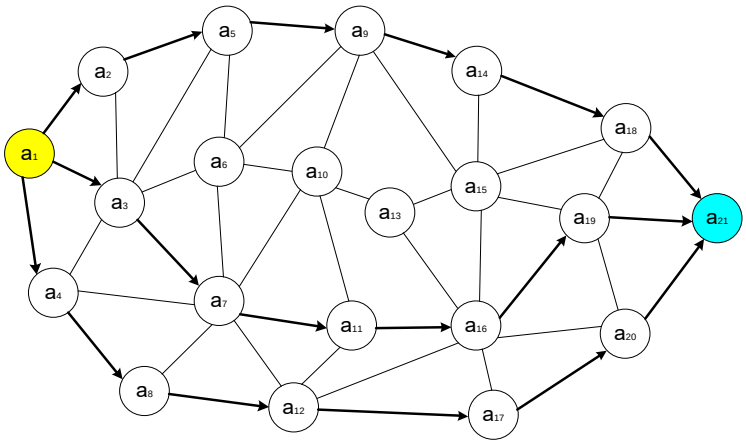

Рис.1 Множество непересекающихся путей

3. Постановка задачи. В связи с динамической структурой мобильной сети и большой вероятностью компрометации узлов актуальной является задача ремаршрутизации, связанная с поиском альтернативного пути, удовлетворяющего заданным параметрам качества передачи информации. В связи с этим возникает необходимость в разработке нового подхода к организации многопутевой безопасной маршрутизации.

4. Решение поставленной задачи. Одним из подходов к решению данной задачи является организация многопутевой структуры с обходом скомпрометированных узлов, используя запасные пути, минимально пересекающиеся с основными путями.

Для уменьшения времени задержки передачи информации в данной работе предлагается формировать запасные маршруты максимально близкие к основному пути.

С этой целью для каждого пути $l_i \in L_0=\{l_i|\ i=1,\dots n\}$ из множества основных путей строим ближайший один или два непересекающиеся с ним пути. В результате этого формируется множество дополнительных путей $L_n=\{l_j|\ j=1,\dots m\}$.

В предельном случае запасные пути могут принадлежать множеству L_0. В этом случае целесообразно выполнять процедуру обхода только «проблемных» узлов с возвращением на основной маршрут. Запасной путь строится как непересекающийся с основным путем, частично или полностью совпадать с каким-то другим путем множества L_0.

a_i – вершина сети $A_j=\{a_i|i=1,2,\dots k\}$ множества вершин пути l_j.

Пути l_j и l_m не пересекаются при условии $A_i \cap A_m=\varnothing$. Пути l_j и l_m частично пересекаются, если $A_j \cap A_m \neq \varnothing$.

Мощность множества пересекающихся узлов определяется количеством общих узлов пути. При одном общем узле мощность множества пересечения равна 1.

Рассмотрим формирования запасных путей (рис. 2).

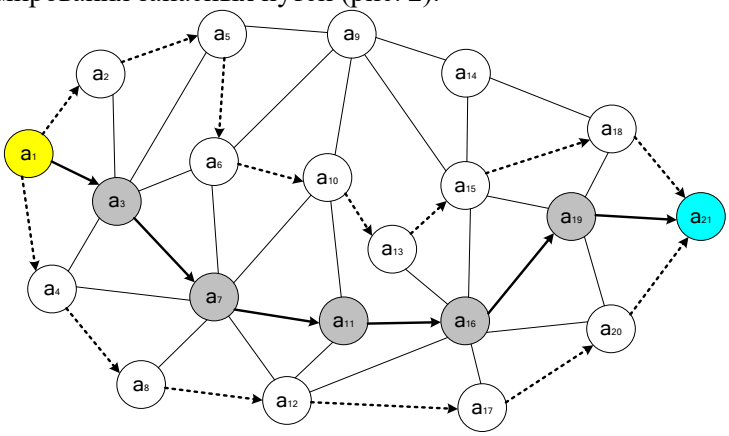

Рис. 2 Формирование запасных путей

При этом может формироваться два пути справа и слева от основного пути, при этом обход может осуществляться по одному или другому пути в зависимости от топологии графа. После обхода скомпрометированной вершины осуществляется переход с запасного на основной путь. На каждом шаге выбирается ближайшая следующая вершина запасного пути, связанная с текущей вершиной основного пути. Например, основной путь $l_0=(a_1>a_3>a_7>a_{11}>a_{16}>a_{19}>a_{21})$.

Для вершины a_3 ближайшими являются вершины a_2 и a_4. Для вершины a_7 ближайшие вершины a_6 и a_8. Для вершины a_{11} ближайшие вершины a_{10} и a_{12}. Для вершины a_{16} ближайшие вершины a_{13} и a_{17} и для вершины a_{19} ближайшие вершины a_{18} и a_{20}. На пути между вершинами a_{13} и a_{18} расположена вершина a_{15}, через которую и будет проходить кратчайший запасной путь.

В результате работы алгоритма формируется один основной путь l_0 и два запасных пути:

1) $l_1=(a_1>a_2>a_5>a_6>a_{10}>a_{13}>a_{15}>a_{18}>a_{21})$;

2) $l_2=(a_1>a_4>a_8>a_{12}>a_{17}>a_{20}>a_{21})$.

Поиск осуществляется на основе опроса соседних вершин по протоколу RIP [10]. Алгоритм сходится быстро, так как расстояние между вершинами не больше 6 переходов. Например, при выходе из строя вершины a_{19} – вершина ищет путь через вершину a_{20} – два перехода, и через вершину a_{15} – три перехода. Путь для передачи выбирается $a_{16}>a_{20}>a_{21}$.

После нахождения основного и двух запасных путей, рассмотрим пример передачи сообщения из узла a_i в узел a_j (рис. 3).

Рассмотрим пример успешной передачи информации:

1. Перед началом передачи информации узел a_i записывает сообщение в свой буфер передачи.
2. В момент времени t_1 узел a_i передает сообщение узлу a_j.

Время передачи сообщения исчисляется как:

$$T_{перед.} = \sum_{\substack{i=1 \\ j=i+1}}^{N-1} \tau_{i,j}$$

где: N – число промежуточных узлов;

$$\tau_{i,j} = t_j - t_1.$$

При $\tau_{i,j}$ =const= $\tau_{ср}$

$$T_{перед.} = (N-1)\tau_{ср.}$$

$$\tau_{ср.} = \frac{\sum_{i=1}^{N-1} \tau_i}{N-1}$$

3.В промежуток времени t_2–t_3 узел a_j обрабатывает информацию.

4. В случае успешного приема информации узел a_j в момент времени t_3 пересылает узлу a_i положительное подтверждение передачи (ACK).

5. В момент времениt_4 получив положительное подтверждение узел a_i удаляет сообщение из буфера.

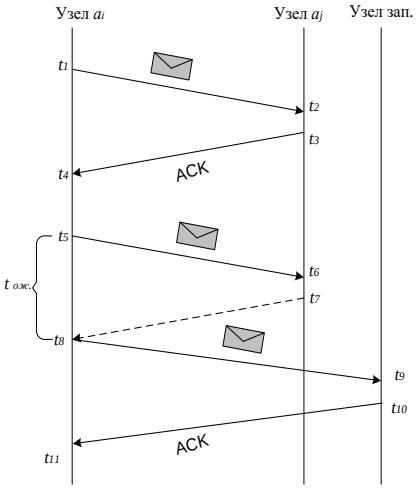

Рис. 3 Временная диаграмма передачи сообщения

В случае получения отрицательного подтверждения или отсутствия такого в интервал времени (t_7-t_8), сообщение направляется по запасному пути, осуществляя обход скомпрометированного узла.

Время задержки перехода:

$$T_{зад.перех.} = T_{пер.} + T_{обхода}$$

В рамках технологии GMPLS-VPN с целью возможного перехода с запасного пути на основной путь присваивание меток осуществляется следующим образом. Нечетная метка присваивается при передаче сообщения по основному пути, а четная присваивается при переходе на запасной путь. Таким образом, если на вход узла поступает сообщение с нечетной меткой, это соответствует тому, что сообщение движется по своему основному пути. При поступлении на вход узла сообщения с четной меткой это соответствует тому, что сообщение движется по запасному пути и необходимо попытаться вернуть его на основной путь.

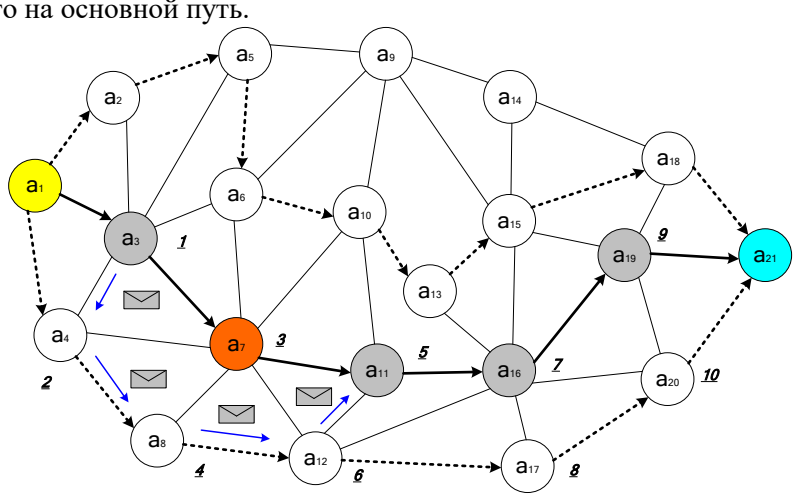

Рис. 4 Маршрутизация по меткам

На рис.4 узлам основного и запасного маршрутов присвоены соответствующие метки. Среднее время задержки зависит от близости запасных маршрутов к основному маршруту, коэффициента связности маршрутов, длинны маршрутов и вероятности компрометации узлов. Например, необходимо осуществить переходе с $a_3>a_7>a_{11}$, количество тактов равно T=2. Предположим, что вероятность компрометации узла $p_{a7}=1$, необходимо осуществить обход скомпрометированного узла через запасной путь $a_3>a_4>a_8>a_{12}>a_{11}$. Для этого нам понадобится T=4, количество тактов увеличивается на два. Коэффициент задержки перехода равен: $k = 1 + \frac{T}{N_{пер.}}$

Рассмотрим пример передачи сообщения по маршруту $a_7>a_{11}>a_{16}$. По основному пути количество тактов равно T=2. Допустим, что узел a_{11} скомпрометирован, и необходимо обойти его запасным путем$a_7>a_{12}>a_{16}$. Количество тактов по запасному пути не увеличилосьT=2.

Построение максимально близких путей минимизирует время задержки передачи данных. При максимальной связности путей задержка перехода равна нулю.

5. Выводы. В данной статье предложен способ и средства конструирования трафика на основе безопасной многопутевой маршрутизации в мобильных сетях. В качестве решения было предложено использовать запасные пути при отказе в работе узлов из основного маршрута. Такой подход значительно улучшил безопасность передаваемых данных, сбалансировал нагрузку на сеть и улучшил пропускную способность, позволяет минимизировать задержку передачи в случае использования запасных путей.

Литература

1. S. Saqaeeyan. Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks / S. Saqaeeyan, M. Roshanzadeh // Computer Network and Information Securit. – 2012. – №2. – pp. 8-14.
2. Madhusudan G. Novel Technique of Multipath Routing Protocol in Ad hoc Network / Madhusudan G, D.S.Vinod// International Journal of Computer Networks & Communications (IJCNC). - May 2012. - Vol.4, No.3. - pp.109-119.
3. T. Nirmal Raj. Secured Multi Path Routing with Trust Establishment Using Mobile Ad Hoc Networks /T. Nirmal Raj, S. Saranya, S. Arul Murugan, G. Bhuvaneswari // International Journal of Scientific & Engineering Research. – 2012. – Volume 3, Issue 1. – pp. 1-5.
4. S. G. N. Anjaneyulu. Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks / G. S. G. N. Anjaneyulu, V. MadhuViswanatham, B. Venkateswarlu // Advances in Applied Science Research. – 2011. - № 2 (4):177-186. - pp. 177-186.
5. Кулаков Ю.А. Многопутевая маршрутизация в беспроводных сетях / Кулаков Ю.А., А.В. Левчук // Електроніка та системи управління. – 2010. – № 4(26). – С. 142-147.
6. Zhou L., Haas Z. J. Securing ad hoc networks // IEEE Network Magazine – 2001- vol. 13, no. 6, pp. 24-30.
7. Кулаков Ю.А. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности / Ю.А. Кулаков, В.В. Лукашенко, А.В. Левчук // Защита информации. – 2011. – № 2 (51). – стр. 120-126.
8. Кулаков Ю.А. Разработка и моделирования процесса безопасной многопутевой передачи информации в мобильных сетях/ Кулаков Ю.А., Коган А.В., Пирогов А.А. // Вісник НТУУ «КПІ».Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+. – 2011. – № 54. – стр. 145-149.
9. Isaias Martinez-Yelmo. Modeling Traffic-Engineering VPN aggregation in GMPLS-based VPN networks / Isaias Martinez-Yelmo // 2004 IEEE International Conference, 07/2004. – pp. 1-9.
10. LydiaParziale. TCP/IP Tutorial and Technical Overview /Lydia Parziale, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews, Nicolas Rosselot // ibm, redbooks. – 2006. – pp. 1-1004.

UOT 004.724

Y.A. Kulakov, V.V. Lukaşenko, A.B. Koqan. Mobil şəbəkələrdə çoxyollu təhlükəsiz marşrutlaşma əsasında trafikin konstruksiya edilməsinin üsul və vasitələri.

İşdə mobil şəbəkələrdə çoxyollu təhlükəsiz marşrutlaşma əsasında trafikin konstruksiya edilməsinin üsul və vasitələrinin yaradılması məsələlərinə baxılmışdır. İnformasiyanın ötürülməsinin əsas yoluna maksimum yaxın olan ehtiyat marşrutların yaradılması üsulu təklif olunmuşdur. Marşrutdan kənar edilmiş qovşaqlardan yan keçməklə ötürmənin gecikməsini minimallaşdıran alqoritm yaradılmışdır. GMPLS (Generalized Multi-Protocol Label Switching) texnologiyası çərçivəsində bu alqoritmin realizasiyasını göstərən misal verilmişdir.

Açar sözlər: mobil şəbəkələr, çoxyollu marşrut, hesablama alqoritmi

Y.A. Kulakov, V.V. Lukashenko, A.B. Kogan. Method and means for designing of the traffic on the basis of safe multi-path routing in mobile networks.

In this paper, issues related to developing the method and means for designing of the traffic on the basis of safe multi-path routing in mobile networks are considered. The way of formation of the spare routes as much as possible close to the basic way of information transfer is offered. The algorithm of detour of the knots compromised or excluded from a route, with the minimum through delay of transfer is presented. The example of realization of the given algorithm within GMPLS (Generalized Multi-Protocol Label Switching) technology is resulted.

Keywords: mobile network, multi-path route, calculation algorithm

Национальный технический университет (Украина),
Киевский политехнический институт,
Национальный авиационный университет

Представлено 18.02.2014