УДК 004.724.4(045)

Ю. А. Кулаков[1], В. В. Лукашенко[2], А. В. Коган[2]
[1]Национальный технический университет Украины
«Киевский политехнический институт»
Проспект Победы, 37, 03056 Киев, Украина
[2]Национальный авиационный университет
Проспект Космонавта Комарова, 1, 03680 Киев, Украина
e-mail: levchukAlla@yandex.ru; тел. (044) 406-74-64

Организация на основе теории игр многопутевой безопасной передачи информации

Предложен способ повышения безопасности маршрутизации в беспроводных сетях с помощью теории игр, которая используется для решения вопросов, связанных с пребыванием наиболее эффективного или наиболее экономичного способа выполнения любых сложных задач.

***Ключевые слова**: многопутевая маршрутизация, безопасная маршрутизация, теория игр, беспроводные сети.*

Введение

В настоящее время, в связи с расширением сферы использования мобильных компьютерных сетей, особую актуальность приобретают вопросы безопасной передачи информации.

В силу специфики мобильной компьютерной сети, связанной с ее динамически изменяющейся топологией сети, ряд методов защиты передаваемой информации, используемый в компьютерных сетях с фиксированной структурой системы передачи информации, оказывается неэффективным.

В свою очередь, однопутевые защищенные протоколы маршрутизации, описанные в работах [1–3], формируют один путь для маршрутизации данных от отправителя к получателю. Этот подход является уязвимым для атак, так как перехват информации или подслушивание могут быть достигнуты с минимальным количеством ресурсов.

При использовании многопутевой маршрутизации для безопасной передачи информации от источника к адресату снижается риск перехвата сообщения. При этом от выбора лучших путей и распределения потоков между ними в существенной мере зависит безопасность передачи информации, что является актуальной задачей на сегодняшний день.

Обзор и анализ существующих решений

Большинство подходов оптимизации маршрутизации были предложены для решения проблемы распределения трафика. Так, например: в [4] предлагается оптимальный алгоритм маршрутизации с маршрутизацией метрического сочетания обоих требований узла — надежность и производительность; в работе [5] предложен алгоритм динамической маршрутизации, направленный на случайный поиск путей для передачи данных, которым присуще сходство двух маршрутов, что, в свою очередь, позволит увеличить безопасность; в работе [6] представлены два алгоритма *Bound-Control* и *Lex-Control* для оптимизации распределения данных между двумя путями; в [7] предложен тайный обмен распространения данных по нескольким путям, и предлагается метод безопасной оптимизации данных.

В работе [8] предложен способ организации многопутевой безопасной маршрутизации в беспроводной сети MPLS, что позволит обеспечить построение магистральных сетей, имеющих практически неограниченные возможности масштабирования, повышенную скорость обработки трафика и беспрецедентную гибкость с точки зрения организации дополнительных сервисов.

Однако, все эти алгоритмы требуют дополнительных вычислительных затрат, снизить которые можно за счет использования теории игр. В частности, в работе [9] предлагается метод теории игр, чтобы получить наибольшую надежность пути с дальнейшей оптимизацией размещения сообщений на этих путях; в [10] предлагается протокол, который использует разницу пропускной способности линий между различными путями для определения оптимальной скорости передачи сообщения для каждого выбранного пути.

Постановка задачи

На основе анализа известных протоколов защищенной маршрутизации можно сделать вывод, что большинство из них не удовлетворяют требованиям *QoS*, а именно требованию равномерного распределения нагрузки по каналам связи и не обеспечивают достаточно безопасную передачу данных.

Одним из подходов к решению данной задачи является организация многопутевой маршрутизации с использованием теории игр, основной целью которой является обеспечение равномерной загрузки сети и безопасная передача данных.

Решение поставленной задачи

Особенность постановки данной задачи позволяет свести ее к задаче теории игр. Причем количество игроков соответствует количеству управляемых объектов.

Рассмотрим отдельный домен сети, состоящий из узлов и связей, соединяющих их, который представим в виде направленного графа $G = (N,\ L)$, где N — множество узлов (маршрутизаторов), а L — множество связей. Определим множество путей P между узлом-отправителем S и узлом-получателем D. Допустим, что: f_i — вероятность надежности между узлами S и D, которые перемещаются по путям $i \in P$; d — доставка пакетов; θ — коэффициент компромиссов между безопасностью и производительностью. Будем считать, что узел S знает открытый

ключ узла *D*. Узел-отправитель будет инициировать процедуру открытия маршрута, чтобы оперативно находить новые пути к узлу-получателю.

В работе [11] предложен способ Шамира. С помощью пороговой схемы секретное сообщение разделяют на *N* частей — $S_1, S_2, \ldots, S_N$, называемыми долями. При использовании теории игр каждый из *N* участников системы $P_1, P_2, \ldots, P_N$ содержит, соответственно, одну часть сообщения. Такой метод деления гарантиирует, что при использовании эффективных алгоритмов, любые *T* из *N* участников могут восстановить сообщение. В то время как от числа участников, меньшего *T*, невозможно получить никаких данных о системном сообщении *K*. Процесс разделения на части достаточно простой и основан на вычислении многочлена степени $(T-1)$:

$$f(x) = \left(a_0 + a_1 x + \ldots + a_{T-1} x^{T-1}\right) \bmod p .$$

В точке $x = i$ получаем *i*-ю часть: $S(i) = f(i)$, где *p* — большое простое число, большее чем любой из коэффициентов, известное и разделителю, и сборщику; коэффициент $a_0 \left(= K\right)$ — секретная информация; остальные коэффициенты $a_0,\ a_1, \ldots,\ a_{T-1}$ выбираются случайным образом.

В работе [12] предложено два способа передачи секретного сообщения предварительно разбитого на части. На рис. 1 представлен способ оптимального распределения

$$k_{опт} = \frac{N_ч}{N_{р\ опт}},$$

где $k_{опт}$ — оптимальное распределение, $N_ч$, — количество частей сообщения, $N_{р\ опт}$ — количество оптимальных маршрутов.

На рис. 1 представлен пример оптимального распределения сообщения на основе теории игр, где ✉ — количество игроков; → *u* — количество стратегий.

Допустим, что (*S*, *f*) — игра *n* лиц, где *n* — количество игроков, $n = N_ч$; *S* — набор стратегий, $S = N_{р\ опт}$; *f* — набор выигрышей, *f* = количеству маршрутов (стратегий).

Каждый игрок $i \in \{1,...n\}$ выбирает стратегию $x_i \in S$ из набора стратегий $x = \{x_1,...,x_n\}$, игрок *i* получает выигрыш $f_i(x)$. Профиль стратегий $x^* \in S$ является равновесием по Нэшу, если изменение своей стратегии не выгодно ни одному игроку, т.е. для любого *i* выполняется условие:

$$f_i(x^*) \geq f_i(x_i, x^*_{-i}) .$$

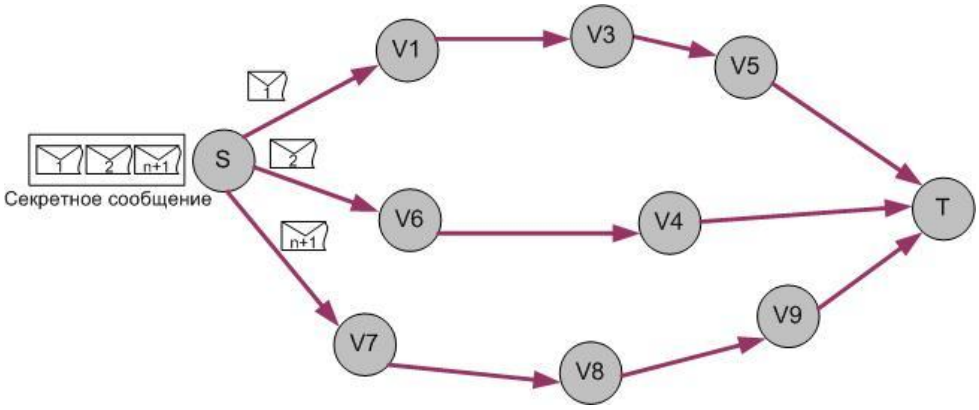

Рис. 1. Оптимальное распределение сообщение

Пусть $S = \{1,2,...,n\}$ — индексы всех компонент вектора x; $S_i \in S$ — совокупность индексов, определяющих информационную структуру для i-го игрока, имеющего стратегию $u_i = u_i(d_i)$, $d_i = (x_j)_{j \in s_i}$; $i \in I = \{1,2,...,n+1\}$ — множество игроков.

Условие разной информированности игроков:

$$\frac{\partial u_i(d_i)}{\partial x_j} = 0,\ j \notin S_i. \tag{1}$$

Соответственно, функция полезности i-го игрока запишется в виде интегрального выигрыша

$$J_i = \int_a^b ... \int_a^b F_i(x,u)\Phi(x)dx, \quad i \in I,$$

где $x \in X$ и имеет плотность распределения $\Phi(x)$. Следовательно, игровая постановка задачи примет вид:

$$J_i(u) = \int_a^b ... \int_a^b F_i(x,u)\Phi(x)dx \to \max_{u_i \in U_i},\ i \in I,$$

где $U_i = \left\{ u_i : \frac{\partial u_i(d_i)}{\partial x_j} = 0,\ (j \notin S_i),\ u_i \in C^2(X) \right\}$.

Рассмотрим случай квадратичной структуры $F_i(x,u),\ i \in I,\quad F_i(x,u) = \left\langle A^i(u,x),(u,x) \right\rangle,\quad i \in I$ — квадратичная форма с матрицей $A^i = (a^i_{ks})_{(2+n)(2+n)}$. Таким образом, получаем следующее уравнение:

$$J_i(u) = \int_a^b \ldots \int_a^b \left\langle A^i(u,x),(u,x) \right\rangle \Phi(x)dx \to \max_{ui},\ i \in I, \tag{2}$$

Равновесие по Нэшу в задаче (2) при условии (1) существует, если

$$a_{ii}^i < 0,\ \forall i\,. \tag{3}$$

На рис. 2 представлена зависимость безопасности сети от количества атак. На графике видно, что риск безопасности существенно увеличивается с увеличением числа атак. Результаты моделирования показывают, что предложенная схема повышает безопасность сети при активных атаках.

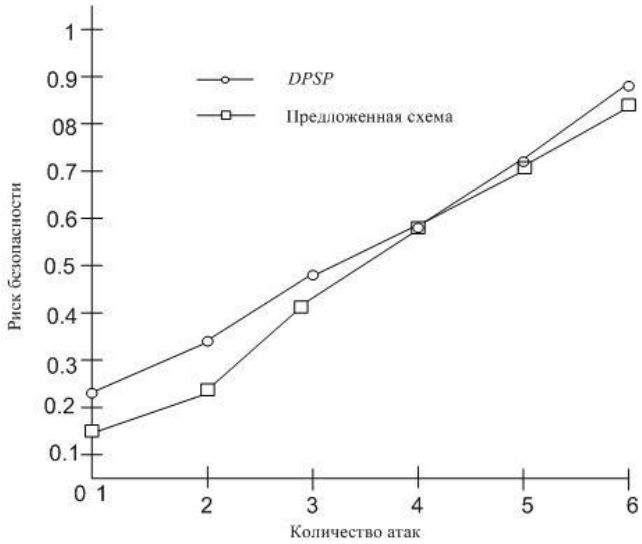

Рис. 2. Риск безопасности

Выводы

В представленной работе был предложен способ повышения безопасности маршрутизации в беспроводных сетях с помощью теории игр, которая использует для решения вопросов, связанных с нахождением наиболее эффективного или наиболее экономичного способа, выполнения каких-либо сложных заданий. Предложенный способ позволяет, по сравнению с известными способами безопасной маршрутизации, при уменьшении вычислительной сложности процесса формирования маршрутов на 15–20 % повысить безопасность передачи информации и обеспечить более равномерную загрузку системы передачи данных.

1. *Siguang Chen.* Anonymous Multipath Routing Protocol Based on Secret Sharing in Mobile Ad Hoc Networks / Siguang Chen, Meng Wu // J. of Systems Engineering and Electronics. — 2011. — Vol. 22, N 3. — P. 519–527.

2. *Zapata MG.* Secure Ad hoc On-Demand Distance Vector Routing / M.G. Zapata, N. Asokan // ACM Mobile Computing and Communications Review. — 2002. — Vol. 3, N 6. — P. 106–107.

3. *Papadimitratos P.* Secure Link State Routing for Mobile Ad Hoc Networks / P. Papadimitratos, Z.J. Haas // Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks. — IEEE Press. — 2003. — P. 27–31.

4. *Yu M.* A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments / M. Yu // IEEE Transactions on Vehicular Technology. — 2009. — Vol. 58, N 1. — P. 449–460.

5. *Kuo C.F.* Dynamic Routing with Security Considerations / C.F. Kuo // IEEE Transactions on Parallel and Distributed Systems. — 2009. — Vol. 20, N 1. — P. 48–58.

6. *Lee P.P.C.* Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks / P.P.C. Lee // IEEE ACM Transactions on Network. — 2007. — Vol. 15, N 6. — P. 1490–1501.

7. *Lou W.* SPREAD: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks / W. Lou // Wireless Networks. — 2009. — Vol. 15, N 3. — P. 279–294.

8. *Кулаков Ю.О.* Спосіб організації багатошляхової безпечної маршрутизації в безпроводовій мережі MPLS / Ю.О. Кулаков, В.В. Лукашенко, А.В. Левчук // Вісник Національного авіаційного університету. — 2012. — № 1. — С. 101–105.

9. *Naserian M.* Game Theoretic Approach in Routing Protocol for Wireless Ad Hoc Networks / M. Naserian // Ad Hoc Networks. — 2009. — Vol. 7, N 3. — P. 569–578.

10. *Hui T.* A Game Theory Based Load-Balancing Routing with Cooperation Stimulation for Wireless Ad Hoc Networks / T. Hui // The 11th IEEE Internation. Conf. on High Performance Computing and Communications. — 2009. — P. 266–272.

11. *Кулаков Ю.О.* Многопутевая маршрутизация в беспроводных сетях / Ю.О. Кулаков, А.В. Левчук // Електроніка та системи управління. — 2010. — № 4 (26). — С. 142–147.

12. *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). — С. 120–126.

Поступила в редакцию 07.02.2012