**УКРАЇНА**

**(19) UA (11) 105743 (13) U**

**(51)** МПК (2016.01)
**H04L 12/00**
**H04W 40/00**
**H04K 1/00**

**ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ**

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

**(21)** Номер заявки: **u 2015 06071**

**(22)** Дата подання заявки: **18.06.2015**

**(24)** Дата, з якої є чинними права на корисну модель: **11.04.2016**

**(46)** Публікація відомостей про видачу патенту: **11.04.2016, Бюл.№ 7**

**(72)** Винахідник(и):
**Лемешко Олександр Віталійович (UA),**
**Єременко Олександра Сергіївна (UA)**

**(73)** Власник(и):
**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**,
пр. Леніна, 14, м. Харків, 61166 (UA)

**(54) СПОСІБ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ СЕКРЕТНОГО ПОВІДОМЛЕННЯ З ОПТИМАЛЬНИМ БАЛАНСУВАННЯМ ЙОГО ФРАГМЕНТІВ ЗА ШЛЯХАМИ, ЯКІ НЕ ПЕРЕТИНАЮТЬСЯ**

**(57)** Реферат:

Спосіб безпечної маршрутизації секретного повідомлення з оптимальним балансуванням його фрагментів за шляхами, які не перетинаються, включає безпечну маршрутизацію секретного повідомлення від вузла-відправника до вузла-отримувача з фрагментацією за схемою Шаміра (T, N), причому зловмиснику необхідно скомпрометувати не один шлях, а множину шляхів, за якими передаються фрагменти цього секретного повідомлення в Ad Hoc мережі. Процес розподілу фрагментів за маршрутами носить збалансований характер за рахунок використання запропонованого критерію оптимальності, що пов'язаний з мінімізацією квадратичної цільової функції, де як вагові коефіцієнти виступають ймовірності компрометації шляхів мережі.

UA 105743 U

Корисна модель належить до галузі електрозв'язку, є технологією безпечної маршрутизації секретних повідомлень, і може знайти застосування на вузлах (маршрутизаторах і комутаторах третього рівня) транспортної телекомунікаційної мережі (ТКМ) при розв'язанні задач маршрутизації для покращення інформаційної безпеки.

Відомий спосіб багатошляхової безпечної маршрутизації в Ad-Hoc мережах (Lee C.K.-L. A Multipath Ad Hoc Routing Approach for Secure Data Delivery/C K.-L. Lee, X.-H. Lin, and Y.-K. Kwok//Proc. ICC. - 2003. - Vol. 1. - PP. 448-452) полягає у реалізації захищеної передачі фрагментів повідомлення за шляхами, які не перетинаються, з метою мінімізації або навіть виключення можливості несанкціонованого доступу до нього.

Основним недоліком даного способу є відсутність забезпечення балансування фрагментів повідомлення за маршрутами, які не перетинаються. Також у відомому способі не передбачене урахування параметрів безпеки елементів мережі при передачі секретного повідомлення.

Найбільш близьким до запропонованого технічного рішення є спосіб безпечної маршрутизації фрагментів секретного повідомлення, на які воно розділяється відповідно до схеми Шаміра (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). В цьому способі зниження ймовірності компрометації повідомлення, яке передається, здійснюється за рахунок того, що зловмиснику необхідно скомпрометувати не один шлях, а множину шляхів, за якими передаються фрагменти цього секретного повідомлення в Ad Hoc мережі.

В рамках цього способу передбачається, що відомими є такі вихідні дані: $S_{msg}$ і $D_{msg}$ - вузли відправник та отримувач повідомлення, яке передається; $M$ - кількість використаних шляхів, які не перетинаються, при маршрутизації фрагментів повідомлення; $(T, N)$ - параметри схеми Шаміра, де $N$ - загальне число фрагментів, на яке розділяється передане повідомлення в результаті застосування схеми Шаміра, $T$ - мінімальна кількість фрагментів, за якими можливе відновлення переданого повідомлення $(T \le N)$; $p_i^j$ - ймовірність компрометації j-го елемента (вузла, каналу) і-го шляху; $M_i$ - число елементів і-го шляху, які можуть бути скомпрометовані; $\gamma_P$ - допустима ймовірність компрометації повідомлення в мережі. Крім того, додатково введені такі позначення: $n_i$ - число фрагментів, переданих за і-м шляхом $(i = \overline{1, M})$; $P_{msg}$ - ймовірність компрометації повідомлення в цілому при його передачі фрагментами по мережі.

Однак даний спосіб не враховує збалансованого розподілення кількості фрагментів повідомлення за шляхами, які не перетинаються, та параметрів безпеки (ймовірності компрометації) елементів мережі (вузлів, каналів) окремих шляхів.

В основу корисної моделі поставлена задача забезпечення заданого рівня ймовірності компрометації секретного повідомлення та мінімізації можливості його компрометації за рахунок оптимального балансування кількості фрагментів повідомлення за шляхами, що не перетинаються, при цьому зловмиснику необхідно скомпрометувати усі шляхи, за якими передаються фрагменти, а також забезпечення адаптованості рішень щодо параметрів безпеки елементів мережі (вузлів, каналів) цих шляхів.

Поставлена задача вирішується тим, що в способі безпечної маршрутизації секретного повідомлення з оптимальним балансуванням його фрагментів за шляхами, які не перетинаються, який включає безпечну маршрутизацію секретного повідомлення від вузла-відправника до вузла-отримувача з фрагментацією за схемою Шаміра $(T,N)$, причому зловмиснику необхідно скомпрометувати не один шлях, а множину шляхів, за якими передаються фрагменти цього секретного повідомлення в Ad Hoc мережі, згідно з винаходом, процес розподілу фрагментів за маршрутами носить збалансований характер за рахунок використання запропонованого критерію оптимальності, що пов'язаний з мінімізацією квадратичної цільової функції, де як вагові коефіцієнти виступають ймовірності компрометації шляхів мережі, що дозволило забезпечити адаптацію кінцевих рішень щодо безпечної маршрутизації секретного повідомлення до параметрів безпеки вузлів, каналів та шляхів.

На Фіг. 1 як ТКМ зображена мобільна Ad Hoc мережа, структура якої містить пару вузлів відправник та отримувач секретного повідомлення, вісім вузлів-маршрутизаторів та десять каналів зв'язку. Між заданою парою вузлів відправник та отримувач доступні чотири шляхи, які не перетинаються, з різною кількістю елементів: вузлів і каналів. Зазначено ймовірності

компрометації каналів зв'язку відповідно до їх нумерації і належністю до шляхів. На Фіг. 2 зображена та ж структура мобільної Ad Hoc мережі та її параметри, але з додаванням розрахованих ймовірностей компрометації окремих шляхів та числом фрагментів, розподілених за цими шляхами.

Зміст заявленого способу пояснюється наступним.

Тут і далі передбачається, що відправник і одержувач безпечні, тобто ймовірності компрометації вузла-відправника і вузла-отримувача дорівнюють нулю. Крім того, в рамках способу вважається, що якщо елемент (вузол, канал) шляху скомпрометований, то всі фрагменти, які передаються через цей елемент, також будуть скомпрометовані. Тоді ймовірність компрометації і-то шляху, що складається з $M_i$ елементів, можна розрахувати за допомогою виразу:

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

Крім того, при розрахунку керуючих змінних $(n_i)$, що регламентують процес розподілу фрагментів переданого повідомлення за шляхами, які не перетинаються, повинна виконуватися така умова:

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

Варто зазначити, що однією з основних умов, яка в обов'язковому порядку повинна виконуватися в ході безпечної маршрутизації, є те, що ймовірність компрометації повідомлення при його передачі по мережі не повинна перевищувати заданого допустимого значення, тобто

$$P_{msg} \le \gamma_p. \quad (3)$$

Тоді ймовірність компрометації повідомлення, розділеного на $N$ фрагментів відповідно до схеми Шаміра $(N, N)$ і яке передається за $M$ шляхами, визначається виразом:

$$P_{msg}\prod_{i=1}^{M} p_i. \quad (4)$$

При цьому виконання умови (3) відповідно до виразів (1) і (4) повинне забезпечуватися в ході попереднього рішення задачі розрахунку множини мережних маршрутів, які не перетинаються.

Тоді як оптимальне балансування фрагментів секретного повідомлення за шляхами, які не перетинаються, забезпечується мінімізацією квадратичної цільової функції:

$$J = \sum_{i=1}^{M} p_i (n_i)^2. \quad (5)$$

В ході розв'язання задачі як ТКМ була використана мобільна Ad Hoc мережа, структура якої представлена на Фіг. 1. ТКМ містила пару вузлів відправник та отримувач секретного повідомлення, вісім вузлів-маршрутизаторів та десять каналів зв'язку. Між заданою парою вузлів відправник та отримувач доступні чотири шляхи з різною кількістю елементів: вузлів і каналів. В рамках даного прикладу вважається, що скомпрометованими можуть бути лише канали зв'язку, що є справедливим для Ad Hoc мереж (MANET). У ході розрахунків як вихідні виступають такі дані:

для розділення повідомлення на фрагменти реалізується схема Шаміра з надмірністю (9, 10);

ймовірності компрометації каналів зв'язку відповідно до їх нумерації і належністю до шляхів, які не перетинаються, приймають такі значення: $p_1^1 = 0{,}5$; $p_1^2 = 0{,}6$; $p_2^1 = 0{,}75$; $p_3^1 = 0{,}45$; $p_3^2 = 0{,}1$; $p_3^3 = 0{,}2$; $p_4^1 = 0{,}5$; $p_4^2 = 0{,}45$; $p_4^3 = 0{,}3$; $p_4^4 = 0{,}2$, що також зазначено на Фіг. 1.

Тоді в результаті розрахунків отримуємо наступні результати:

ймовірності компрометації шляхів у відповідності з виразом (1) приймають наступні значення: $p_1 = 0{,}8$; $p_2 = 0{,}75$; $p_3 = 0{,}604$; $p_4 = 0{,}846$;

порядок розподілу десяти фрагментів за чотирма шляхами, які не перетинаються:

$n_1 = 1;\ n_2 = 1;\ n_3 = 1$ і $n_4 = 7$ - при використанні прототипу;

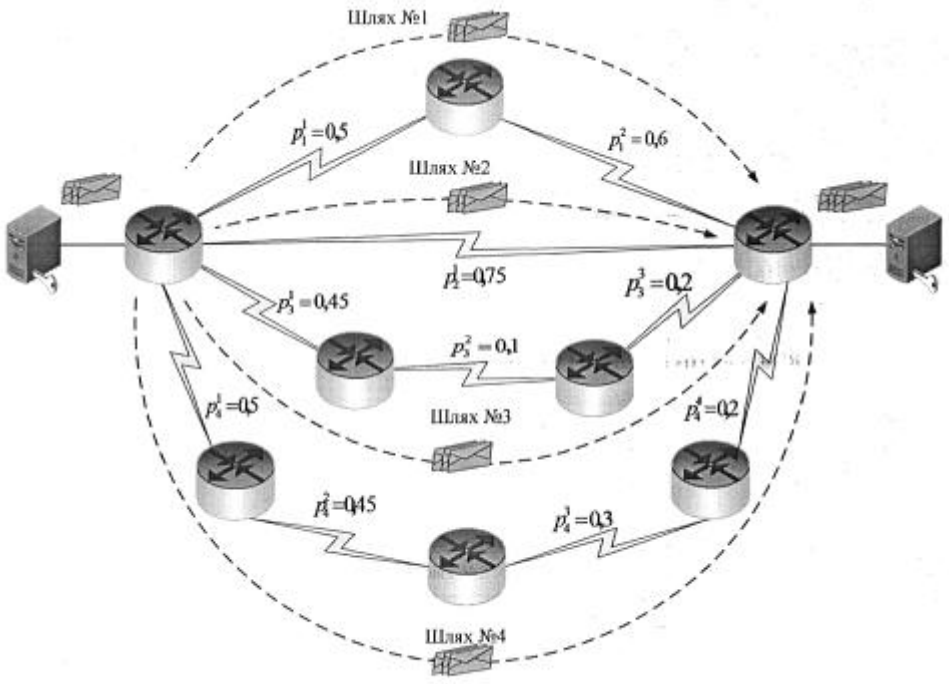
$n_1 = 2;\ n_2 = 3;\ n_3 = 3$ і $n_4 = 2$ - при використанні запропонованої корисної моделі (Фіг. 2).

В рамках запропонованої моделі здійснюється збалансований розподіл фрагментів секретного повідомлення за маршрутами (Фіг. 2). При використанні даної моделі вдається забезпечити, з одного боку, оптимальний розподіл числа фрагментів за окремими шляхами, які не перетинаються, в мережі, а з іншого - адаптацію до параметрів безпеки (ймовірності компрометації) окремих елементів мережі: каналів і шляхів. При цьому за гіршим з точки зору ймовірності компрометації шляхом передається мінімальне число фрагментів ( $n_4 = 2$ ), тоді як за кращим маршрутом - їх максимальне число ( $n_3 = 3$ ) (Фіг. 2).

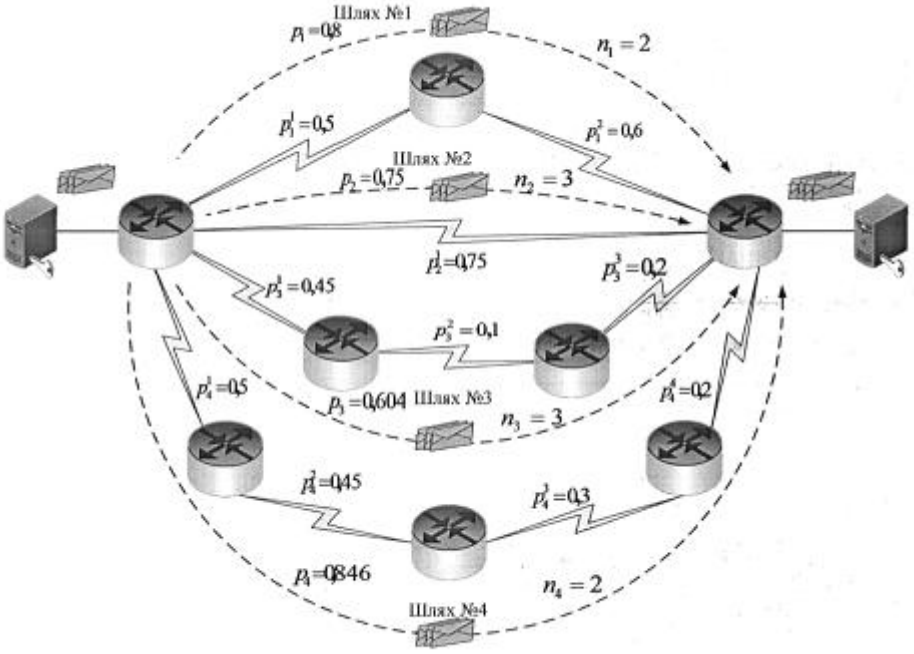
Таким чином, використання запропонованої корисної моделі дозволяє здійснювати безпечну маршрутизацію секретного повідомлення з оптимальним балансуванням його фрагментів за шляхами, які не перетинаються, із забезпеченням адаптації до параметрів безпеки елементів мережі: вузлів, каналів та шляхів.

## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб безпечної маршрутизації секретного повідомлення з оптимальним балансуванням його фрагментів за шляхами, які не перетинаються, який включає безпечну маршрутизацію секретного повідомлення від вузла-відправника до вузла-отримувача з фрагментацією за схемою Шаміра (T, N), причому зловмиснику необхідно скомпрометувати не один шлях, а множину шляхів, за якими передаються фрагменти цього секретного повідомлення в Ad Hoc мережі, який **відрізняється** тим, що в ньому процес розподілу фрагментів за маршрутами носить збалансований характер за рахунок використання запропонованого критерію оптимальності, що пов'язаний з мінімізацією квадратичної цільової функції, де як вагові коефіцієнти виступають ймовірності компрометації шляхів мережі, що дозволяє забезпечити адаптацію кінцевих рішень щодо безпечної маршрутизації секретного повідомлення до параметрів безпеки вузлів, каналів та шляхів.




**Фіг. 1**




Фіг. 2

Комп'ютерна верстка О. Рябко

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601