# Организация надежной передачи данных в беспроводных компьютерных сетях большой размерности

**Кулаков Ю. А.[1], Коган А. В.[2], Диброва М. А.[3]**
[1]Проф., д.т.н., профессор кафедры вычислительной техники, Национальный технический университет Украины "Киевский политехнический институт"
пр-т Победы, 37, г. Киев, Украина, ya.kulakov@gmail.com
[2]Асист. кафедры автоматизированных систем обработки информации и управления, Национальный технический университет Украины "Киевский политехнический институт"
пр-т Победы, 37, г. Киев, Украина, koganav@yandex.ru
[3]Аспирант кафедры вычислительной техники, Национальный технический университет Украины "Киевский политехнический институт"
пр-т Победы, 37, г. Киев, Украина, dibmichen@gmail.com

**Аннотация — в работе предложено решение задачи обеспечения надежной передачи данных в беспроводных компьютерных сетях. Для этого предложен способ многопутевой безопасной маршрутизации, который за счет выбора оптимального соотношения между безопасностью путей и предельным значением кодирования информации позволяет обеспечить гарантированную передачу данных в сети. Решение данной задачи достигается благодаря применению теории графов и теории множеств, которые используются при решении задачи многопутевой маршрутизации.**

***Ключевые слова: многопутевая маршрутизация, непересекающиеся пути, вероятность перехвата сообщения, безопасностная передача информации.***

# Organization of reliable data transmission in wireless computer networks of large dimension

**Kulakov Y. A.[1], Kogan A. V. [2], Dibrova M. A.[3]**

[1]Prof., Professor of Computer Engineering, National Technical University of Ukraine "Kyiv Polytechnic Institute"
Prospect Peremohy, 37, Kiev, Ukraine, ya.kulakov@gmail.com
[2]Asist. Department of automated information processing systems and management, National Technical University of Ukraine "Kyiv Polytechnic Institute"
Prospect Peremohy, 37, Kiev, Ukraine, koganav@yandex.ru
[3]Aspirant Department of Computer Engineering, National Technical University of Ukraine "Kyiv Polytechnic Institute"
Prospect Peremohy, 37, Kiev, Ukraine, dibmichen@gmail.com

**Abstract - in the suggested solution of the problem to ensure reliable data transmission in wireless computer networks. To this end, it provides a method for secure multi-path routing, which is due to the choice of the optimal balance between security and ways to limit the value of the information coding ensures reliable transfer of data on the network. This objective is achieved through the use of graph theory and the theory of sets, which are used in solving the problem of multipath routing.**

***Keywords: multipath routing, disjoint path, probability of intercept messages, safety information transfer.***

## Введение

Беспроводные сети приобретают все большего распространения в нашей жизни. Современный ритм жизни требует постоянного перемещения, поэтому коммуникации являются неотъемлемым атрибутом нашей жизни, и расширение сферы использования компьютерных сетей и повышение их мобильности предъявляет новые, более высокие, требования к качеству обслуживания трафика разного типа, обеспечению надежности и безопасности передачи информации. Методы защиты информации, используемые в сетях с фиксированной структурой, основанные на анализе топологии сети и анализе IP-адресов не используются в мобильных сетях в связи с постоянно меняющейся топологией таких сетей. В свою очередь, открытая среда передачи данных позволяет без усилий перехватить поток информации, передаваемый по беспроводному каналу передачи данных.

Использование многопутевой маршрутизации с передачей частей сообщения по множеству непересекающихся маршрутов затрудняет процесс перехвата всех частей сообщения. При этом эффективность многопутевой маршрутизации во многом зависит от выбора оптимальное соотношение между уровнем безопасности и надежности передачи информации.

## Организация многопутевой безопасной маршрутизации

При формировании множества путей для передачи сообщения, важное значение необходимо уделить их безопасности. В работе [1] предложен и обоснован модифицированный метод ветвей и границ, с помощью которого строится дерево решений и в результате формируется дерево путей. В работе [2] предложен и обоснован способ формирования множества максимально безопасных путей, которые за счет операций над множеством $B = \{вj \mid j = 1, 2, ..., k\}$ вершин позволяет уменьшить временную сложность алгоритма формирования множества максимально безопасных путей.

Для беспроводных сетей большой размерности целесообразно применять разбиение сети на домены маршрутизации, что обеспечивает минимальный объем служебного трафика. В основе данной процедуры лежит принцип самоорганизации, при котором каждый узел $в_m \in B$ компьютерной сети формирует множество $\Gamma_k(в_m)$ смежных с ним узлов с учетом плотности сетевого окружения k-го порядка:

$$\delta_k(v_m) = \frac{S(v_m) + \sum_{v_i, v_j \in \Gamma^k(v_m)} e_{i,j}}{S(v_m)},$$

где: $S(v_m)$ - максимальная степень связности вершины $v_m$;

$\Gamma(v_m)$ - соответствие первого порядка, множеств всех вершин, связанных с вершиной $v_m$, $\Gamma^2(v_m) = \Gamma(\Gamma(v_m))$;

$e_{i,j}$ - связь между смежными вершинами vi и vj с максимальной степенью;

$k$ - порядок сетевого окружения вершины.

При организации междоменной многопутевой маршрутизации, определение оптимального числа предельных маршрутизаторов сводится к задаче определения минимального разделяющего множества в подграфе $G_0 (B_0, E_0)$, образованном в результате пересечения подграфов $G_1 (B_1, E_1)$ и $G_2 (B_2, E_2)$, где $B_0 = B_1 \cap B_2$. При этом каждой вершине $B$ и $B_r$ подграфа $G_0 (B_0, E_0)$ соотносится граничный маршрутизатор.

Для обеспечения соответствующего уровня QoS необходимо повысить уровень безопасности передачи информации при многопутевой маршрутизации с помощью разделения сообщений на оптимальное количество частей с последующим кодированием частей передаваемого сообщения.

В общем случае вероятность перехвата информации по пути $L_i$, кроме начального и конечного узла, равна: $p_i = N_i / N_0$,

где: $N_i$ – количество узлов пути $L_i$, кроме начального и конечного узла;

$N_0$ – общее число узлов в беспроводной сети.

С учетом перехвата начального и конечного узлов вероятность перехвата пути $L_i$ равна: $ps = N_i / N_0 + 2 / N_0$ или $p_s = p_i + p_s$, где: $p_s = 2 / N_0$ - вероятность перехвата начального или конечного узлов.

При передаче сообщения по множеству независимых путей злоумышленник для восстановления сообщения должен прослушивать хотя бы один узел на каждом из использованных путей:

$$p_m = \frac{2 + \prod_{i=1}^{m} N_i}{N_0},$$

где: $m$ - общее количество использованных путей, не пересекаются.

При непосредственной близости двух путей, то есть при связи между узлами двух путей, существует вероятность одновременного прослушивания двух путей:

$$p_i = \frac{S_p}{S_i} \times \frac{N_b}{N_i},$$

где: $S_p$ - площадь сечения зон покрытия двух станций; $S_i$ - площадь зоны покрытия одной станцией $N_b$ - количество смежных станций; $Ni$ - количество станций пути $L_i$. На рис. 1 приведена вероятность прослушивания станций соседних путей в зависимости от расстояния $d$ между смежными узлами и радиуса $R$ передачи станцией беспроводной сети, где: $d$ - расстояние между узлами $R$ - радиус передачи станцией беспроводной сети. При отсутствии смежных станций $pi = 0$. При пересечении двух путей $Sp = Si$, в этом случае $p_i = 1 / N_i$.

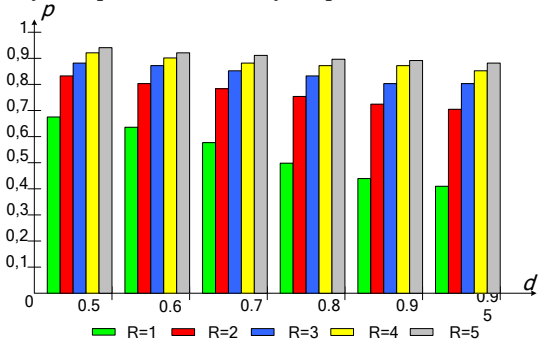


Рис. 1. Вероятность прослушивания станций соседних путей

Припустим, что $q_i$ - вероятность того, что узел перехвачен. Тогда вероятность того, что путь L1, l, скомпрометирован, равна:

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

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

В сети необходимо найти оптимальный набор путей, чтобы вероятность $P_{msg}$ была с минимальным значением. Вероятность перехвата сообщения:

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

где $p_i$ - вероятность, которая всегда меньше 1.

Чем больше частей $p_i$, тем меньше вероятность и лучше защита.

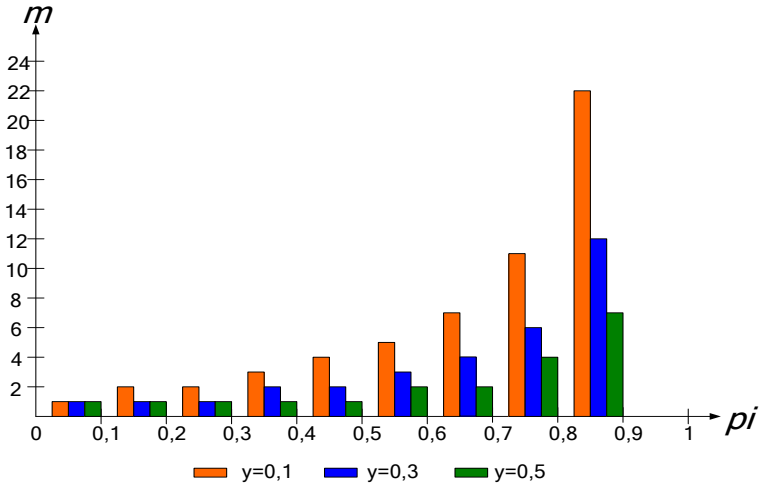


Рис. 2. Зависимость количества путей от вероятности их компрометации при разном уровне защиты

На рис. 2 представлен график зависимости количества путей от вероятности компрометации путей при разном уровне защиты.

При известной топологии сети злоумышленнику для перехвата всех частей сообщений между двумя станциями достаточно перехватывать сообщения в минимальном множестве $Br = \{bi \mid i = 1, 2, .., m\}$ вершин графа $G_0$, удаление которых разбивает граф $G_0$ на два несвязанных подграфа.

Для повышения уровня защиты в работе используется кодирование информации с помощью пороговой $(T, N)$ схемы разделения сообщения, где $N$ - количество частей, на которое разбивается сообщение, а $T$ - количество частей сообщения, достаточное для его восстановления. В данном случае уровень защиты $y = T / N$.

В работе [3] предложен и обоснован алгоритм разделения и сборки секретного сообщения на основе периодической функции $cos\ (x)$ и уравнение «волны»: $z = cos\ (x + N * \Delta x)$, где $N$ - целое число, в данном случае определяет порядковый номер символа, который шифруется (0-256) $\Delta x$ - прирост функции, задается в секретном ключе (любое число) $x$ - значение, взятое из открытого текста (0-256).

## Выводы

В работе предложен способ надежной передачи данных в беспроводных компьютерных сетях. Для этого предложен способ формирования множества неперетинаючих путей и доменов маршрутизации, который за счет учета плотности сетевого окружения $k$-го порядка узлов сети позволяет минимизировать объем служебного трафика в беспроводной компьютерной сети. На основе анализа основных факторов, влияющих на возможность перехвата информации, приведен расчет вероятности перехвата информации в беспроводных сетях в зависимости от расположения узлов, радиуса передачи сигналов, длины маршрута, а также места расположения злоумышленника.

## ЛІТЕРАТУРА REFERENCES


[1] Кулаков Ю. А. Способ организации многопутевой маршрутизации с помощью модифицированного метода ветвей и границ / Кулаков Ю. А., Коган А. В., Морозовский Т. О. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: збірник наукових праць. – К.: Століття +, 2015. – №62. – С.27-31.

[2] Диброва М. А. Способ формирования множества путей в сетевых центрах данных / Диброва М. А., Коган А. В., Воробьева А. Л. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: збірник наукових праць. – К.: Століття +, 2015. – №63. – С.60-64.

[3] Кулаков Ю. О. Алгоритм поділу і збірки секретного повідомлення для багатошляхової маршрутизації в бездротових мережах / Кулаков Ю. О., Коган А. В., Пирогов А. А. // Вісник НТУУ «КПІ». Інформатика, управління та Обчислювальна техніка: збірник наукових праць. – К.: Століття +, 2012. – №57. – С.46-50.