Системы телекоммуникации, связи и защиты информации

УДК 004.724.4(045)

Ю.А. Кулаков, д-р.техн.наук, **А.В. Коган**
Национальный технический университет Украины" Киевский политехнический институт",
пр. Победы 37, Киев-56, 03056, Украина.

Способ минимизации времени обхода скомпрометированных узлов в мобильных сетях

В работе предложен способ обеспечения заданных параметров качества обслуживания QoS в случае вынужденной реконфигурации маршрута. 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 информации. Библ. 6, рис. 5.

Ключевые слова: *многопутевая маршрутизация, параметры качества обслуживания QoS, беспроводные сети, конструирования трафика, смежные вершины, запасные пути.*

Введение

Передача информации по беспроводным каналам, используя один маршрут, позволяет злоумышленникам, легко и без особых усилий получить доступ к передаваемой информации. Обеспечение безопасности передаваемых данных предполагает защиту данных от пассивных атак, таких как подслушивание. Традиционным способом для обеспечения конфиденциальности является шифрование передаваемых данных. А из-за отсутствия инфраструктуры проблематично управление ключами. Более серьезной проблемой в беспроводных сетях является то, что мобильные узлы обычно постоянно находятся в открытой и враждебной среде, где могут быть легко перехвачены. В этом случае, вся информация, хранящаяся в узлах, становится известна злоумышленнику, включая ключи, используемые для кодирования сообщения. Любая схема кодирования, независимо от того, насколько она безопасна, в данном случае не достаточно эффективна.

Таким образом, в связи с динамической структурой мобильной сети и большой вероятностью компрометации или поломки узлов актуальной является задача ремаршрутизации, связанная с поиском альтернативного пути, удовлетворяющего заданным параметрам качества передачи информации.

1. Обзор и анализ существующих решений

В настоящее время с целью повышения безопасности передачи информации широко используется многопутевая маршрутизация. В частности в работе [6] предлагается оптимальный алгоритм маршрутизации с маршрутизацией метрического сочетания обоих требований узла – надежность и производительность. В работе [3] предложен алгоритм динамической маршрутизации, который направлен на случайный поиск путей для передачи данных, в которых присуще сходство двух маршрутов, что в свою очередь позволяет увеличить безопасность передачи информации. В работе [4] разработаны два алгоритма Bound-Control и Lex-Control для оптимизации распределения данных между двумя путями. В работе [5] предложен тайный обмен распространения данных по нескольким путям и предлагается метод безопасной оптимизации данных.

Многопутевая маршрутизация так же обеспечивает балансировку нагрузки и защиту от отказов путем распределения трафика по множеству непересекающихся путей [1, 2] (рис.1). Данный подход эффективен при высоком уровне доверия к узлам сети и относительно стабильной структуре сети. В случае, когда узел скомпрометирован или не доступен, при многопутевой маршрутизации происходит исключение данного маршрута или его реконфигурация. В первом случае узел - отправитель информации осуществляет повторную передачу информации по новому пути. Во втором случае инициируется процедура локальной ремаршрутизации. В том и другом случае это приводит к задержкам в передачи информации. Например, при необходимости обхода узла $в_{14}$, узел $в_9$ определяет

ближайший к узлу $в_{14}$ узел на пути к получателю информации, в данном случае это узел $в_{18}$. Затем узел $в_9$ осуществляет поиск кратчайшего пути к вершине $в_{18}$. В данном случае этот путь проходит через вершину $в_{15}$. Процесс повторяется до тех пор, пока не будет найдена первая не скомпрометированная вершина на исходном пути.

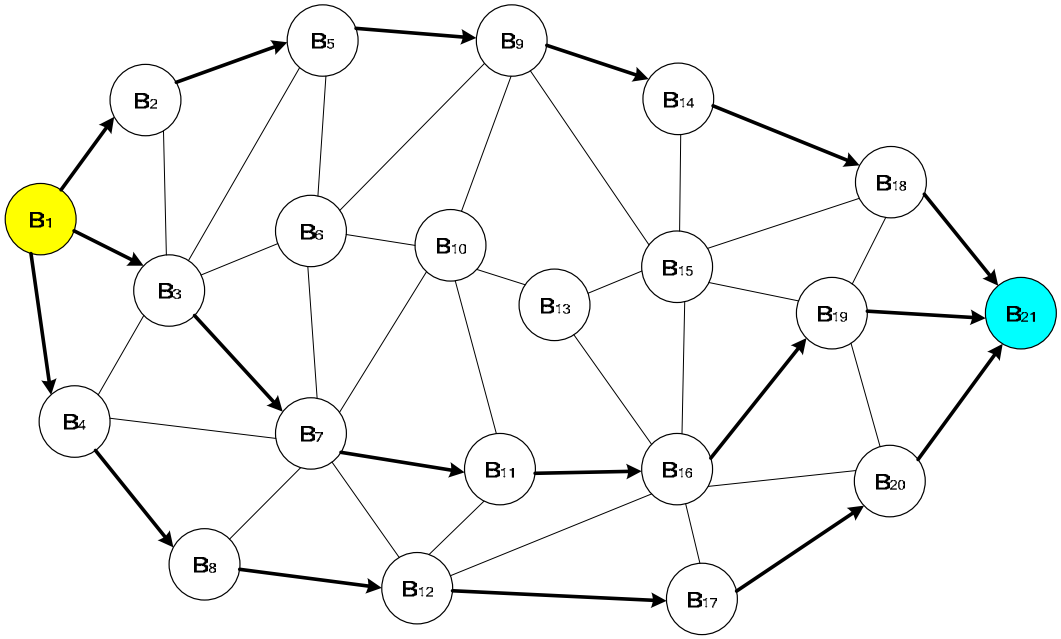

Рис. 1. Граф распределения трафика по множеству непересекающихся путей

На рис. 1 представлено множество непересекающихся путей, что позволит сбалансировать нагрузку на сеть и защитить передаваемую информацию от отказов узлов.

2. Решение поставленной задачи

В данной работе предлагается способ обхода скомпрометированных вершин с использованием заранее сформированных запасных путей, минимально пересекающихся с основным путем.

Для уменьшения времени задержки передачи информации в данной работе предлагается для основного пути $l_i \in L_0=\{l_i|\ i=1,\ldots n\}$ формировать множество дополнительных путей $L_n=\{l_j|\ j=1,\ldots m\}$, максимально близких к множеству основных путей $L_0=\{l_i|\ i=1,\ldots n\}$. Каждый путь l_j будем определять множеством $B_j=\{в_i|i\ =1,2,\ldots k\}$ входящих в него вершин.

В общем случае, для каждого основного пути $l_i \in L_0$ может быть два максимально близких к нему запасных путей l_j и l_m, один из которых располагается слева, а второй справа от основного пути. В общем случае, 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. Если основной путь содержит хотя бы одну граничную вершину сети, то формируется только один запасной путь, максимально близкий к основному пути.

При организации многопутевой маршрутизации в предельном случае запасные пути могут принадлежать множеству L_0. При этом запасной путь строится как непересекающийся с основным путем, который может частично или полностью совпадать с каким- то другим путем множества L_0. В этом случае целесообразно выполнять процедуру обхода только «проблемных» узлов с возвращением на основной маршрут. Пути l_j и l_m не пересекаются при условии $B_i \cap B_m=\varnothing$. Пути l_j и l_m частично пересекаются, если $B_j \cap B_m \neq \varnothing$.

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

Суть способа заключается в формировании запасного пути на основании выбора очередной смежной вершины, максимально близкой одной из вершин основного пути. Выбор очередной вершины осуществляется на основании операций над множествами смежных вершин.

3. Алгоритм формирования запасных путей заключается в следующем

На первом этапе формируется множество вершин $B_0 = \{в_i | \ i = 1,\ldots,n\}$ основного пути.

Для начальной вершин $в_i \in B_0$ множества вершин основного пути L_0 формируется множество смежных с ней вершин $B_{Si} = \{в_j | \ j = 1,\ldots,k\}$.

Для каждой вершины $в_j$ множества $B_{Si} = \{в_j | \ j = 1,\ldots,m\}$ формируется соответствующее множество смежных с ней вершин $B_{Sk} = \{в_k | k = 1,\ldots,r\}$.

Для $j = 1,\ldots,m$ выполняется операция пересечения множеств $B_{Sj} = B_0 \cap B_{Sk}$.

Среди полученных множеств выбирается множество B_{Sp} с максимальной степенью, соответственно, в качестве очередной вершины запасного пути выбирается вершина $в_p$

Если вершина $в_p$ является конечной вершиной основного пути, то переход к пункту 8.

Для вершины $в_p$ формируется множество смежных с ней вершин

$B_{Si} = \{в_j | \ j = 1,\ldots,k\}$. Переход к пункту 3.

Рассмотрим способ формирования запасных путей на примере графа, представленного на рис. 2.

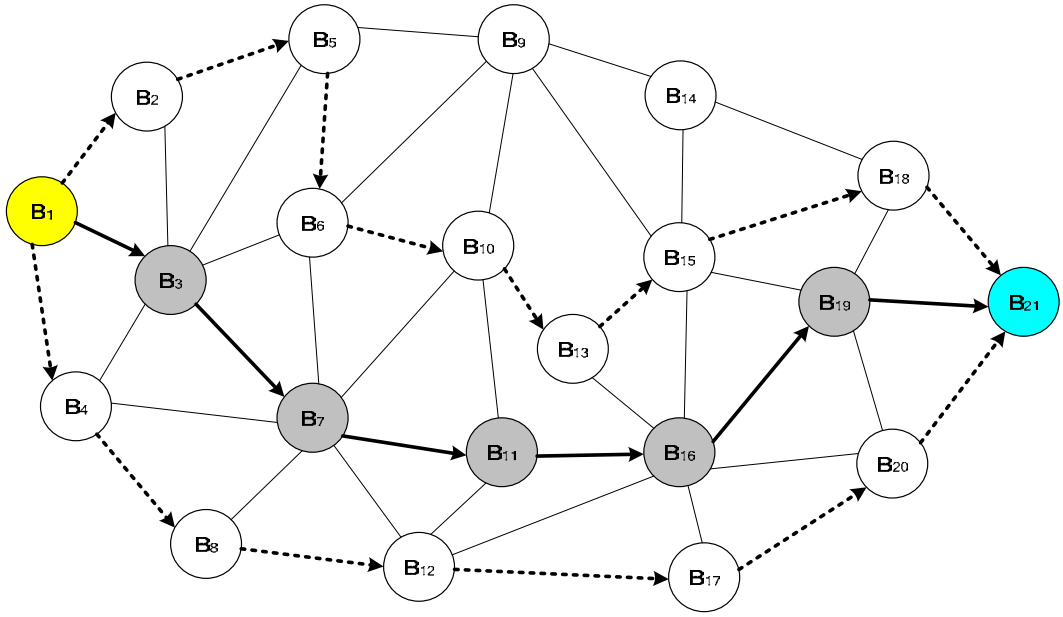

Рис. 2. Граф формирования запасных путей распределения трафика в беспроводной сети

На рис. 2 представлен граф беспроводной сети, где основной путь представлен в виде множества темных узлов, а пунктирными линиями два запасных пути.

3.1. Формирование первого запасного пути

Формируем множество вершин основного пути $B_0 = \{в_1, в_3, в_7, в_{11}, в_{16}, в_{19}, в_{21}\}$.

Для начальной вершин $в_1 \in B_0$ множества вершин основного пути L_0 множество смежных с ней вершин $B_{S1} = \{в_2, в_4\}$.

Для вершин a_2 и a_4 множество смежных вершин соответственно равны: $B_{S2} = \{в_1, в_3, в_5\}$, $B_{S4} = \{в_1, в_3, в_7, в_8\}$.

Определяем пересечение множеств $B_2 = B_0 \cap B_{S2} = \{в_1, в_3\}$, мощность данного множества равна 2. Соответственно, пересечение множеств $B_4 = B_0 \cap B_{S4} = \{в_1, в_3, в_7\}$. Мощность данного множества равна 2.

В качестве очередной вершины запасного пути выбирается вершина $в_4$.

Для вершины $в_4$ множество смежных с ней вершин, не принадлежащих основному пути равно $B_{S4} = \{в_8\}$, поэтому в качестве следующей вершины выбирается вершина $в_8$.

Для вершины $в_8$ множество смежных с ней вершин, не принадлежащих основному пути равно $B_{S8} = \{в_{12}\}$. В качестве следующей вершины выбирается вершина $в_{12}$.

Для вершины $в_{12}$ множество смежных с ней вершин, не принадлежащих основному пути равно $B_{S12} = \{в_{17}\}$. В качестве следующей вершины выбирается вершина $в_{17}$.

Для вершины $в_8$ множество смежных с ней вершин, не принадлежащих основному пути равно $B_{S17} = \{в_{20}\}$. В качестве следующей вершины выбирается вершина $в_{20}$.

Для вершины $в_{20}$ множество смежных с ней вершин, не принадлежащих основному пути равно 0. Первый запасной путь сформирован. Общее число переходов равно 6, что соответствует числу переходов основного пути.

3.2. Формирование второго запасного пути

Множество вершин основного пути B_0={ $в_1$, $в_3$, $в_7$, $в_{11}$, $в_{16}$, $в_{19}$, $в_{21}$}.

Для начальной вершин $в_1 \in B_0$ множества вершин основного пути L_0 множество смежных с ней вершин B_{S1}={$в_2$, $в_4$}.

Вершина $в_4$ была выбрана на предыдущем шаге, поэтому в качестве очередной вершины запасного пути выбирается вершина $в_2$.

Для вершины $в_2$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S2}={$в_1$, $в_3$, $в_5$}. Вершины $в_1$ ив$_3$, принадлежат основному пути, поэтому в качестве следующей вершины выбирается вершина $в_5$.

Для вершины $в_5$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S5}={$в_2$, $в_6$, $в_9$}. Вершина $в_2$ является входящей для вершины $в_4$, поэтому рассматриваются вершины $в_6$ и $в_9$.

Для вершин $в_6$ и $в_9$ множество смежных вершин соответственно равны:

B_{S6}={$в_3$, $в_5$, $в_7$, $в_9$, $в_{10}$} , B_{S9}={$в_5$, $в_6$, $в_{10}$, $в_{14}$}.

Определяем пересечение множеств $B_6=B_0 \cap B_{S6}$={$в_3$, $в_7$}, мощность данного множества равна 2. Соответственно, пересечение множеств $B_9=B_0 \cap B_{S9}=\varnothing$. Таким образом, в качестве следующей вершины запасного пути выбирается вершина $в_6$.

Для вершины $в_6$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S5}={$в_9$, $в_{10}$}.

Для вершин $в_{10}$ и $в_9$ множество смежных вершин соответственно равны: B_{S10}={$в_6$, $в_7$, $в_9$, $в_{11}$, $в_{13}$} , B_{S9}={$в_5$, $в_6$, $в_{10}$, $в_{14}$}.

Определяем пересечение множеств $B_{10}=B_0 \cap B_{S10}$={$в_7$,$в_{11}$}, мощность данного множества равна 2. Соответственно, пересечение множеств $B_9=B_0 \cap B_{S9}=\varnothing$. Таким образом, в качестве следующей вершины запасного пути выбирается вершина $в_{10}$.

Для вершины $в_{10}$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S10}={$в_6$,$в_9$,$в_{13}$}. Вершины $в_6$, $в_9$ являются пройденными, поэтому следующей вершиной на запасном пути будет вершина $в_{13}$.

Для вершины $в_{13}$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S13}={$в_{10}$, $в_{15}$}. Вершина $в_{10}$ является входящей для вершины $в_{13}$, поэтому в качестве следующей вершины выбирается вершина $в_{15}$.

Для вершины $в_{15}$ множество смежных с ней вершин, не принадлежащих основному пути равно B_{S15}={$в_9$,$в_{14}$,$в_{18}$}. Вершина $в_{18}$ непосредственно связана с конечной вершиной $в_{21}$. На этом формирование второго запасного пути заканчивается. Общее число переходов равно 8, на 2 больше по сравнению с основным путем.

На рис. 3 представлены способы обхода поломанных или скомпрометированных вершин при использовании запасных путей.

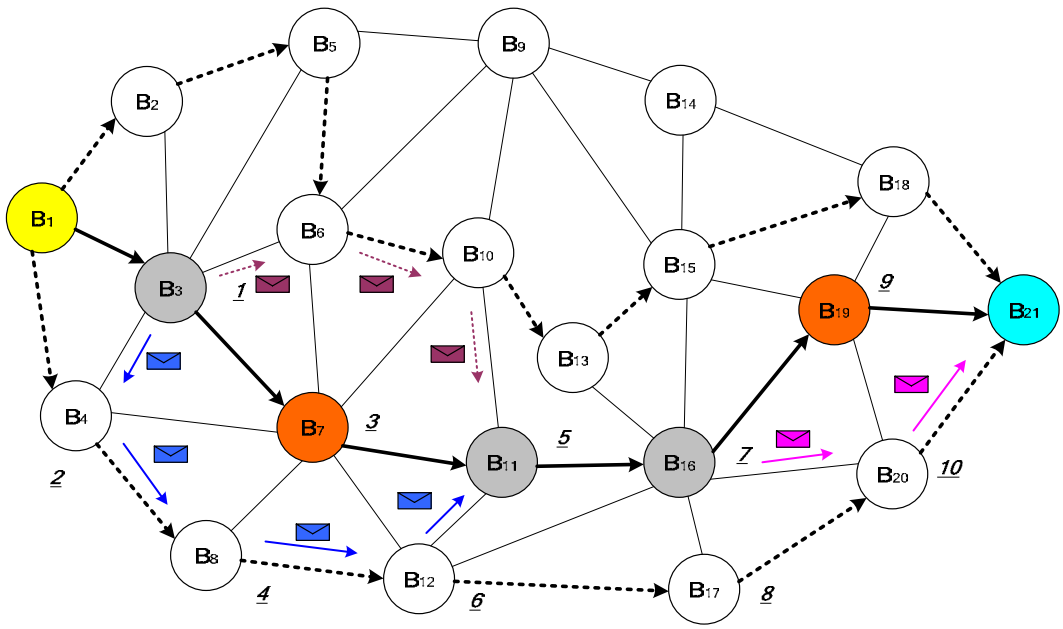

Рис. 3. Представление способов обхода скомпрометированных вершин при использовании запасных путей в распределенном трафике беспроводной сети

Существует три способа обхода одной скомпрометированной вершины через запасные пути:

- Обход по треугольнику;
- Обход по трапеции;
- Обход по прямоугольнику.

Первый случай обхода происходит, когда обходим одну скомпрометированную вершину через одну смежную с ней вершину. Например, узел $в_{19}$ – скомпрометированная вершина, обход осуществляется через смежную вершину $в_{20}$ по маршруту $в_{16}>в_{20}>в_{21}$.

Обход по трапеции осуществляется через две смежные вершины. Например, узел $в_7$ – скомпрометированная вершина, обход осуществляется через две смежных вершины $в_6$ и$в_{10}$ по маршруту $в_3>а_6>в_{10}>в_{11}$.

Обход по прямоугольнику осуществляется через три смежные вершины. Например, узел $в_7$ – скомпрометированная вершина, обход осуществляется через три смежных вершины $в_4$ $в_8$ и $в_{12}$ по маршруту $в_3>в_4>в_8>в_{12}>в_{11}$.

Коэффициент задержки перехода равен:

$$k_з = \frac{N_{пер.} - N_{осн.}}{N_{осн.}} = \frac{N_{пер.}}{N_{осн.}} - 1,$$

где: $N_{осн}$ – количество каналов основного участка пути, который обходится; $N_{пер}$ – количество каналов участка запасного пути, по которомуосуществляется обход вершины основного пути.

При обходе по треугольнику $N_{пер}$ =$N_{осн}$=2, в этом случае $k_з$=0.

При обходе по трапеции $N_{пер}$=3, $N_{осн}$=2, в этом случае $k_з$=0,5.

При обходе по прямоугольнику $N_{пер}$=4, $N_{осн}$=2, в этом случае $k_з$=1.

Обход двух смежных вершин может осуществляться по трапеции или по прямоугольнику. При обходе по трапеции двух смежных вершин $N_{осн}$=$N_{пер}$=3, в этом случае $k_з$=0. При обходе большего числа вершин при равной длине основного и запасного пути $k_з$=0.

При обходе по прямоугольнику двух смежных вершин $N_{пер}$=5, $N_{осн}$=3, в этом случае $k_з$=0,67. При обходе по прямоугольнику трех смежных вершин $N_{пер}$=6, $N_{осн}$=4, в этом случае $k_з$=0,5. При обходе по прямоугольнику четырех смежных вершин $N_{пер}$=7, $N_{осн}$ =5, в этом случае $k_з$=0,4. При обходе по прямоугольнику пяти смежных вершин $N_{пер}$ =8, $N_{осн}$=6, $k_з$=0,33. При обходе по прямоугольнику шести смежных вершин $N_{пер}$=5, $N_{осн}$=7, в этом случае $k_з$=0,28. Следует заметить, что при обходе по прямоугольнику $N_{пер}$-$N_{осн}$ =2 и не зависит от количества смежных вершин, которые обходятся. В этом случае:

$$k_з = \frac{N_{пер.} - N_{осн.}}{N_{осн.}} = \frac{2}{N_{осн.}}.$$

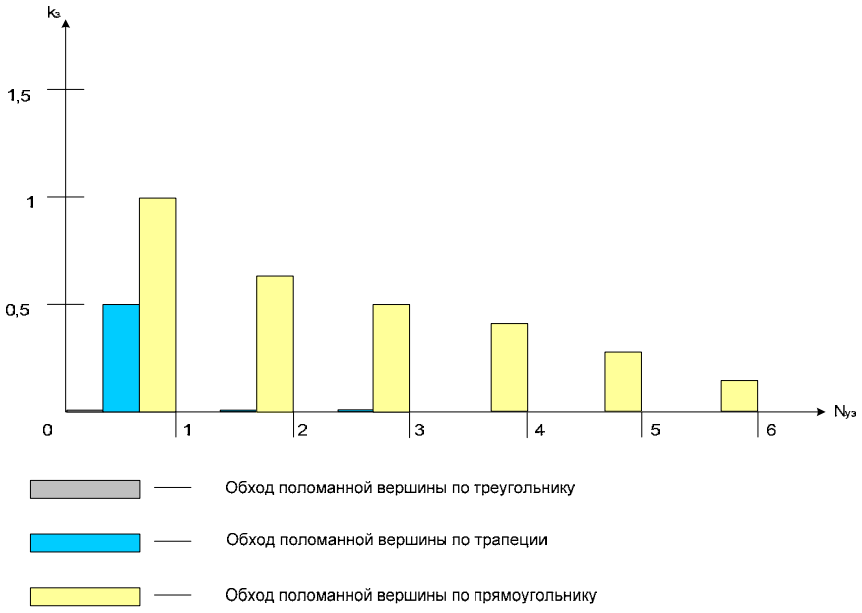

Рис. 4. Значение коэффициента задержки при различных способах перехода

На рис. 4 представлено значение коэффициента задержки при различных способах перехода. При переходе по треугольнику одной вершины $К_З$ равен 0. При переходе по трапеции одной вершины $К_З$ равен 0,5, а при переходе двух и трех вершин равен 0. При переходе по прямоугольнике одной вершины $К_З$ равен 1, а при переходе всех остальных стремится к 0.

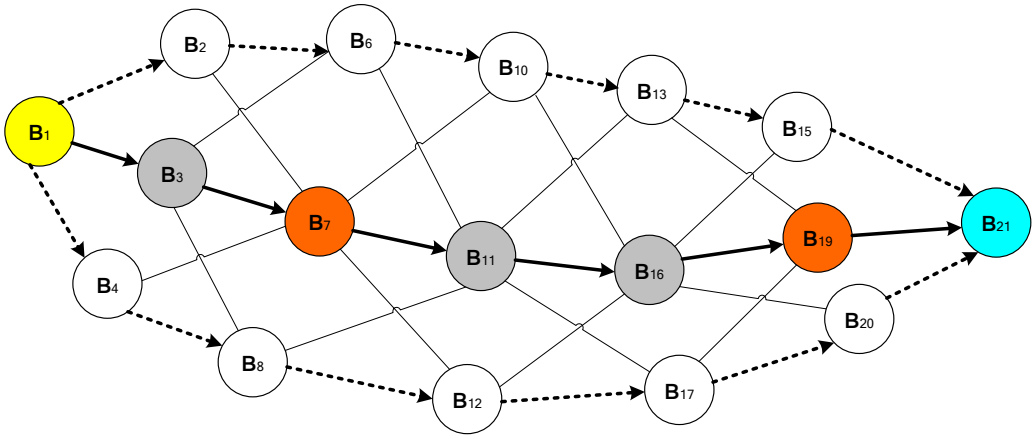

Рис. 5. Регулярная структура графа с обходом каждой из вершин основного пути трафика по

На рис. 5 представлена регулярная структура графа с обходом каждой из вершин основного пути по треугольнику. На основе анализа структуры графа (рис.5) можно сделать вывод, чем регулярнее граф сети, тем коэффициент задержки будет меньше.

Выводы

В данной статье предложен способ конструирования трафика с использованием запасных путей максимально связанных с основным путем, но не пересекающихся с ним. Использование таких путей позволяет минимизировать задержку передачи при реконфигурации маршрутов. Предложенный алгоритм формирования запасных путей, максимально связанных с основным путем, позволяет минимизировать время ремаршрутизации, обеспечивая тем самым заданные параметры качества обслуживания.

Список использованных источников

1. *As'ad Mahmoud As'ad Alnaser, Kulakov Y.O.* Reliable Multipath Secure Routing In Mobile Computer Networks // Computer Engineering and Intelligent Systems,ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online). – 2013. – Vol.4. – No.2. – Pp. 8-16.
2. *As'ad Mahmoud As'ad Alnaser, Kulakov Y.O.* Multipath Routing in Wireless Networks. // Contemporary Engineering Sciences. – 2012. – Vol. 5. – no. 6. – Pp. 251- 264.
3. *Kuo C.F., Pang A.-C., Chan S.-K.* Dynamic routing with security considerations // IEEE transactions on parallel and distributed systems. – Jan. 2009. – vol. 20. – no. 1. – Pp. 48-58.
4. *Lee P. P.C., Misra V., Rubenstein D.* Distributed algorithms for secure multipath routing in attack-resistant networks. // IEEE/ACM transactions on network. – Dec. 2007. – vol.15. – no.6. – Pp. 1490-1501.
5. *Lou W., Liu W., Zhang Y., Fang Y.* SPREAD: Improving network security by multipath routing in mobile ad hoc networks // Wireless Networks. Apr. 2009. – vol. 15. – no. 3. – Pp. 279-294.
6. *Yu M., Zhou M.C., Su W.* A secure routing protocol against byzantine attacks for MANETs in adversarial environments. // IEEE transactions on vehicular technology. – Jan. 2009. – vol. 58. – no. 1. – Pp. 449-460.

Поступила в редакцию 16 декабря 2013 г.

УДК 004.724.4 (045)

Ю.О. Кулаков, д-р.техн.наук, **А.В. Коган**

Національний технічний університет України "Київський політехнічний інститут ",

пр. Перемоги 37 , Київ- 56, 03056, Україна.

Спосіб мінімізації часу обходу скомпрометованих вузлів в мобільних мережах

У роботі запропоновано спосіб забезпечення заданих параметрів якості обслуговування QoS в разі вимушеної реконфігурації маршруту. Запропоновано спосіб формування запасних маршрутів, максимально близьких до основного шляху передачі інформації. Представлено алгоритм обходу вузлів, скомпрометованих або виключених з маршруту, з мінімально наскрізною затримкою передачі інформації. Бібл. 6, рис. 5.

Ключові слова: *багатошляхова маршрутизація, параметри якості обслуговування QoS, бездротові мережі, конструювання трафика, суміжні вершини, запасні шляхи.*

UDC 004.724.4 (045)

Y.A. Kulakov, Dr.Sc., **A.V. Kogan**

National Technical University of Ukraine "Kiev Polytechnic Institute",

Prospect Pobedy 37, Kiev -56, 03056, Ukraine.

Way to minimize the time bypass compromised nodes in mobile networks

The paper proposes a method for providing the specified parameters QoS- reconfiguration in case of a forced route. Method of forming alternate routes as close as possible to the main routes of transmission of information. An algorithm bypass nodes compromised or excluded from the route, with minimal end delay transmission of information. References 6, figures 5.

Keywords: *multi-path routing, Quality of Service QoS, wireless networks, traffic engineering, adjacent vertices, sidings.*

References

1. *As'ad Mahmoud As'ad Alnaser, Kulakov Y.O.* (2013), “Reliable Multipath Secure Routing In Mobile Computer Networks. Computer Engineering and Intelligent Systems,ISSN 2222-1719 (Paper)”. ISSN 2222-2863 (Online). Vol.4, No.2, pp. 8-16.
2. *As'ad Mahmoud As'ad Alnaser, Kulakov Y.O.* (2012), “Multipath Routing in Wireless Networks”. Contemporary Engineering Sciences. Vol. 5, No. 6, Pp. 251- 264.
3. *Kuo C. F., Pang A.-C., Chan S.-K.* (2009), “Dynamic routing with security considerations”. IEEE transactions on parallel and distributed systems. Vol.20, No. 1, Pp. 48-58.
4. *Lee P. P. C., Misra V., Rubenstein D.* (2007), “Distributed algorithms for secure multipath routing in attack-resistant networks”. IEEE/ACM transactions on network. Vol.15, No.6, Pp. 1490-1501.
5. *Lou W., Liu W., Zhang Y., Fang Y.* (2009), “SPREAD: Improving network security by multipath routing in mobile ad hoc networks”. Wireless Networks. Vol. 15, No. 3, Pp. 279-294.
6. *Yu M., Zhou M.C., Su W.* (2009), “A secure routing protocol against byzantine attacks for MANETs in adversarial environments”. IEEE transactions on vehicular technology. Vol. 58, No. 1, Pp. 449-460.