УДК 004.738.2 (045)

ОРГАНІЗАЦІЯ ПРОЦЕСІВ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В МОБІЛЬНИХ МЕРЕЖАХ AD HOC

Жуков І.А., Дворська Л.О.
Національний авіаційний університет
zhukov@iit.nau.edu.ua

У статті висвітлено: 1. Аналіз відомих методів розподілу множин з метою вибору найбільш ефективного способу формування максимально стійкої інфраструктури мобільної комп'ютерної мережі з урахуванням обмежень на діаметр комірок і припустимих значень сумарної інтенсивності потоків у кожній комірці. 2. Аналіз існуючих способів і алгоритмів маршрутизації з метою вибору найбільш ефективного алгоритму за критеріями часу ремаршрутизації та обсягу керуючої інформації. 3. Спосіб підвищення рівня безпеки за рахунок вибору оптимального набору шляхів. 4. Теоретичне доведення організації передавання даних у мобільних мережах.

The work contains: 1. Analysis of known shared methods of sets with the purpose to choose the most efficient method of constructing of maximally durable infrastructure of a mobile computer set according to districtions of a cells' diameter and available values of the sum intensity of channels in each cell. 2. Analysis of existing methods and algorithms of routing with the purpose to choose the most efficient algorithm by the criteria of re-routing time and the volume of control information. 3. The method of increasing of the security level by means of choosing the optimal set of paths. 4. The theoretical proof of the organization of data transmitting in mobile nets.

Вступ

Ad Hoc мережа — це група комп'ютерів, кожний із мереженим адаптером, підключених до самостійних мереж. Ad Hoc бездротові мережі використовуються як у малих і домашніх офісах, так і для робочих груп та підрозділів. Ці мобільні мережі характеризуються динамічною структурою зв'язків, наявністю бездротових каналів передавання інформації. Для них неефективні більшість способів і алгоритмів захисту інформації, що використовуються в провідних мережах. У зв'язку з цим актуальним є завдання пошуку нових рішень щодо організації безпечної передавання інформації в такій мережі. Одним із підходів до розв'язання даної проблеми є використання режиму багатошляхової маршрутизації, так, у працях [1; 2; 3] запропоновано низка схем захисту на рівні протоколів маршрутизації. Швидке збільшення кількості комп'ютерних мереж, розвиток оптоволоконних і бездротових засобів зв'язку супроводжуються безупинною зміною мережевих технологій, спрямованих на підвищення швидкодії й надійності мереж, можливості інтегрованого передавання даних, голосу та відеоінформації. Останнім часом поряд із традиційними комп'ютерними даними велику частку трафіка становлять мультимедійні дані.

Постановка завдання

Актуальність роботи з**умовлена** широким використанням сучасних комп'ютерних мереж у різних сферах діяльності людини. Одним із основних завдань управління функціонуванням комп'ютерної мережі є організація ефективної системи доставки інформації, що набуває особливої актуальності у мобільних мережах у зв'язку з постійним переміщенням АС. Крім того, в режимі віртуальних каналів потрібно забезпечити необхідну стійкість віртуального з'єд-нання. Стійкістю віртуального з'єднання називатимемо його здатність забезпечувати сеанс обміну без реконфігурації поточного з'єднання. Як відомо, більшість методів маршрутизації забезпечують формування віртуальних з'єднань за критерієм мінімальної довжини і при цьому фактично не враховується можливе переміщення абонентських систем (АС) та проміжних вузлів. У зв'язку з цим виникає необхідність розроблення способів і засобів, спрямованих на підвищення ефективності процедури передавання інформації в мережах, де структура зв'язків між АС динамічно перебудовується.

Усе це й визначає необхідність розроблення і дослідження нових підходів до побудови мобільних комп'ютерних мереж.

Таким чином, розробленя і дослідження способів і засобів підвищення продуктивності мобільних комп'ютерних мереж за рахунок ефективнішої організації доставки повідомлень, є актуальними і мають теоретичне і практичне значення.

Спосіб формування стійкого підграфа доставки повідомлень. Для мобільних комп'ютерних мереж як критерій оптимальності вибору маршруту необхідно розглядати час ремаршрутизації, що є складовою часу пересилання. Ремаршрутизація містить у собі процедуру керування місцем розташування, що складається з реєстрації місцеположення і оновлення маршрутної інформації. В загальному вигляді час ремаршрутизації $T_{\text{р}}$ дорівнює: $T_{\text{р}} = k_u \times T_u + k_s \times T_s$, де T_s — час реєстрації місця розташування; T_u — час оновлення маршрутної інформації про одне переміщення між суміжними комірками; коефіцієнти k_u і k_s вибираються з урахуванням відношення r середнього числа запитів на з'єднання до числа переміщення між областями реєстрації, при цьому $k_u = 1/r$ і $k_s = r$.

З урахуванням цього час ремаршрутизації $T_р$ дорівнює: $T_р = r Ч T_s + 1/r Ч T_u$.

У свою чергу, час відновлення маршруту залежить від кількості й часу повернень по віртуальному дереву в результаті переміщення мо-більних АС. Вузол дерева, в якому здійснюється зміна маршруту, називатимемо точкою розгалуження маршруту. Час відновлення маршруту T_c між двома суміжними листами дорівнює:

$$T_с = T_з + T_р,$$

де $T_з$ — затримка в передавання по ланці дерева, тобто між сусідніми вершинами; $T_р$ — час комутації в точці розгалуження.

За наявності деякого числа k проміжних ланок час маршрутизації дорівнює: $T_с = T_з Ч\ k + T_р$.

При розташуванні точки розгалуження на i-му рівні T_i дорівнює $T_i = T_з Ч\ i + T_р$.

При послідовному обході всіх листів кожна точка розгалуження обходиться (m – 1) раз, де m — число спадних гілок дерева. У цьому випадку сумарний час відновлення маршруту з обходом усіх листів визначається величиною:

$$T_m = \sum_{i=1}^{L} \sum_{i}^{n_i} T_i \cdot i + T_р \ . \qquad (1)$$

На підставі аналізу виразу (1) можна зробити висновок, що зі скороченням числа рівнів дерева скорочується час відновлення маршруту. Таким чином, завдання скорочення часу відновлення маршруту можна звести до завдання побудови дерева з мінімальним числом рівнів.

На основі аналізу відомих способів розподілу множин був запропонований алгоритм формування комірок мобільної мережі, що відрізняється від відомих кращою збіжністю. Як критерій розподілу мережі на комірки розглядається мінімальна вартість мережі, що досягається при мінімальному числі комірок і базових станцій (БС). Як обмеження виступають: максимально припустимий діаметр комірки; максимальне значення пропускної здатності БС. Додатковим параметром оптимізації є інтенсивність потоку між комірками.

У мобільних комп'ютерних мережах з реконфігурацією топології виникає потреба в досить частій зміні маршрутної інформації. Це визначає необхідність розробки швидких і ефективних алгоритмів маршрутизації. Аналіз відомих алгоритмів маршрутизації показав, що жодний з них не є оптимальним. У мобільних мережах з рекон-фігурацією топології необхідно застосовувати адаптивний алгоритм маршрутизації, що дає змогу в кожному конкретному випадку використовувати переваги табличних і лавиноподібних протоколів маршрутизації.

Розбиття повідомлення на оптимальну кількість частин. У цій статті пропонується передавати попередньо поділене повідомлення кількома шляхами. При цьому з погляду безпеки передавання даних виникає завдання визначення оптимальної кількості частин, на які слід розбивати повідомлення.

У працях [4; 5] для отримання частин вихідного повідомлення використовується так званий пороговий алгоритм розділення секрету (ПАРС). ПАРС ділить секретне повідомлення на N частин, що називаються долями (*share* або *shadow*). При цьому, маючи будь-яку кількість частин, менше T, не можна отримати ніяких даних про секретне повідомлення. Водночас, використовуючи відповідний алгоритм, можна відновити секретне повідомлення із будь-якого числа T (або більше) частин. Такий спосіб розділення секрету дістав назву порогового способу (T, N) (*threshold secret sharing*) [6]. Таким чином, використовуючи пороговий спосіб розділу (T, N), секретне повідомлення може бути розділене на N частин. Для того щоб перехопити повідомлення, противник повинен перехопити як мінімум T частин. При перехопленні кількості частин менше порогового значення, T, противник не може отримати ніяких даних про повідомлення і фактично шанси його дорівнюють нулю.

На другому етапі відбувається вибір набору шляхів, що відповідають значенням (T, N), і розподіл частин на кожен із обраних шляхів для досягнення максимальної безпеки. Основною метою є максимізація безпеки передавання шляхом розподілу частин повідомлення таким чином, щоб противнику довелося перехопити всі шляхи, аби відновити повідомлення.

Застосування ПАРС. Припустимо, що пороговий алгоритм розподілу (T, N) застосований до повідомлення, яке потрібно захистити, в вихідному вузлі. Нехай на сітьовому рівні є лише M шляхів, що не перетинаються, шлях 1, шлях 2, …, шлях M, доступних від джерела до адресата. Для позначення характеристик безпеки шляхів використовується вектор $p = [p_1, p_2, ..., p_M]$, де $pi(i = 1, 2, ..., M)$ — це імовірність, що шлях i скомпрометований. Не відходячи від узагальнення, далі приймається $p_1 \le p_2 \le ... \le p_M$, це означає, що шляхи упорядковуються від більш безпечного до менш безпечного. При цьому інформація про безпечність шляху p доступна у джерелі із протоколів маршрутизації. Припускається, що, якщо вузол перехоплений, усі частини повідомлення, що проходять через цей вузол, перехоплені. Відповідно $p_i > 0$, коли один чи більше будь-яких вузлів на шляху скомпрометовані. Для кожного шляху допускається, що, якщо він скомпрометований, то всі частини повідомлення, направлені цим шляхом, скомпрометовані. Оскільки використовуються шляхи, що не перетинаються,

то імовірність компрометації окремого шляху незалежна від імовірності компрометації інших шляхів. Імовірності p_i не враховують імовірність того, що джерело або адресат скомпрометований, тобто передбачається, що і джерело, і адресат надійні.

Позначимо розподіл частин як

$$n = [n_1, n_2, ..., n_M],$$

де n_i — кількість частин, розподілених по шляху i, n_i — ціле число, $n_i \geq 0$

$$\sum_{i=1}^{M} n_i = N.$$

Відповідно до алгоритму розподілу, ймовірність того, що повідомлення скомпрометоване, дорівнює імовірності того, що частини у кількості T або більше скомпрометовані. Позначимо ймовірність, що повідомлення скомпрометоване, як $P_{msg}(n)$. Тоді розподіл частин може бути сформульований у вигляді проблеми оптимізації:

$$\min P_{msg}(n),$$

якщо $\sum_{i=1}^{M} ni = N$, n_i — ціле число, $n_i \geq 0$.

Розглянемо питання досягнення максимальної безпеки передавання повідомлення без додавання в його частини надлишкової інформації.

Визначаємо

$$r = 1 - \frac{T}{N},$$

як коефіцієнт надлишкової схеми розподілу (T, N).

Без надлишковою є схема з $r = 0$, тобто $N = T$. За наявності M доступних шляхів і відповідних характеристик безпеки, $p = [p_1, p_2, ..., p_M]$, безнадлишкова (N, M) ($N \geq M$), схема розподілу повідомлення забезпечує максимальну безпеку, тобто мінімальну ймовірність перехоплення повідомлення, коли н менше одної і не більше T – 1 частин розподілені по кожному із доступних шляхів, тобто

$$\begin{cases} 1 \leq n_i \leq T - 1, \quad i = 1, ..., m; \\ \sum_{i=1}^{m} n_i = N. \end{cases}$$

Цей розподіл змушує противника перехопити всі шляхи, щоб перехопити повідомлення. Ймовірність перехоплення дорівнює імовірності, що всі шляхи скомпрометовані. Рівень безпеки значною мірою залежить від вибору оптимального набору шляхів. Кількість їх залежить від коефіцієнта надлишковості. Таким чином, використання ПАРС дає змогу досягнути більш високого ступеня захисту передавання інформації в мобільних мережах, порівняно зі звичайними методами, при цьому зводячи ризик втрати частини по-відомлення до мінімуму.

Висновки. Наукова новизна одержаних результатів визначається такими положеннями:

1. Запропонований і обґрунтований підхід до синтезу інфраструктури мобільної комп'ютерної мережі, яка враховує реконфігурацію топології, що передовсім стосується міграції АС під час передавання інформації.

2. Запропонований і обґрунтований спосіб формування стійкого підграфа доставки повідомлень, що забезпечує підвищення ефективності процедури маршрутизації в мобільних мережах з недостатньою стійкістю віртуальних з'єднань.

3. Обґрунтований і розроблений алгоритм маршрутизації, який, порівняно з відомими алгоритмами, дозволяє підвищити ефективність функціонування мобільних комп'ютерних мереж за рахунок скорочення обсягу керуючої інформації та часу ремаршрутизації.

Практичне значення одержаних результатів дисертаційної роботи визначається тим, що обґрунтований вибір методу і запропоновані засоби формування структури мобільної мережі та способи організації передавання інформації, які дають змогу істотно підвищити ефективність функ-
ціонування мобільних комп'ютерних мереж.

Запропоновані математичні моделі, процедури й алгоритми доведені до практичної реалізації у вигляді програм і можуть використовуватися при розробленні нового чи модифікації існуючих способів організації передавання інформації.

ЛІТЕРАТУРА

1. *Hu Y.-C., Johnson D.B., Perrig A.* SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks // Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), 2002. — Calicoon (NY, USA). — P. 3—13.

2. *Paradimitratos P., Haas Z. J.* Secure routing for mobile ad hoc networks // SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002). — San Antonio (TX, USA), 2002.

3. *Venkatraman L., Agrawal D. P.* Strategies for enhancing routing security in protocols for mobile ad hoc networks // Journal of Parallel and Distributed Computing, 2003. — Vol. 63. — № 2. — P. 214—227.

4. *Simmon G. J.* An Introduction to Shared Secret and/or Shared Control Schemes and The Application // Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992. — P. 441—497.

5. *Shamir A.* How to Share a Secret // Communications of the ACM, 1979. — №11. — P. 612—613.
Schneier B. Applied Cryptography, 2nd edition.

Стаття надійшла до редакції 19.05.09