УДК 004.724.4(045) **Кулаков Ю.А., Лукашенко В.В., Левчук А.В. (НАУ)**

БЕЗОПАСНАЯ МНОГОПУТЕВАЯ МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ СЕТЯХ БОЛЬШОЙ РАЗМЕРНОСТИ

В статье рассматриваются протоколы безопасной маршрутизации в беспроводных сетях, определяются их достоинства и недостатки в соответствии с заданными параметрами QoS и предлагается модифицированный способ безопасной маршрутизации, что позволит обеспечить безопасную передачу информационных сообщений и равномерно загрузит все каналы связи.

Ключевые слова: многопутевая маршрутизация, однопутевая маршрутизация, беспроводная сеть, безопасная маршрутизация.

Введение. Известные методы многопутевой маршрутизации в мобильных компьютерных сетях направлены на повышения качества передачи информации и обеспечения равномерной загрузки компьютерной сети [1] и, как правило, не обеспечивают требуемого уровня защиты информации.

Беспроводные технологии имеют принципиальный недостаток с точки зрения безопасности – доступ к беспроводной среде передачи данных не составляет особого труда. При этом следует отметить, что известные методы повышения безопасности в основном ориентированы на сети с фиксированной структуры.

Одним из важнейших аспектов безопасности сети является безопасная маршрутизация. В связи с этим сформулируем основные требования к *QoS* для маршрутизации в беспроводных сетях [2]:

- 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.

В работе [3] описаны два основных способа маршрутизации: однопутевая и многопутевая. Однопутевая маршрутизация подразумевает передачу информационного сообщения по одному наилучшему маршруту. Это наиболее простой способ маршрутизации, однако он не учитывает возможные «аварийные» ситуации и загрузку отдельных каналов, что может привести к перегрузке отдельных участков сети. Многопутевая маршрутизация отличается от протоколов однопутевой маршрутизации (таких как *OSPF* [4]) тем, что выбирается не один оптимальный путь к получателю, а формируется несколько путей для передачи. Следует отметить, что так называемые многопутевые равноценные подходы (*ECPM*) используют пересылку напрямую, позволяя использовать несколько путей с одинаковой минимальной стоимостью передачи и распределяют трафик равномерно по ним.

Одним из недостатков многопутевой маршрутизации является более значительный объем служебной информации по сравнению с однопутевой маршрутизацией. В настоящее время для уменьшения объема служебной информации, необходимой для решения задачи маршрутизации, в беспроводной сети используется *VPN* технология.

В связи с этим задача разработки безопасной многопутевой маршрутизации в беспроводных *VPN* сетях является актуальной.

Анализ протоколов безопасной маршрутизации. Многопутевые протоколы маршрутизации позволяют обеспечить конфиденциальность информации путем передачи разных частей информации по различным маршрутам. В работах [5], [6], [7] предложены способы защиты на уровне протоколов маршрутизации. Как правило, эти способы предназначены для обеспечения корректности маршрутизации в беспроводных сетях.

Сравнительный анализ протоколов безопасной маршрутизации для беспроводных сетей приведен в табл. 1.

Сравнительный анализ протоколов безопасной маршрутизации Таблица 1

	Преимущества	**Недостатки**
Ariadne	– уменьшение объема вычислений путем использования идентификационных кодов сообщения с симметричными ключами; – гарантируется истинность маршрутной информации; – защита от DoS-атак путем запроса маршрута.	– источник и адресат должны иметь общий ключ; – не производится шифрование данных; – задержки при доставке пакетов на прикладной уровень вследствие необходимости открытия ключа; – задержки при поиске маршрута.
CONFIDANT	– контроль за отправленным пакетом данных; – узлы не могут сами изменять свой приоритет; – удаление путей со скомпрометированным узлом/узлами; – обнаружение некорректного поведения узлов при маршрутизации.	– большой объем хранимых данных; – не предусмотрена возможность повторного включения в сети изолированных узлов (происходит только по таймауту); – возможно подслушивание и перехват данных.
SAR	– использование метрик безопасности; – найденные пути отвечают требованиям запрашиваемого уровня безопасности; – добавление цифровой подписи к пакетам.	– существенные накладные расходы в процессе маршрутизации; – значительные задержки при поиске пути; – при передаче данные не кодируются и могут быть подслушаны.
SRP	– узлы, которые используют злоумышленники, не используются уже после первого шага работы протокола; – регулирование процесса распространения запросов; – для обеспечения целостности сообщения используются MAC.	– изменяемые поля запроса передаются в открытом виде; – наличие безопасной связи между источником и адресатом.

Постановка задачи. Для повышения уровня безопасности передачи информации в беспроводных сетях необходимо сформировать множество непересекающихся путей. С этой целью в данной работе предлагается использовать способ разделения сообщений с помощью схемы Шамира.

Решение поставленной задачи. Для решения поставленной задачи, рассмотрим пример графа состоящий из 9 узлов (рис.1). В качестве алгоритма поиска кратчайшего пути используем алгоритм Дейкстры. В работе [8] рассмотрен пример работы алгоритма Дейкстры, который решает задачу о кратчайших путях из одной вершины для взвешенного ориентированного графа $G = (V, E)$ с исходной вершиной s, в котором веса всех рёбер неотрицательны ($\omega(u, v) \geq 0$ для всех $(u, v) \in E$).

Предположим, что q_i – вероятность того, что узел перехвачен. Тогда вероятность того, что путь $L_{1,l}$, скомпрометирован, равна:

$$p = 1-(1-q_1)\cdot(1-q_2)\cdot\ldots\cdot(1-q_l)$$

В качестве примера рассмотрим беспроводную сеть, состоящую из узлов и связей, соединяющих их, представленную в виде графа $G=(V,E)$, (рис. 1), где $V=\{v_i \mid i=1\ldots N\}$ множество вершина, $E=\{E_j \mid j=1\ldots M\}$ – множество связей между вершинами. Рассмотрим путь $L_{S,T}$ между вершинами S и T, включающий множество вершин $\{S, V1, V3, V5, T\}$.

В данном случае:

$$p = 1-(1-V_1)(1-V_3)(1-V_5)$$

Так как рассматривается безопасность доставки сообщения, то предполагается, что источник и адресат надежны $q_s = q_d = 0$. Вероятность q_i показывает уровень защиты i-го узла.

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

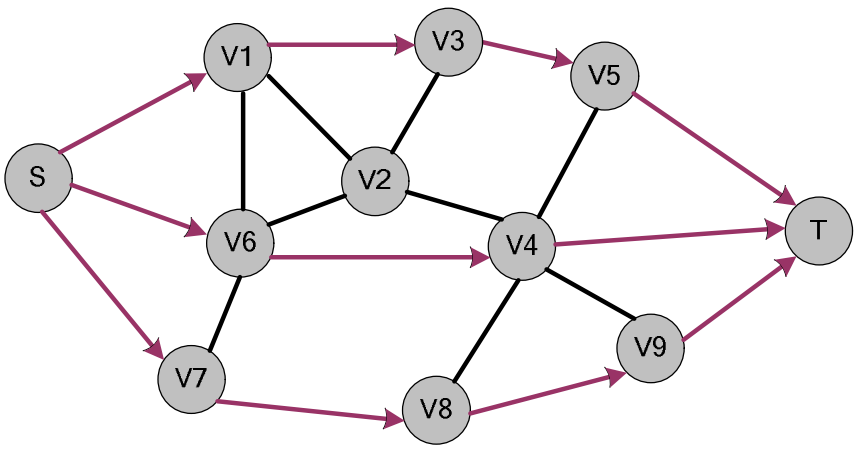

Рис. 1 Граф беспроводной сети

Вероятность перехвата сообщения равна:

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

где p_i – вероятность перехвата части сообщения. Чем больше частей p_i, тем меньше вероятность перехвата сообщения и лучше защита. Таким образом, цель алгоритма поиска путей состоит в том, чтобы найти как можно больше путей, которые в то же время будут наиболее безопасными.

Для наглядного примера рассмотрим способ нахождения оптимального набора путей в виде блок-схемы (рис. 2).

В работе [9] рассмотрены способы решения задачи безопасной маршрутизации на основе однопутевой и многопутевой маршрутизации. Предполагается, что многопутевая маршрутизация является оптимальным способом безопасности передаваемых данных.

В работе [10] предложен способ разделения секретного сообщения на части. Он делит сообщение на N частей, которые называются долями (*share* или *shadow*). При этом, при наличии любого количества частей, меньше T, невозможно получить никаких данных о секретном сообщении. В то же время при использовании соответствующего алгоритма можно восстановить сообщение из любого количества равного или больше T.

При выборе оптимального набора маршрутов необходимо учитывать несколько критериев: удовлетворить требования по задержкам и равномерно загрузить сеть. Существует два способа для выбора оптимального набора путей: оптимальное и жесткое распределение.

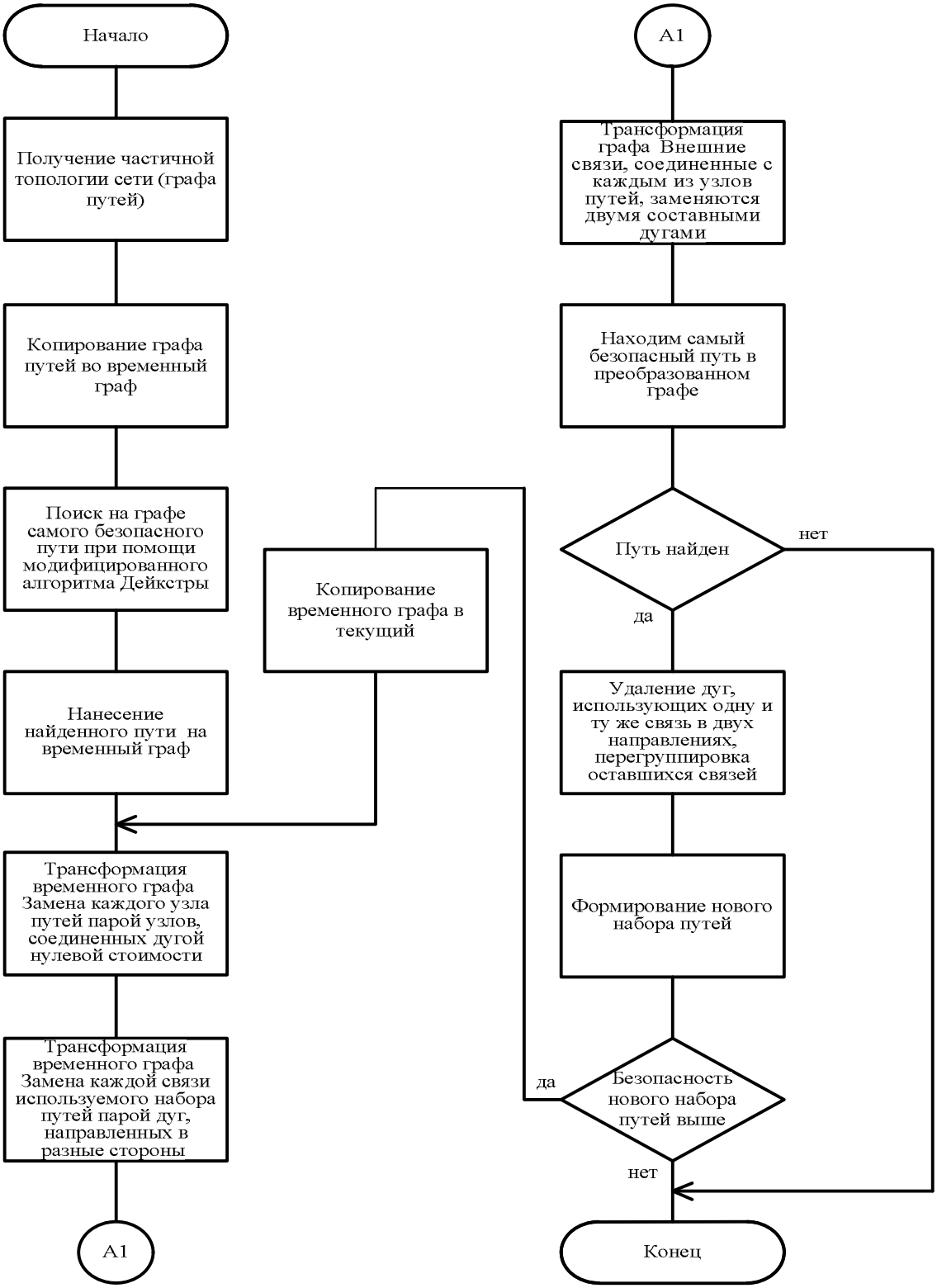

Рис. 2. Блок-схема алгоритма нахождения набора путей

Отличительной особенностью оптимального распределение является возможность деления сообщения на оптимальное количество частей, и по одному маршруту может быть передано несколько частей в зависимости от загруженности канала связи.
где - оптимальное распределение, - количество оптимальных маршрутов.

В отличие от оптимального распределения, жесткое распределение делит секретное сообщение на столько частей, сколько найдено оптимальных путей.

$$k = \frac{N_{ч}}{N_{п}}$$

где k – жесткое распределение, $N_{ч}$ - количество частей сообщения, $N_{п}$ – количество непересекающихся путей. В качестве служебного сообщения будем использовать секретное сообщение, что позволит при разбиении его на n+1 частей обезопасить все части сообщения.

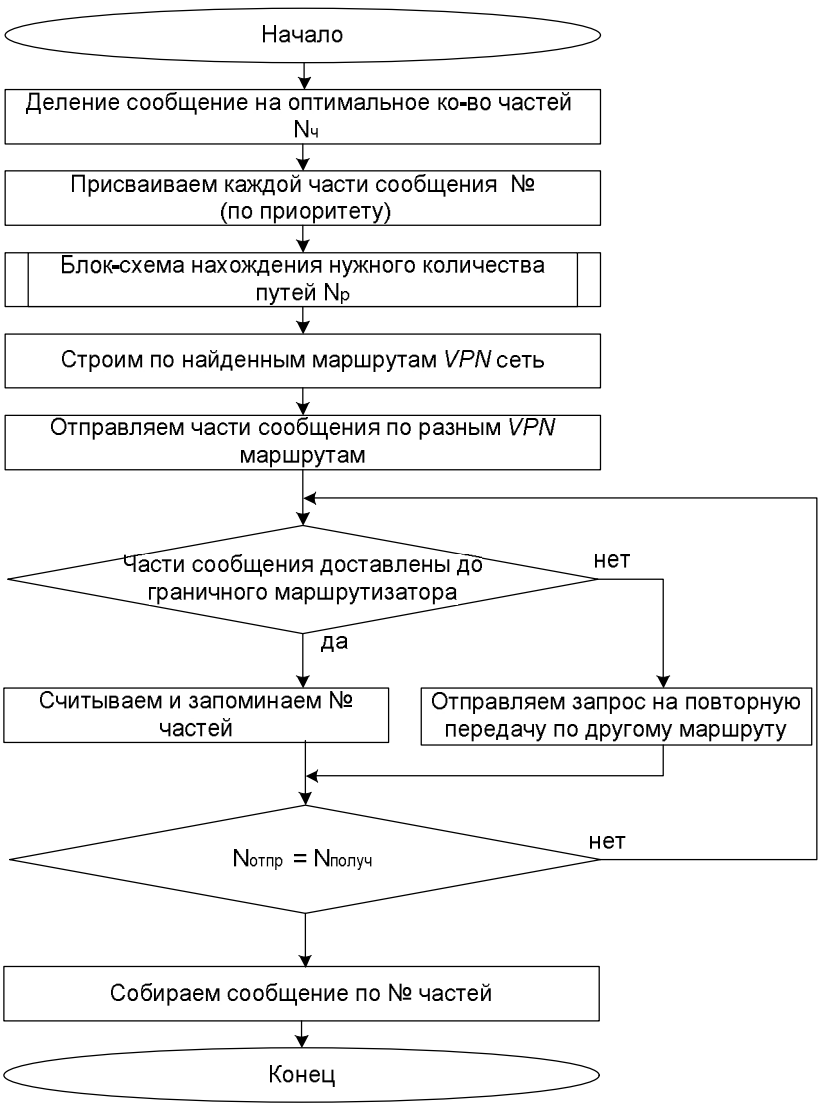

Рис. 3. Блок-схема безопасной маршрутизации

В результате можно сделать выводы, что при оптимальном распределении уровень безопасности ниже, однако удовлетворяет заданный уровень *QoS*. В отличие от оптимального, жесткое распределение не полностью обеспечивает *QoS,* однако обеспечивает максимальный уровень безопасности передаваемых сообщений.

При наличии всех частей секретного сообщения, выполняется проверка и сборка частей в единое целое исходное секретное сообщение. При недостачи некоторого компонента n, повторно передается запрос на повторную передачу недостающей части по другому маршруту, где время доставки одной части минимальное.

На рис. 4. представлен процесс жесткого распределения:

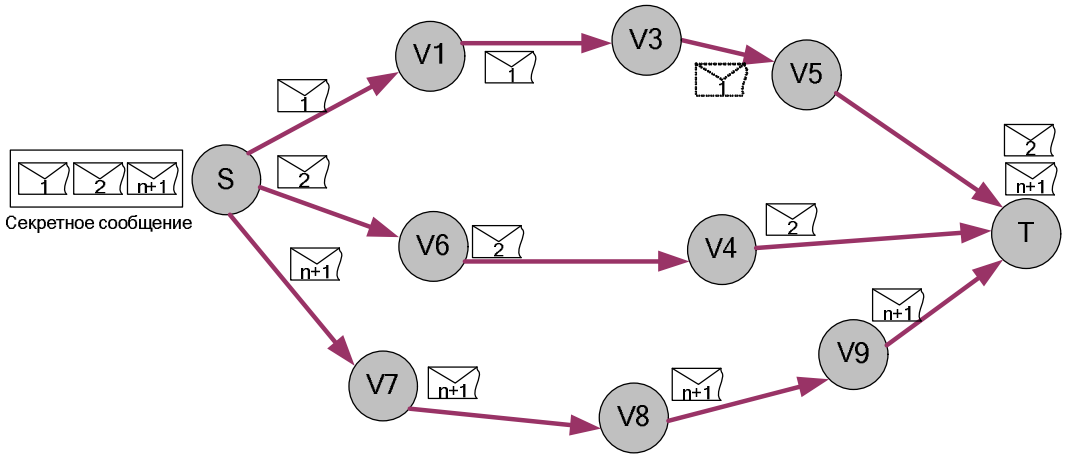

Рис. 4. Жесткое распределение

Выводы. Таким образом, предложенный в работе способ позволит на основе безопасной многопутевой маршрутизации создать модифицированную маршрутизацию, которая обеспечит максимально безопасную передачу информационных сообщений и равномерно загрузит все каналы связи.

Литература

1. Multipath optimized link state routing for mobile ad hoc networks Ad Hoc Networks / Jiazi Yi, Asmaa Adnane, Sylvain David and Benoît Parrein – Vol. 9, Issue 1, January 2011. – P. 28 – 47.

2. Лемешко А. В., Ахмад М. Хайлан. – Результаты исследования метода иерархическо координационной маршрутизации в mpls-сети. – Управління мережами і послугами телекомунікацій. – 2010. – №3(15). – 57-62.

3. Достиярова Алия Мухамедияровна. – Алгоритмы управления качеством обслуживания вызовов в ицсотс. – 2008. – №3(3). – 86-94.

4. Gojmerac, T. Ziegler, P. Reichl. Adaptive Multi-Path (AMP) – a Novel Routing Algorithm for Dynamic Traffic Engineering. Technical report FTW-TR-2008-007, Vienna, 2008.

5. Venkatraman L., Agrawal D.P. Strategies for enhancing routing security in protocols for mobile ad hoc networks. Journal of Parallel and Distributed Computing, Vol.63., 2003, P.214 – 227.

6. Marti S., Giuli T., Lai K., Baker M. P. Mitigating routing misbehavior in mobile ad hoc networks., The 6th annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobi-Com'OO), 2000, 255-265.

7. Ю. А. Кулаков, А. А. Деревянчук. Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей. Вип.3(27), Проблеми інформатизації та управління: Зб.наук.пр.– К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2009. – С.99-103.

8. Кулаков Ю. А. Безопасная передача информации на основе многопутевой маршрутизации / А. Ю. Кулаков, А. О. Деревянчук // Вісн. Нац. техн. ун-ту України "КПІ": Інформатика, управління та обчислювальна техніка: зб. наук. праць. – 2009. – № 51. – С. 125 – 129.

9. И.Н.Давиденко, А.В.Левчук. Способ организации динамической структуры мобильной компьютерной сети большой размерности. Интеллектуальный анализ информации: сб. трудов. – К.: «Просвита», 2009г. – С.94-103.

10. Ю. А. Кулаков, А. В. Левчук. Многопутевая маршрутизация в беспроводных сетях. Вып. 4 (26), Проблеми інформатизації та управління: Зб.наук.пр.– К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2010. – С.142-147.

Надійшла: 26.05.2011 р.

Рецензент: д.т.н., проф. Юдін О.К.