УДК 621.391

УСОВЕРШЕНСТВОВАНИЕ МОДЕЛИ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ СООБЩЕНИЯ С ОПТИМАЛЬНОЙ БАЛАНСИРОВКОЙ ЧИСЛА ЕГО ФРАГМЕНТОВ ПО НЕПЕРЕСЕКАЮЩИМСЯ МАРШРУТАМ

Александр Лемешко, Александра Еременко

Представленная работа посвящена усовершенствованию и исследованию модели безопасной маршрутизации с оптимальной балансировкой числа фрагментов в мобильных самоорганизующихся сетях. В рамках работы была рассмотрена концепция пороговой схемы разделения сообщения при безопасной маршрутизации его фрагментов по непересекающимся маршрутам. На основе анализа недостатков существующего ме-ханизма SPREAD предложено усовершенствование модели распределения фрагментов, которая была сведена к задаче оптимальной балансировки числа фрагментов передаваемого сообщения по непересекающимся маршрутам. Предложено ряд критериев оптимальности, связанных с решением задачи балансировки. В ходе сравнительного анализа обоснован к использованию на практике критерий оптимальности, обеспечивающий с одной стороны минимизацию верхнего динамически управляемого порога числа фрагментов, передаваемых по отдельным непересекающимся путям в сети, а с другой – адаптацию к параметрам безопасности (вероятности компрометации) отдельных элементов сети: узлов, каналов и путей. Представлены численные примеры реализации моделей с различными критериями оптимальности получаемых решений, и проведен их сравнительный анализ. Результаты сравнения подтвердили эффективность предлагаемой модели, когда по худшему с точки зрения вероятности компрометации пути передается минимальное число фрагментов, а по лучшему пути – их максимальное количество.

***Ключевые слова**: безопасная маршрутизация, MANET, вероятность компрометации, балансировка числа фрагментов, маршрут.*

ВВЕДЕНИЕ. Как показал проведенный анализ, в настоящее время широкое применение в различных прикладных областях находят мобильные самоорганизующиеся сети (Mobile Ad Hoc Networks, MANET). В соответствии с принципами своего построения MANET является сложной организационно-технической системой, включающей в себя распределенные на определенной территории мобильные узлы, наделенные функциями по структурной и функциональной адаптации к изменению сигнально-помеховой обстановки, числа и содержания поддерживаемых сервисов, требований к качеству обслуживания и уровню безопасности передаваемых данных. Наряду с задачами обеспечения качества обслуживания при построении и функционировании MANET ключевой проблемой является обеспечение информационной безопасности передаваемых в сети данных [3].

По сравнению с проводными сетями обеспечение информационной безопасности в MANET сопряжено с обнаружением и предотвращением множества существующих уязвимостей и атак [6]. Прежде всего, беспроводные каналы более восприимчивы к атакам, как пассивного прослушивания, так и активного вмешательства в сигналы и осуществление помех. Во-вторых, большинство протоколов маршрутизации в MANET подразумевают доверительные взаимодействия между участвующими узлами для осуществления передачи пакетов. Зависимость от такого взаимодействия делает передачу данных более уязвимой относительно несанкционированного доступа, подмене данных и атакам типа «отказ от обслуживания». В-третьих, отсутствие фиксированной инфраструктуры и централизованного управления делает трудно применимыми многие традиционные решения обеспечения информационной безопасности.

МЕХАНИЗМ ПОРОГОВОГО РАЗДЕЛЕНИЯ СООБЩЕНИЯ И МНОГОПУТЕВОЙ МАРШРУТИЗАЦИИ ЕГО ФРАГМЕНТОВ. Одним из направлений обеспечения заданного уровня информационной безопасности в телекоммуникационных сетях является реализация механизма SPREAD [4, 5, 9, 10], основанного на многопутевой маршрутизации передаваемого сообщения, предварительно разделенного на фрагменты (части) в соответствии со схемой Шамира [4, 5, 9] (рис. 1). В результате применения механизма SPREAD удается снизить вероятность компрометации передаваемого сообщения, т.к. заметно усложняется задача злоумышленника: ему необходимо скомпрометировать не один маршрут, по которому передается неразделенное сообщение, а все пути, по которым передаются его фрагменты. При этом под компрометацией сообщения понимается событие, связанное с несанкционированным доступом к его содержимому, т.е. чтобы скомпрометировать сообщение, передаваемое на основе механизма SPREAD, необходимо скомпрометировать все пути, используемые для доставки фрагментов

данного сообщения. В этой связи, факт компрометации того или иного пути состоит в доступе злоумышленника ко всем фрагментам сообщения, передаваемого по этому пути.

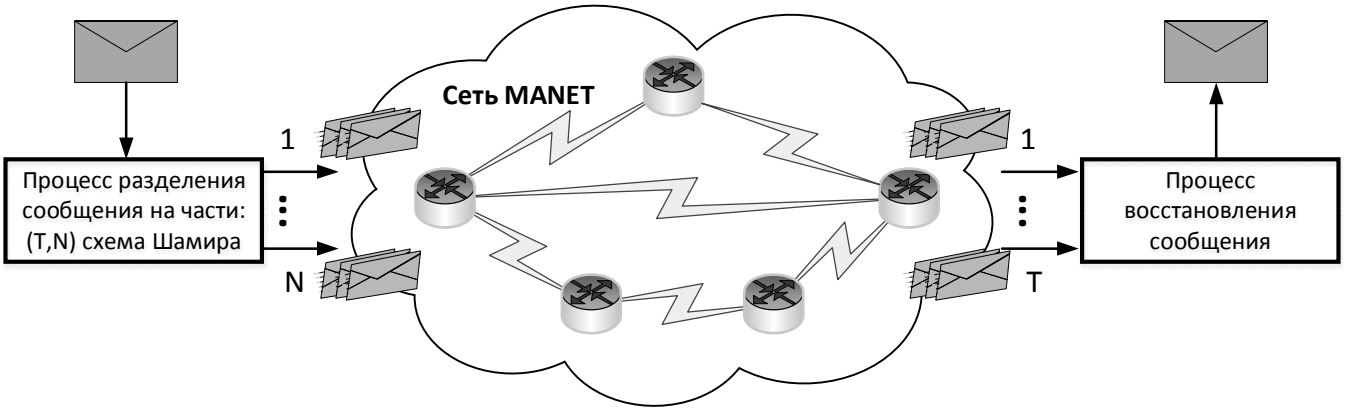

Рис. 1. Разделение сообщения в соответствии со схемой Шамира (T, N)

В общем случае при обеспечении безопасной маршрутизации сообщения в сети в соответствии с механизмом SPREAD необходимо решить следующие задачи [4, 5, 9]:

1. Расчет множества непересекающихся маршрутов между заданными узлами отправитель и получатель. Под непересекающимися понимаются такие маршруты, которые не содержат общих элементов (узлов и каналов) за исключением узлов отправителя и получателя.

2. Разделение передаваемого сообщения на множество фрагментов согласно выбранной схеме Шамира.

3. Распределение числа фрагментов передаваемого сообщения между множеством непересекающихся маршрутов, определенным в ходе решения первой задачи.

Стоит отдельно отметить, что вероятность компрометации пути во многом зависит как от числа составляющих его узлов и каналов связи, так и от параметров их безопасности, т.е. каждый элемент (узел, канал) пути может быть скомпрометирован с определенной вероятностью. В общем случае различные пути, используемые для передачи фрагментов разделенного в соответствии со схемой Шамира [4, 5, 9] сообщения, могут иметь разные значения вероятности компрометации. К сожалению, в рамках известных математических моделей [4, 5, 9], посвященных реализации механизма SPREAD, при распределении фрагментов сообщения по непересекающимся маршрутам в явном виде не учитываются параметры безопасности (в частности вероятность компрометации) этих путей. Таким образом, актуальной представляется задача, связанная с усовершенствованием математической модели безопасной маршрутизации передаваемого в сети сообщения на основе оптимального распределения по непересекающимся путям его фрагментов, получаемых в результате использования схемы разделения Шамира, и более полного учета параметров безопасности доступных маршрутов.

МОДЕЛЬ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ СООБЩЕНИЯ С ОПТИМАЛЬНОЙ БАЛАНСИРОВКОЙ ЧИСЛА ЕГО ФРАГМЕНТОВ. В рамках рассматриваемой модели предполагается, что известными являются следующие исходные данные:

S_{msg} и D_{msg} – узлы отправитель и получатель для передаваемого сообщения;

M – количество используемых непересекающихся путей при маршрутизации фрагментов сообщения;

(T, N) – параметры схемы Шамира, где N – общее число фрагментов, на которое разделяется передаваемое сообщение в результате применения схемы Шамира; T – минимальное количество фрагментов, по которым возможно восстановить передаваемое сообщение ($T \le N$);

p_i^j – вероятность компрометации j-го элемента (узла, канала) i-го пути;

M_i – число элементов в i-м пути, подверженных компрометации;

γ_P – допустимая вероятность компрометации сообщения в сети.

Кроме того, введем дополнительно следующие обозначения:

n_i – число фрагментов, передаваемых по i-му пути ($i = \overline{1, M}$);

P_{msg} – вероятность компрометации сообщения в целом при его передаче фрагментами по сети.

В ходе последующих рассуждений предполагается, что отправитель и получатель безопасны, т.е. вероятности компрометации узла-отправителя и узла-получателя равны нулю. Кроме того, в рамках предлагаемого решения, как и в работах [4, 5, 9], считается, что если элемент (узел, канал) пути скомпрометирован, то все фрагменты, передаваемые через этот элемент, также будут скомпрометированы. Тогда вероятность компрометации i-го пути, состоящего из M_i элементов, можно рассчитать с помощью выражения

$$p_i = 1-(1-p_i^1)(1-p_i^2)\ldots(1-p_i^{M_i}) = 1-\prod_{j=1}^{M_i}(1-p_i^j)\,. \quad (1)$$

Кроме того, в ходе расчета управляющих переменных n_i $(i=\overline{1,M})$, регламентирующих процесс распределения фрагментов передаваемого сообщения по непересекающимся путям, должно выполняться следующее условие [4, 5, 9]:

$$N = \sum_{i=1}^{M} n_i\,. \quad (2)$$

В случае использования схемы Шамира с параметрами $T < N$ необходимо выполнение условий $N - n_i < T$, при $i=\overline{1,M}$. А в случае, когда $T = N$, должны выполняться условия

$$1 \le n_i \le T-1, \quad (i=\overline{1,M}). \quad (3)$$

Выполнение условия (3) гарантирует то, что при компрометации всех маршрутов, кроме i-го, злоумышленнику не удастся восстановить сообщение в целом.

Одним из основных условий, которое в обязательном порядке должно выполняться в ходе безопасной маршрутизации, является то, что вероятность компрометации сообщения при его передаче по сети не должна превышать заданного допустимого значения, т.е.

$$P_{msg} \le \gamma_P\,. \quad (4)$$

Например, вероятность компрометации сообщения, разделенного на N фрагментов в соответствии со схемой Шамира (N,N) и передаваемого по M путям, определяется выражением [5]

$$P_{msg} = \prod_{i=1}^{M} p_i\,. \quad (5)$$

При этом выполнение условия (4) в соответствии с выражениями (1) и (5) должно обеспечиваться в ходе предварительного решения задачи по расчету множества непересекающихся маршрутов в сети. А для обеспечения оптимальной балансировки числа фрагментов передаваемого сообщения по множеству непересекающихся маршрутов в структуру усовершенствованной модели вводится ряд дополнительных условий:

$$n_i \le \beta \quad (i=\overline{1,M}), \quad (6)$$

где β – верхний динамически управляемый порог числа фрагментов, передаваемых по отдельным непересекающимся путям в сети.

Тогда в качестве критерия оптимальности решений по распределению числа фрагментов передаваемого сообщения по непересекающимся маршрутам целесообразно выбрать минимум следующей целевой функции

$$J = \beta + \sum_{i=1}^{M} p_i n_i\,. \quad (7)$$

Минимизация выражения (7) должна осуществляться при выполнении условий-ограничений (2) и (6), что позволит ограничить величиной β максимальное число фрагментов, передаваемых в каждом из выбранных путей. Введение в целевую функцию (7) слагаемого $\sum_{i=1}^{M} p_i n_i$ направлено на достижение следующей цели: в случае если общее число фрагментов N не кратно количеству выбранных путей M, то большее число фрагментов будет передаваться по лучшему с точки зрения вероятности компрометации маршруту. Это является важным положительным отличием предлагаемого решения от ранее известных [4, 5, 9].

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАЗЛИЧНЫХ МОДЕЛЕЙ РАСПРЕДЕЛЕНИЯ ЧИСЛА ФРАГМЕНТОВ ПЕРЕДАВАЕМОГО СООБЩЕНИЯ ПО НЕПЕРЕСЕКАЮЩИМСЯ МАРШРУТАМ. Проведем сравнительный анализ решения задачи распределения фрагментов сообщения по непересекающимся маршрутам с использованием четырех моделей с различными критериями оптимальности получаемых решений. В качестве первой выступала ранее предложенная в работах [4, 5, 9] модель (модель 1), использующаяся в механизме SPREAD и представленная выражениями (1)-(5). Вторая модель (модель 2), подлежавшая сравнению, отличалась от первой тем, что в качестве критерия оптимальности выступал минимум целевой функции, представленной следующим выражением:

$$J = \sum_{i=1}^{M} p_i n_i \,. \qquad (8)$$

Использование критерия (8) позволяет обеспечить такой порядок безопасной маршрутизации сообщения в сети, что максимальное количество его фрагментов будет передаваться по пути с минимальной вероятностью компрометации. И наоборот, по пути с максимальной вероятностью компрометации будет передаваться минимальное количество фрагментов того же сообщения.

Особенностью третьей модели (модель 3) является то, что в качестве критерия оптимальности, дополняя выражения (1)-(6), выступал минимум верхнего динамически управляемого порога числа фрагментов, передаваемых по отдельным непересекающимся путям в сети

$$J = \beta \,. \qquad (9)$$

Четвертая модель (модель 4), предложенная в предыдущем разделе, представлена выражениями (1)-(7).

Особенности предлагаемого решения будут продемонстрированы на следующем примере: пусть между заданной парой узлов отправитель и получатель доступны три пути с различным числом элементов: узлов и каналов (рис. 2). В рамках рассматриваемого примера условимся, что компрометации подвержены лишь каналы связи, что является достаточно справедливым для MANET. В ходе расчетов в качестве исходных будут выступать следующие данные:

–для разделения сообщения на фрагменты реализуется схема Шамира (10, 10);

–вероятности компрометации каналов связи в соответствии с их нумерацией и принадлежностью непересекающимся путям в MANET (рис. 2) принимают такие значения: $p_1^1 = 0,5$; $p_1^2 = 0,6$; $p_2^1 = 0,75$; $p_3^1 = 0,45$; $p_3^2 = 0,1$; $p_3^2 = 0,2$.

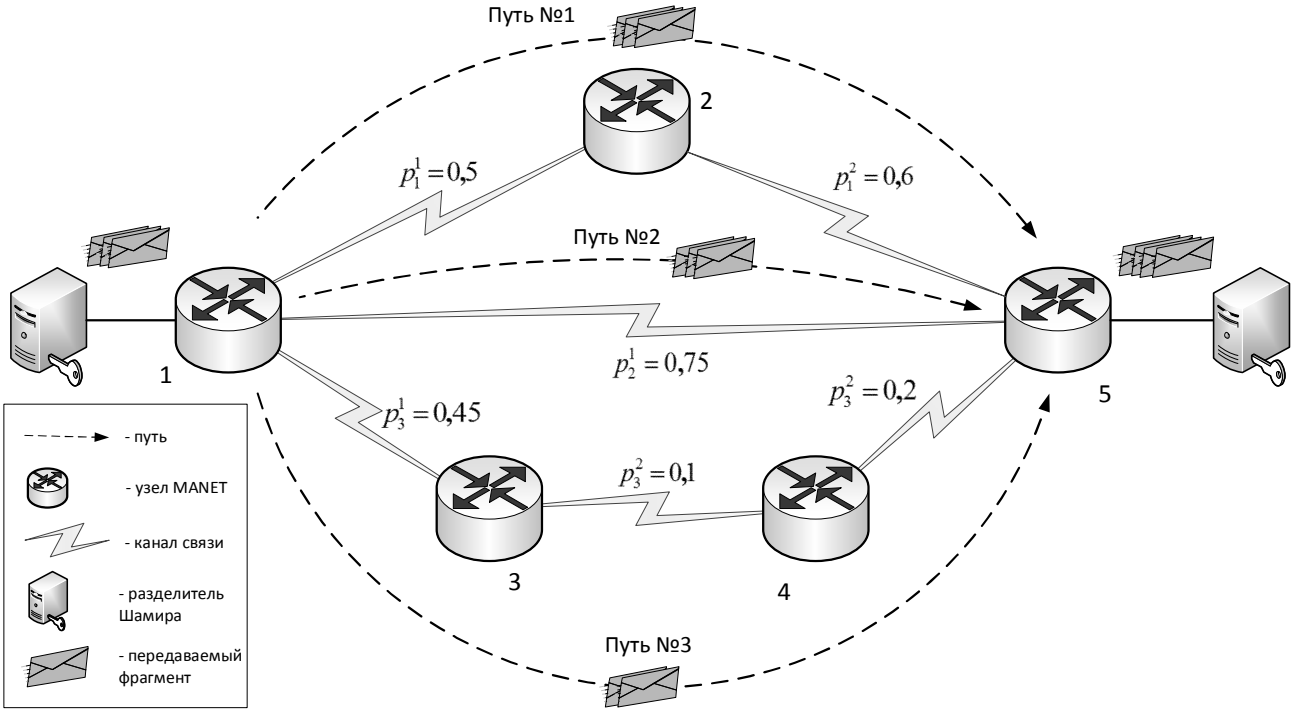

Рис. 2. Исходная структура MANET

Тогда результирующие вероятности компрометации путей, полученные в ходе использования выражения (1), представлены в табл. 1. Кроме того, в данной таблице показаны допустимые решения задачи распределения числа фрагментов по непересекающимся маршрутам, получаемые в ходе использования ранее описанных четырех моделей.

Как показано в табл. 1, при использовании модели 1 одним из допустимых решений задачи по распределению фрагментов сообщения по непересекающимся маршрутам является случай (рис. 1), когда по худшему с точки зрения компрометации пути ($p_1 = 0,8$) будет передаваться максимальное число фрагментов ($n_1 = 8$), что является недостатком данной модели.

Согласно модели 2 обеспечивался такой порядок распределения фрагментов по путям сети в ходе безопасной маршрутизации передаваемого сообщения (табл. 1), что по наилучшему с точки

зрения вероятности компрометации маршруту ($p_3 = 0,604$) передавалось максимальное число фрагментов ($n_3 = 8$), а по худшему ($p_1 = 0,8$) – их минимальное число ($n_1 = 1$).

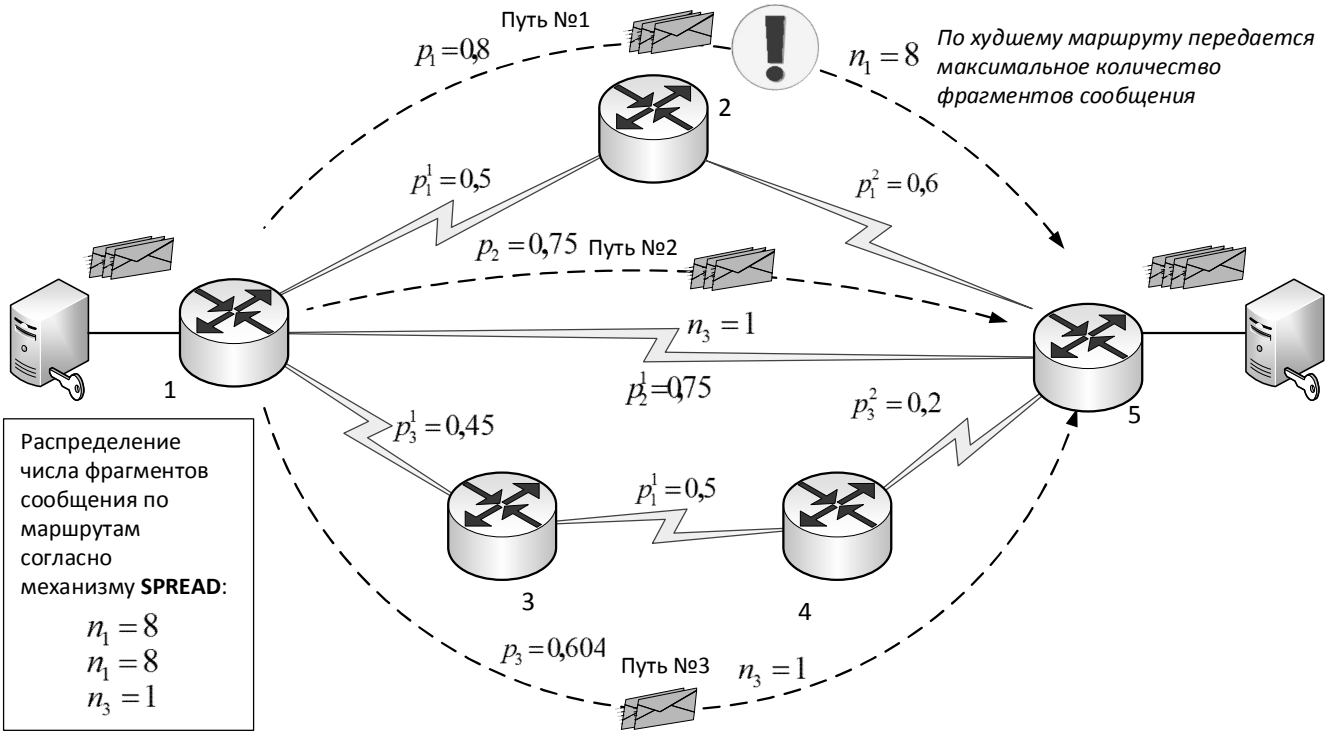

Рис. 3. Распределение числа фрагментов сообщения по маршрутам согласно механизму SPREAD (модель 1)

Таблица 1

Результаты расчетов по распределению фрагментов передаваемого сообщения с использованием моделей 1-4

№ пути	Вероятность компрометации пути	Количество фрагментов в пути в зависимости от метода балансировки			
		Модель 1	Модель 2	Модель 3	Модель 4
1	0,8	8	1	4	2
2	0,75	1	1	4	4
3	0,604	1	8	2	4

Подобный порядок распределения фрагментов является более предпочтительным по сравнению с решением, получаемым в рамках первой модели. Однако с точки зрения практики желательно, чтобы процесс распределения фрагментов по путям сети носил сбалансированный характер, чтобы задача злоумышленника максимально усложнялась.

В этой связи в рамках модели 3 осуществляется более сбалансированное распределение фрагментов по маршрутам (табл. 1), однако не учитывались параметры безопасности каналов и путей в целом. Поэтому наиболее предпочтительной является четвертая модель (1)-(7), основанная на использовании комбинированного критерия оптимальности (7). При использовании данной модели удается обеспечить (рис. 4), с одной стороны, минимизацию верхнего динамически управляемого порога числа фрагментов ($\beta = 4$), передаваемых по отдельным непересекающимся путям в сети, а с другой – адаптацию к параметрам безопасности (вероятности компрометации) отдельных элементов сети: каналов и путей. При этом по худшему с точки зрения вероятности компрометации пути передавалось минимальное число фрагментов ($n_1 = 2$), тогда как по лучшему маршруту – их максимальное число ($n_3 = 4$) (табл. 1).

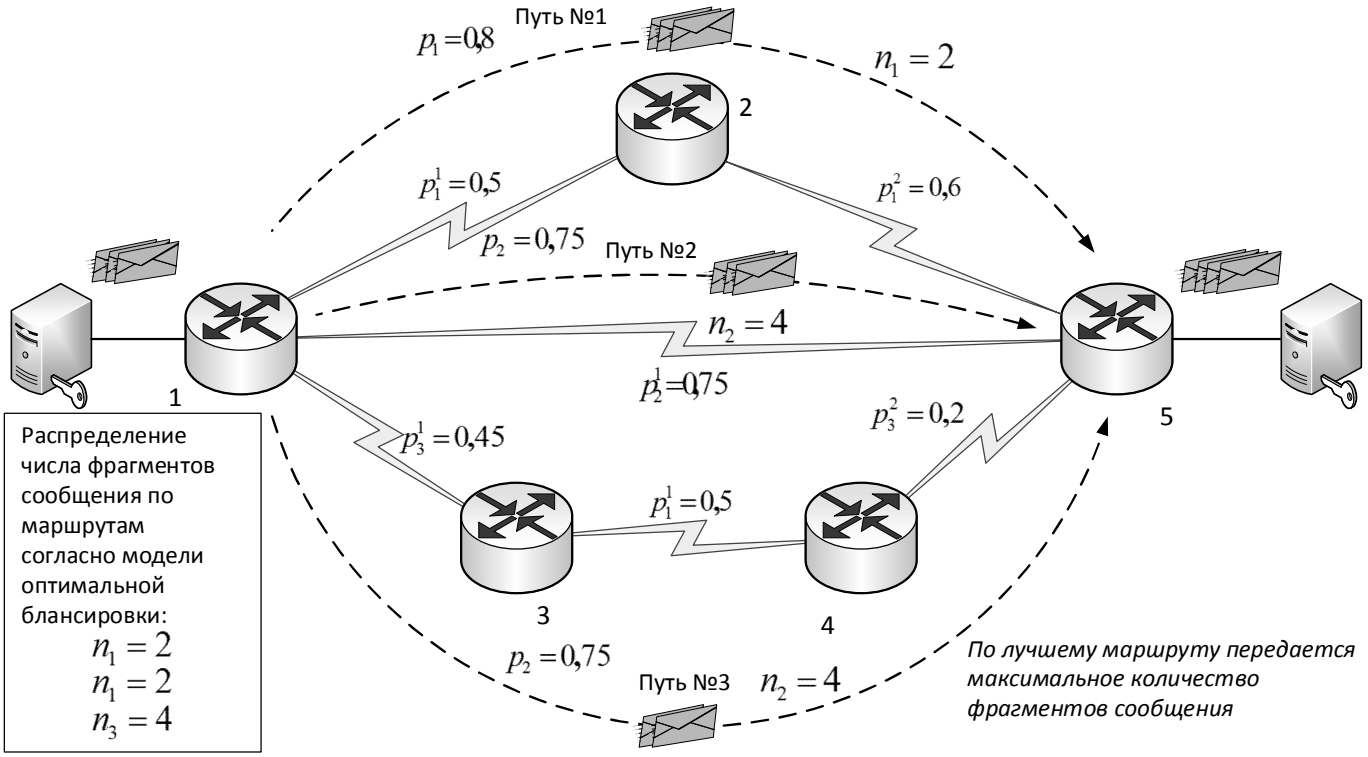

Рис. 4. Распределение числа фрагментов сообщения по маршрутам с учетом модели безопасной маршрутизации с оптимальной балансировкой числа фрагментов (модель 4)

ВЫВОДЫ. Актуальность решаемой задачи усовершенствования модели безопасной маршрутизации с оптимальной балансировкой числа фрагментов передаваемого сообщения по непересекающимся маршрутам связана с тем, что одной из ключевых задач при функционировании мобильных самоорганизующихся сетей является обеспечение безопасности передачи информации по каналам связи, которые в свою очередь являются наиболее уязвимыми в MANET. Недостатки существующих решений заключаются в том, что процесс распределения фрагментов сообщения по непересекающимся маршрутам не носит сбалансированный характер, а также не обеспечивается адаптация получаемых решений к параметрам безопасности элементов сети.

На основе анализа недостатков существующего механизма SPREAD предложено усовершенствование модели распределения фрагментов, которая была сведена к задаче оптимальной балансировки числа фрагментов передаваемого сообщения по непересекающимся маршрутам. Предложено ряд критериев оптимальности, связанных с решением задачи балансировки. В ходе сравнительного анализа обоснован к использованию на практике критерий оптимальности, обеспечивающий с одной стороны, минимизацию верхнего динамически управляемого порога числа фрагментов, передаваемых по отдельным непересекающимся путям в сети, а с другой – адаптацию к параметрам безопасности (вероятности компрометации) отдельных элементов сети: узлов, каналов и путей. Представлены численные примеры реализации моделей с различными критериями оптимальности получаемых решений, и проведен их сравнительный анализ. Результаты сравнения подтвердили эффективность предлагаемой модели, когда по худшему с точки зрения вероятности компрометации пути передается минимальное число фрагментов, а по лучшему пути – их максимальное количество.

ЛИТЕРАТУРА

[1]. Alouneh S. A Multiple LSPs Approach to Secure Data in MPLS Networks / S. Alouneh, A. En-Nouaary, A. Agarwal // Journal of Networks. – 2007. – Vol. 2, Issue 4. – PP. 51 – 58.

[2]. Alouneh S. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing / S. Alouneh, A. Agarwal, A. En-Nouaary // Computer Networks: The International Journal of Computer and Telecommunications Networking. – 2009. – Vol. 53, Issue 9. – PP. 1530 – 1545.

[3]. ITU-T X-805. Security architecture for systems providing end-to-end communications, 2003.

[4]. Lou W. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks / W. Lou, Y. Kwon // Vehicular

Technology, IEEE Transactions on. – 2006. – Vol. 55, Issue 4. – PP. 1320 – 1330.

[5]. Lou W. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Fang // INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE. – 2004. – Vol. 4. – PP. 2404 – 2413.

[6]. Manikandan K.P. A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad Hoc Networks / K.P. Manikandan, Dr.R. Satyaprasad, Dr.K. Rajasekhararao // (IJACSA) International Journal of Advanced Computer Science and Applications. – 2011. – Vol. 2, No. 3. – PP. 7 – 12.

[7]. Pant R. A Novel Holistic Grading for Network Security / R. Pant, C.N. Khairnar // International Journal of Application or Innovation in Engineering & Management (IJAIEM). – 2014. – Vol. 3, Issue 2. – PP. 41-45.

[8]. RFC 2501. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999.

[9]. Кулаков Ю.А. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности. / Ю.А. Кулаков, В.В. Лукашенко, А.В. Левчук // Науково-технічний журнал «Захист інформації». – 2011. – Том 13, №2 (51). – С. 5 – 10.

[10]. Чевардін В.Є. Модель загроз безпеки інформації в сучасних телекомунікаційних мережах з динамічною топологією / В.Є. Чевардін, В.А. Романюк, В.С. Шевченко // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2012. – №2. – С. 90 – 95.

REFERENCES

[1]. Alouneh S., En-Nouaary A., Agarwal A. (2007), "A Multiple LSPs Approach to Secure Data in MPLS Networks", Journal of Networks, Vol. 2, Issue 4, pp. 51-58.

[2]. Alouneh S., Agarwal A., En-Nouaary A. (2009), "A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing", Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 53, Issue 9, pp. 1530-1545.

[3]. ITU-T X-805. Security architecture for systems providing end-to-end communications (2003).

[4]. Lou W., Kwon Y. (2006), "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", Vehicular Technology, IEEE Transactions on, Vol. 55, Issue 4, pp. 1320-1330.

[5]. Lou W., Liu W., Fang Y. (2004), "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks", INFOCOM 2004, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE, Vol. 4, pp. 2404-2413.

[6]. Manikandan K.P., Satyaprasad Dr.R., Rajasekhararao Dr.K. (2011), "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad Hoc Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 3, pp. 7-12.

[7]. Pant R., Khairnar C.N. (2014), "A Novel Holistic Grading for Network Security", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, Issue 2, pp. 41-45.

[8]. RFC 2501. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations (1999).

[9]. Kulakov Yu.A., Lukashenko V.V., Levchuk A.V. (2011), Secure Multipath Routing in Wireless Networks of large Dimension, Ukrainian Information Security Research Journal, Vol. 13, №2 (51), pp. 5-10.

[10]. Chevardin V.E., Romanyuk V.A., Shevchenko V.S. (2012), Model of Information Security Threats in Modern Telecommunication Networks with Dynamic Topology, Zbirnyk naukovykh prats VITI NTUU "KPI", №2, pp. 90-95.

ВДОСКОНАЛЕННЯ МОДЕЛІ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ПОВІДОМЛЕННЯ З ОПТИМАЛЬНИМ БАЛАНСУВАННЯМ КІЛЬКОСТІ ЙОГО ФРАГМЕНТІВ ЗА МАРШРУТАМИ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ

Представлена робота присвячена вдосконаленню і дослідженню моделі безпечної маршрутизації з оптимальним балансуванням числа фрагментів в мобільних самоорганізованих мережах. В рамках роботи була розглянута концепція порогової схеми поділу повідомлення при безпечній маршрутизації його фрагментів по маршрутам, що не перетинаються. На основі аналізу недоліків існуючого механізму SPREAD запропоновано вдосконалення моделі розподілу фрагментів, яка була зведена до задачі оптимального балансування числа фрагментів переданого повідомлення по маршрутам, що не перетинаються. Запропоновано ряд критеріїв оптимальності, пов'язаних з вирішенням задачі балансування. У ході порівняльного аналізу обґрунтований до використання на практиці критерій оптимальності, що забезпечує з одного боку мінімізацію верхнього динамічно керованого порога числа фрагментів, переданих по окремим шляхам в мережі, що не перетинаються, а з іншого – адаптацію до параметрів безпеки (ймовірності компрометації) окремих елементів мережі: вузлів, каналів і шляхів. Представлені числові приклади реалізації моделей з різними критеріями оптимальності рішень, які отримуються, та проведено їх порівняльний аналіз. Результати порівняння підтвердили ефективність запропонованої моделі, коли за гіршим з точки зору ймовірності компрометації шляхом передається міні-

мальне число фрагментів, а за кращим шляхом – їх максимальна кількість.

Ключові слова: безпечна маршрутизація, MANET, ймовірність компрометації, балансування числа фрагментів, маршрут.

MODEL IMPROVEMENT OF MESSAGE SECURE ROUTING WITH OPTIMAL BALANCING ITS FRAGMENTS NUMBER TRANSMITTED OVER NON OVERLAPPING PATHS

The given work is devoted to improvement and investigation of secure routing model with optimal balancing of message fragments number in mobile self-organizing networks. Within the work it was explored the concept of threshold secret sharing scheme in relation to secure routing using non overlapping paths for the message frag-ments transmission. Based on analysis of disadvantages of existing mechanism SPREAD it was proposed the im-provement of fragments allocation model which had been reduced to the optimal balancing of message fragments number transmitted over the non overlapping paths. It was proposed several optimality criterions related to the so-lution of balancing problem. In a comparative analysis it is justified to use on practice optimality criterion, providing on the one hand minimizing dynamically managed upper bound number of fragments transmitted over separate non overlapping paths in the network, and from the other hand – to adapt to security parameters (probability of compromise) of individual network elements: nodes, links and paths. Numerical examples of models with different optimality criterion of the solutions obtained, and their comparative analysis represented. The comparison results confirmed the effectiveness of the proposed model, when by the worst path in terms of the probability of com-promise transmitted the minimum number of fragments, and by the best path – their maximum number.

Index terms: secure routing, MANET, probability of compromise, number of fragments balancing, path.

Лемешко Олександр Віталійович, доктор технічних наук, професор, професор кафедри телекомунікаційних систем Харківського національного університету радіоелектроніки.
E-mail: avlem@ukr.net.

Лемешко Александр Витальевич, доктор технических наук, профессор, профессор кафедры телекоммуникационных систем Харьковского национального универ-ситета радиоэлектроники.

Lemeshko Olexandr, Doctor of Science, Professor, Professor of Telecommunication Systems Department, Kharkiv National Uni-versity of Radio Electronics.

Єременко Олександра Сергіївна, кандидат технычних наук, старший науковий співробатний, доцент кафедри телекомунікаційних систем Харківського національного університету радіое-лектроніки.
E-mail: alexere@ukr.net.

Еременко Александра Сергеевна, кандидат технических наук, старший научный сотрудник, доцент кафедры телекоммуникационных систем Харьковского национального университета радиоэлектроники.

Yeremenko Oleksandra, PhD, Senior Researcher, Associate Professor of Telecommunication Systems Department, Kharkiv National University of Radio Electronics.

УДК 681.3.06:006.354

ПРИНЦИПИ ПОБУДОВИ І ОСНОВНІ ВЛАСТИВОСТІ НОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ БЛОКОВОГО ШИФРУВАННЯ УКРАЇНИ

Роман Олійников, Іван Горбенко, Олександр Казимиров, Віктор Руженцев, Юрій Горбенко

З 1-го липня 2015 р. в Україні вводиться в дію криптографічний стандарт блокового симетричного перетворення ДСТУ 7624:2014 [3], що визначає шифр "Калина" та режими його роботи для забезпечення конфіденційності і цілісності. Національний стандарт розроблений у співпраці Державної служби спеціального зв'язку та захисту інформації України і провідних українських науковців на основі проведення відкритого конкурсу криптографічних алгоритмів. Порівняно із відомим міжнародним стандартом AES, алгоритм ДСТУ 7624:2014 забезпечує вищий рівень криптографічної стійкості (із можливістю застосування блока та ключа шифрування включно до 512 бітів) і порівняну або вищу швидкодію на сучасних і перспективних програмних і програмно-апаратних платформах, суттєво