УДК 004.724.4(045)

КУЛАКОВ Ю.А.,
КОГАН А.В.,
ПИРОГОВ А. А.

РАЗРАБОТКА И МОДЕЛИРОВАНИЕ ПРОЦЕССА БЕЗОПАСНОЙ МНОГОПУТЕВОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В МОБИЛЬНЫХ СЕТЯХ

Предложен способ многопутевой безопасной маршрутизации. Организация процесса нахождения множества путей определена с помощью модифицированного алгоритма Дейкстры. Разбиение сообщения осуществляется на основе пороговой схемы Шамира. Разработана программа и приведен пример моделирования процесса безопасной многопутевой передачи информации.

A method for secure multipath routing. Organizing the process of finding the set of paths defined by a modified Dijkstra algorithm. Splitting messages is based on Shamir's threshold scheme. The program is an example of modeling and process secure multipath transmission.

1. Введение

В настоящее время область применения беспроводных сетей значительно расширилась, появляются новые требования к используемым технологиям. В частности, актуальным вопросом является безопасность в беспроводных сетях. Это связано с тем, что прослушивание передающей беспроводной среды не составляет особого труда. Кроме того, существующие методы повышения безопасности ориентированы в основном на сети фиксированной структуры. В то же время целый ряд беспроводных технологий позволяют обеспечивать высокую мобильность узлов, для которых известные методы защиты информации, используемые в сетях со статической структурой, требуют значительных накладных расходов, а возможно и не применимы вообще.

Известные методы многопутевой маршрутизации в мобильных компьютерных сетях направлены на повышения качества передачи информации и обеспечения равномерной загрузки компьютерной сети [1,2] и, как правило, не обеспечивают требуемого уровня защиты информации. В данной работе реализован способ безопасной передачи информации с использованием многопутевой маршрутизации в виде программы.

2. Обзор существующих решений

Многопутевая маршрутизация – хорошо изученная проблема в литературе о компьютерных сетях. Некоторые протоколы маршрутизации, такие как DSR [3] осуществляют равномерную балансировку нагрузки, где маршрутизаторы распространяют трафик между несколькими путями с равными метриками маршрута. Другим примером является BitTorrent [4], протокол обмена файлами использующий peer-to-peer соединение, который использует многопутевую маршрутизацию, чтобы быстро и эффективно распределять файлы.

Многопутевая маршрутизация также была предложена [5] для уменьшения эффективности атаки, в сетях с низкой латентностью анонимности. В отличие от совокупности сетей, что препятствуют этим атакам посредством дозирования сообщения и внедрения искусственных задержек, Фейгенбаум [6] вводит новую структуру для анонимного общения, называемая как многоуровневая меш-топология, которая защищает от таких атак, не задерживая пользовательский трафик.

3. Организация процесса многопутевой безопасной передачи информации

Многопутевая безопасная маршрутизація предполагает разбиение отправляемого сообщения на части и передачу их по множеству непересекающихся максимально безопасных путей. Алгоритм нахождения максимального количества непересекающихся путей [7] является модификацией алгоритма Дейкстры с помощью которого находиться множество кратчайших непересекающихся путей. В работе [8] предложен алгоритм нахождения оптимального количества непересекающихся путей с максимальным уровнем безопасности, которая оценивается с помощью коэффициента S_{Li} характеризующего вероятность того, что путь L_i безопасен.

$$S_{Lj} = \prod_{i=1}^{N} (1 - p_i),$$

где: p_i – вероятность того, что узел скомпрометирован.

Значение вероятности p_i определяет уровень защиты i-го узла. Начальное значение p_i задается при генерации сети, затем в процессе работы оно может меняться в зависимости от атак на сеть.

Разбиение сообщения на части осуществляется с помощью пороговой схемы Шамира [9], при этом используется интерполяционный многочлен Лагранжа [10].

Сформированные пакеты передаются по мобильной сети в соответствии с найденными путями. Выбор пути осуществляется на основании теории игр [11], с помощью которой каждый игрок $i \in \{1,..., n\}$ (часть сообщения) выбирает стратегию $x_i \in S$ (путь) из набора стратегий $x = \{x_1,..., x_n\}$, гирок i получает выигрыш $f_i(x)$ [12], то есть максимально лучший путь из всего набора путей, по которому будет происходить передача части сообщения.

При доставке первого пакета к получателю включается счетчик ожидания пакетов (время ожидания равно длине самого длинного пути минус длина пути текущего пакета плюс 1). Если не доставлены все пакеты в период ожидания, то посылается сервисный пакет с просьбой переслать неполученные сообщения по другим путям, и увеличивается время ожидания пакетов на величину равную длине пути сервисного пакета плюс длина максимально длинного пути плюс 1.

После того когда все части сообщения доставлены, оно восстанавливается с помощью интерполяционного многочлена Лагранжа.

С целью повышения надежности передачи сообщений по беспроводным каналам передачи данных предусмотрен режим контроля передачи информации между смежными узлами, который заключается в следующем. После передачи кадра данных, передающий узел прослушивает передающую среду на предмет активности принимающего узла. В том случае, если принимающий узел не передает кадр данных следующему узлу, передающий узел на основании теории игр выбирает новый путь к получателю.

Если пакет попадает в скомпрометированный узел, то есть попадает к злоумышленнику, то информация об этом лавинообразно распространяется по сети.

4. Моделирование процесса безопасной многопутевой передачи информации

В рамках данной работы была разработана программа моделирования процесса безопасной многопутевой передачи информации. На первом шаге моделирования (Такт: 0) с помощью модифицированного алгоритма Дейкстры осуществляется поиск множества непересекающихся путей, для каждого из которых вычисляется значение S_{Li}, характеризующее надежность доставки информации по каждому из выбранных путей. Пути и степень их надежности, а также опции вершин отображаются в сервисном окне (рис. 1), при данной топологии сети формируется 4 маршрута с различной надежностью.

На втором шаге осуществляется разбиение исходного сообщения, на пары символов (с дополнением символов «0» в начало сообщения в случае несоответствия длины сообщения с требованиями алгоритмов разбиения/сборки сообщения). Далее полученные пары символов преобразуются в соответствии с измененным пороговым алгоритмом в функцию, из которой получаем пары значений <коэффициент> |<значение функции>. Из этих пар значений формируются пересылаемые пакеты. Преобразования отображаются в «Окне отправителя».

В данном примере исходное сообщение 092C04 с помощью функции: $(09x^2 + 2Cx + 04) \bmod 257$ делится на 3 части:

Пакет №0 с содержимым: 1|57.

Пакет №1 с содержимым: 2|128.

Пакет №2 с содержимым: 3|217.

Для передачи трех пакетов среди 4 маршрутов для передачи частей сообщения выбираются 3 наиболее надежных маршрута:

L_1: B_0->B_{10}->B_{12}->B_{18}->B_7, S_{L1}= 0,863;

L_2: B_0->B_{13}->B_{17}->B_8->B_5->B_7, S_{L1}= 0,817;

L_3: B_0->B_{14}->B_{11}->B_2->B_{16}->B_7, S_{L1}= 0,817.

На первом шаге маршрутизации пакет №0 передается по самому надежному пути L_1 в направлении узла B_{10}. Пакет №1 передается по пути L_2 в направлении узла B_{13}. Пакет №2 передается по пути L_3 в направлении узла B_{14}.

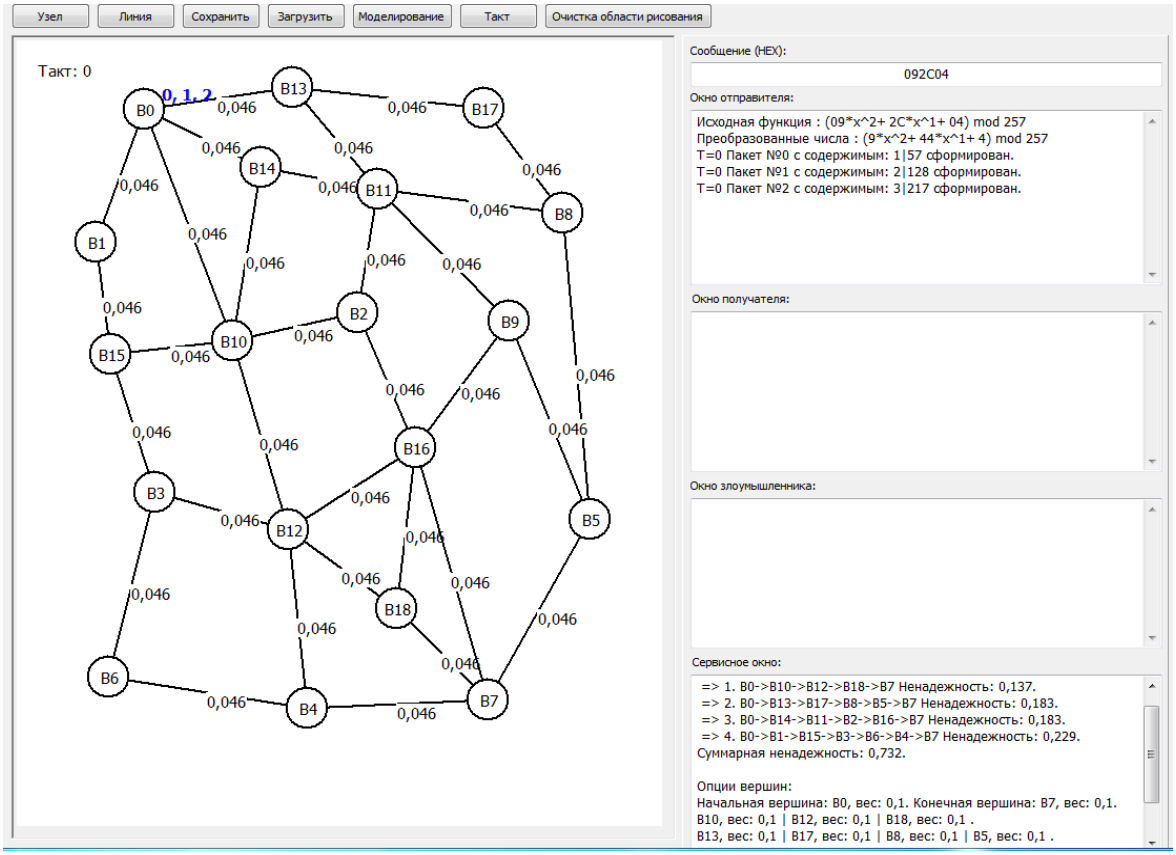

Рис. 1. Формирование множества непересекающихся путей

После 6 такта маршрутизации все пакеты сообщения достигают адресата и в окне получателя появляется следующая информация:

T=5 Ожидание всех пакетов до: 8.

T=5 Получен пакет №0 с содержимым: 1|57.

T=6 Получен пакет №1 с содержимым: 2|128.

T=6 Получен пакет №2 с содержимым: 3|217.

T=6. Все пакеты получены.

Получена формула: 217*(x-2)/(3-2)*(x-1)/(3-1)+128*(x-3)/(2-3)*(x-1)/(2-1)+57*(x-3)/(1-3)*(x-2)/(1-2)

Разложение формулы:

9*x^2+ 44*x^1+ 4

Преобразование коэффициентов:

09*x^2+ 2C*x^1+ 04

Сообщение: 092C04

Это свидетельствует о корректности передачи сообщения.

В том случае, когда злоумышленник перехватывает информацию по всем маршрутам передачи сообщений, например, в вершинах B_{10}, B_{11} и B_{17} (рис.2), он может собрать целиком все сообщение.

В моделирующей программе этот факт отражается в окне злоумышленника:

T=2 Получен пакет №0 с содержимым: 1|57

T=3 Получен пакет №1 с содержимым: 2|128

T=3 Получен пакет №2 с содержимым: 3|217

T=3 !!! Все пакеты получены !!!

При перемещении или отключении вершины, вершина в которой в данный момент находиться пакет осуществляет реконфигурацию исходного маршрута Например, при исключении вершины B_2 (рис.3) пакет №2 из вершины B_{11} перенаправляется в вершину B_9, при этом маршрут L_3 соответствующим образом реконфигурируется L_3: B_0->B_{14}->B_{11}->B_9->B_{16}->B_7. Соответствующая коррекция маршрута отражается в сервисном окне.

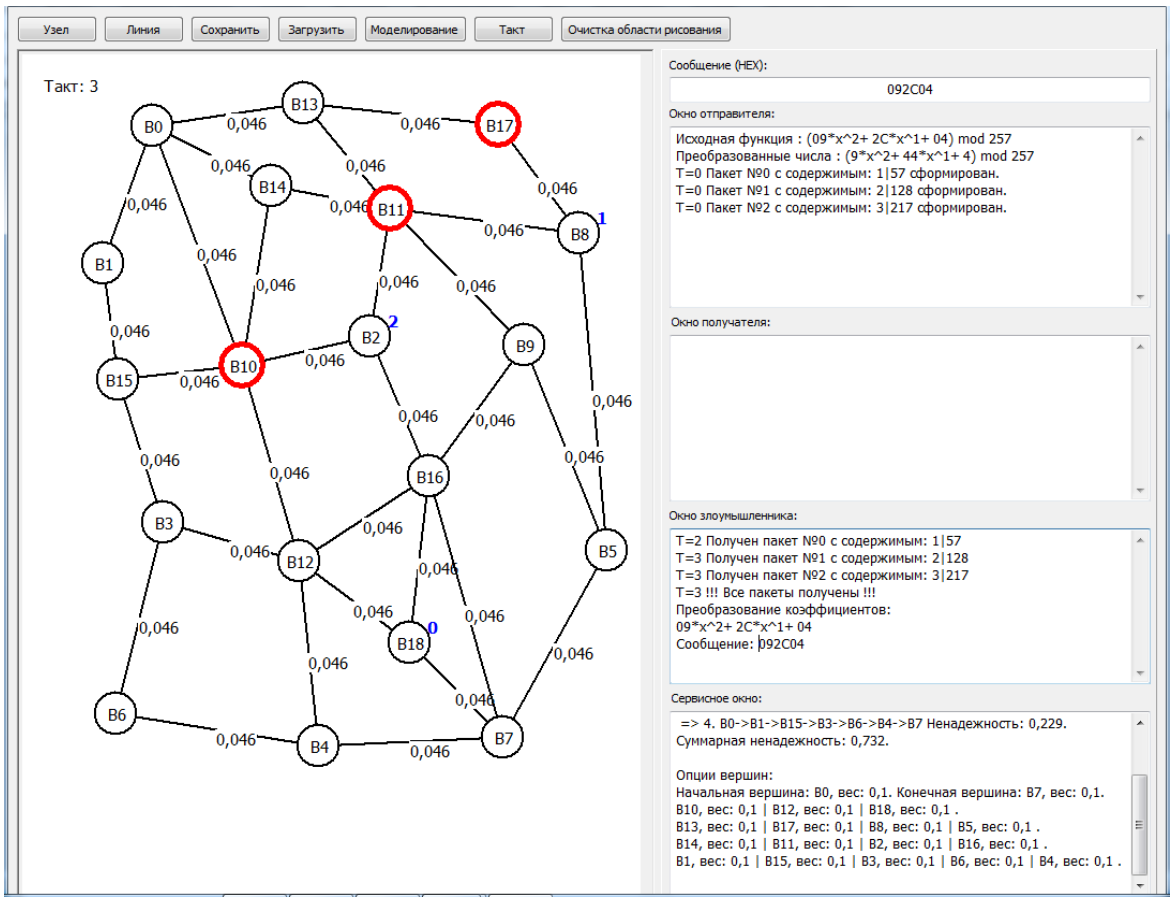

Рис.2. Злоумышленник перехватил все сообщение

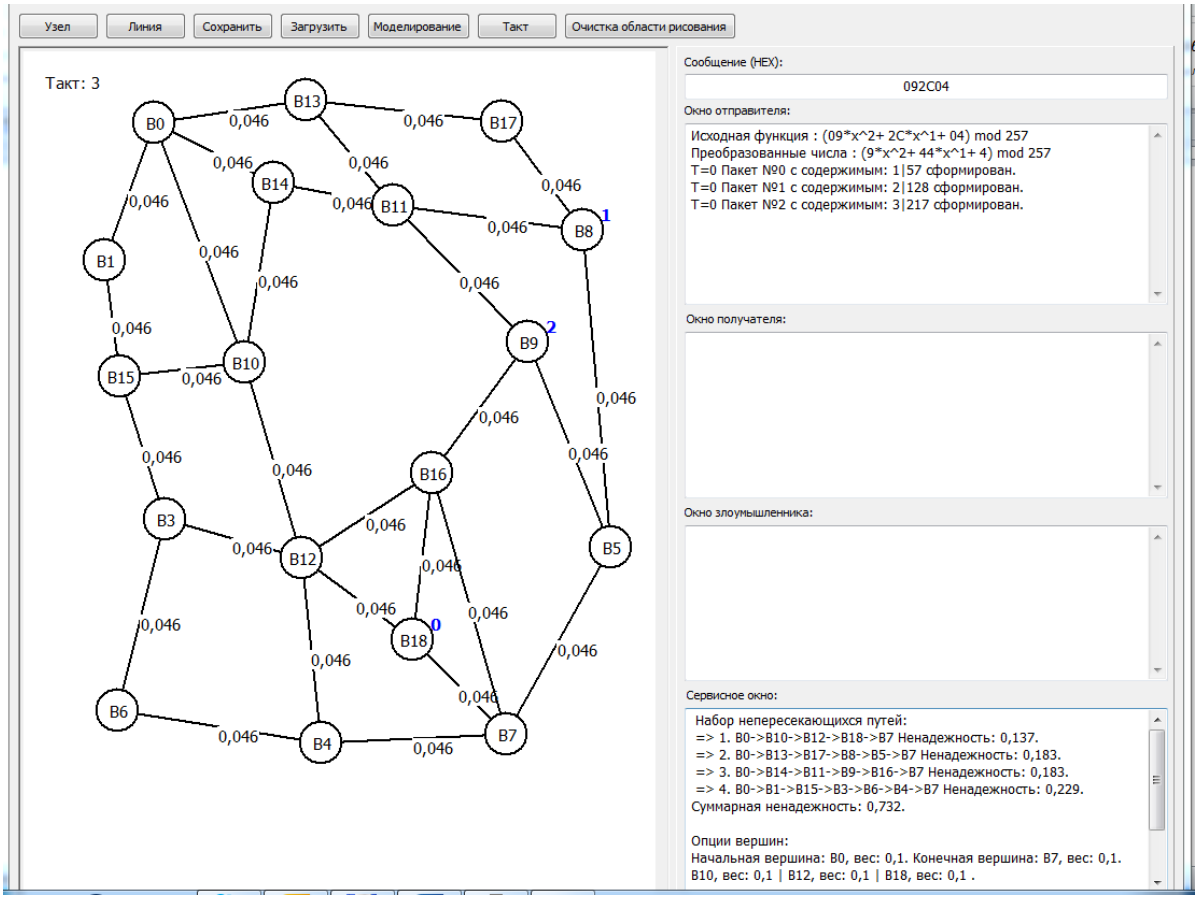

Рис. 3. Реконфигурация маршрута

Выводы

Предложенный в работе способ многопутевой маршрутизации за счет анализа надежности маршрутов позволяет обеспечить максимально безопасную передачу информационных сообщений и равномерно загрузит все каналы связи. Использование элементов теории игр также способствует выбору оптимального пути из всего набора независимых путей.

Предложенный в работе режим контроля передачи информации между смежными узлами по сравнению с известными методами квитирования передачи информации позволяет оперативно реагировать на изменения в топологии мобильной сети и своевременно осуществлять коррекцию маршрутов. Использование способа динамической распределенной маршрутизации позволяет сократить задержку передачи отдельных частей сообщения.

Чем ближе злоумышленник находиться к источнику или получателю информации, тем больше вероятность перехвата и восстановления всего сообщения. Вероятность перехвата равна единице при прослушивании всех каналов передачи информации источника или получателя информации. В этом случае необходимо принимать дополнительные меры по защите информации, например, использовать элементы BitTorrent маршрутизации.

Список литературы

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. A. Tsirigos, Z. J. Haas. Analysis of multipath routing, Part 2: mitigation of the effects of frequently changing network topologies. IEEE Trans. on Wireless Communications, 2004, 3(2): 500–511.
3. D. B. Johnson, D. A. Maltz, Y.C. Hu. The dynamic source routing protocol for mobile Ad Hoc networks (DSR). draft- ietf-manet-dsr-09.txt, 2003.
4. BitTorrent protocol specification. BitTorrentSpecification, June 2011. Accessed August 2011.
5. Vitaly Shmatikov and Ming-Hsui Wang. Timing analysis in low-latency mix networks: Attacks and defenses. In Proceedings of ESORICS 2006, pages 18–33, September 2006.
6. Joan Feigenbaum, Aaron Johnson, and Paul Syverson. Preventing active timing attacks in low-latency anonymous communication. In Proceedings of the 10th Privacy Enhancing Technologies Symposium, pages 166–183, 2010.
7. Кулаков Ю.А., Максименко Е.В., Рущак О.А. Повышение уровня безопасности передачи информации в мобильных сетях // Вісн. Національного техн. ун-ту України “КПИ”: Інформатика, управління та обчислювальна техніка. – К.: ТОВ “ВЕК+”, 2007. – Вип. 47. – С.297–304.
8. 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.
9. 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
10. Кулаков Ю.А., Деревянчук А.О., Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей // Проблеми інформатизації та управління: Зб.наук.пр.– К.: НАУ, 2009.– Вип.3(27) С.99-
11. T. Hui et al., “A game theory based load-balancing routing with cooperation stimulation for wireless ad hoc networks,” in Proc. the 11th IEEE international conference on high performance computing and communications, 2009, pp. 266-272.
12. M. Naserian et al., “Game theoretic approach in routing protocol for wireless ad hoc networks,” Ad Hoc Networks, vol.7, no. 3, pp. 569-578, May. 2009.