

Реалізація Методу Виділення Зон Управління в Захищеній Комп'ютерній Мережі

Любомир Пархуць
кафедра захисту інформації
Національний університет "Львівська політехніка"
Львів, Україна
par7@i.ua

Марина Костяк
кафедра захисту інформації
Національний університет "Львівська політехніка"
Львів, Україна
markost@i.ua

Implementation of The Method of Allocation Zones Management in Secure Computer Network

Lubomyr Parkhuts
dept. of Information Protection
Polytechnic National University
Lviv, Ukraine
par7@i.ua

Maryna Kostiak
dept. of Information Protection
Polytechnic National University
Lviv, Ukraine
markost@i.ua

Анотація—Робота присвячена вирішенню проблеми що стосується підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення при їх створенні чи модернізації. Запропоновано евристичні алгоритми для реалізації методу виділення зон управління в захищеній комп'ютерній мережі та приведено основні результати досліджень.

Abstract—The work deals with the problem relating to improving the functioning of secure information networks for special purposes in their creation or modernization. A heuristic algorithms to implement the method of allocation zones management in a secure computer network and shows the main results of the research..

Ключові слова—алгоритм, інформаційна мережа, захист інформації, управління трафіком, оптимізація мережі.

Keywords—algorithm, information network, information security, traffic management, network optimization

I. ВСТУП

Подання структури захищеної інформаційної мережі у вигляді сукупності і способів взаємодії елементів, що входять до її складу, передбачає задання конфігурації мережі зв'язку, через яку проходить обмін інформацією між елементами мережі. При цьому, конфігурація мережі в основному визначається її топологією, просторовим розташуванням джерел та користувачів інформації, а конфігурація і вид мережі зв'язку є важливою структурною характеристикою її [1].

Для оптимізації структури захищеної інформаційної мережі та мінімізації трафіків зручно використовувати апарат теорії графів [2], який дозволяє реалізувати алгоритм впорядкованого перебору при пошуку оптимальної структури та мінімального трафіку [3, 4].

Із збільшенням розмірності інформаційної мережі при реалізації алгоритмів маршрутизації і управління інтенсивністю потоків виникає ряд труднощів, обумовлених багатьма причинами та специфікою функціонування захищеної інформаційної мережі спеціального призначення. Так, зокрема, при збільшенні розмірності мережі збільшується частка службового трафіку в загальному обсязі мережного трафіку і, отже зменшується продуктивність мережі, оскільки частина запитів користувачів не може бути обслужена через наявність службової інформації.

Маршрутні таблиці, якщо вони містять повну інформацію про те, як досягти будь-якого адресата мережі, можуть виявитися дуже великими, унаслідок чого значно ускладнюється реалізація вузлів комутації. Збільшується час доставки службової інформації і, отже, при виборі маршрутів використовується інформація, яка може в значній мірі не відповідати реальній ситуації, що має місце в мережі в даний момент часу.

Можливим варіантом вирішення проблеми маршрутизації і управління обсягом потоків в мережі є застосування принципу ієрархічної зонової адресації і маршрутизації [6].

В роботах [5-7] розглянуто питання оптимізації потоків трафіку в інформаційних мережах, запропоновано алгоритми адаптивної маршрутизації в захищеній інформаційній мережі з обмеженим вибором витікаючих каналів зв'язку, ієрархічну зону адресацію і маршрутизацію, а також розглянуто алгоритми адаптивної внутрішньозонової маршрутизації в захищеній локальній мережі.

Дана робота є логічним продовженням вказаних робіт. В ній розглянуто евристичні алгоритми для реалізації методу виділення зон управління в захищеній інформаційній мережі.

II. ОСНОВНА ЧАСТИНА

Знайти математично оптимальне теоретичне рішення щодо виділення зон управління в захищеній інформаційній мережі при достатньо великій кількості вузлів комутації є дуже непростою задачею, оскільки практично неможливо врахувати всі особливості її функціонування в екстремальних умовах, а також той факт, що в таких умовах необхідно враховувати особливу пріоритетність окремих видів інформації.

В такому випадку запропоновано застосувати евристичні алгоритми для реалізації методу виділення зон управління в захищеній інформаційній мережі спеціального призначення.

Розглянемо два евристичні алгоритми, що реалізують запропонований нами метод виділення зон управління [7].

При описі алгоритмів вважатимемо, що оргграф, який відображає інформаційну мережу, перетворений в неорієнтований граф, причому довжина кожного з ребер рівна сумі довжин ребер, що сполучають відповідні вершини оргграфа, тобто довжина ребра одержуваного графа відобразатиме інтенсивність сумарного (в двох напрямках) транзитного трафіку між суміжними вузлами інформаційної мережі.

Введемо такі позначення: N_u^0 – максимально допустиме число вузлів комутації (ВК) в зоні при використуванні децентралізованого методу управління; N_u^0 – максимально допустиме число в зоні при використуванні централізованого методу управління. Нехай для визначеності $N_u^0 > N_u^0$.

Розглянемо послідовний алгоритм виділення зон управління, суть якого полягає в тому, що куски $G_i = (X_i, Y_i)$ графа G_i формуються так, щоб кожний з них в множині Y_{ii} містив ребра з можливо більшою сумарною довжиною.

При цьому отримуємо локальний мінімум сумарної довжини V сполучних ребер.

Послідовний алгоритм складається з таких кроків:

1. Визначити початкову вершину x_i . Як початкова вибирається вершина з найменшим локальним ступенем

$p(x_i) = \min_{x_i \in X} p(x_i)$, тобто вершина, що має мінімальну сумарну довжину суміжних з нею ребер. Якщо таких вершин декілька, то вибираємо ту, у якій одне з ребер має найбільшу довжину.

При такому виборі початкової вершини формування зони починається з периферійних ВК, тобто ВК, які найменше пов'язані з іншими.

2. Сформувати черговий кусок розбиття. Включаємо в X_j вершину x_i і всі вершини, суміжні з нею. Позначимо множину вершин, включених в X_j , через Γx_i .

3. Якщо

$$\left(\left| X_j \right| = N_u^0 \ \& \ k_{u_i} \geq k_{u_i}^{(2)} \right) \vee \left(\left| X_j \right| = N_u^0 \ \& \ k_{u_i} < k_{u_i}^{(2)} \right),$$

то перейти до п.6.

Якщо

$$\left(\left| X_j \right| = N_u^0 \ \& \ k_{u_i} \geq k_{u_i}^{(2)} \right) \vee \left(\left| X_j \right| = N_u^0 \right)$$

то перейти до п.4.

Якщо

$$\left(\left| X_j \right| = N_u^0 \right) \vee \left(\left| X_j \right| < N_u^0 \ \& \ k_{u_i} < k_{u_i}^{(2)} \right),$$

то перейти до п.5.

4. Видалити "зайві вершини", тобто вершини, сумарна довжина зв'язків яких з рештою вершин в куску G_j мінімальна. Перейти до п.6.

5. Вибрати в G вершину, що задовольняє умові

$$\sigma(x_k) = p(x_k) - a_k = \max_{x_k \in X} G(x_k),$$

де a_k – сумарна довжина ребер, що з'єднують вершину x_k зі всіма вершинами, що не належать G_j . Побудувати множину Γx_k і перейти до п.3.

6. Вилучити кусок G_j , з графа G^* . Після вилучення отримуємо граф

$$G^* = (X^*, Y^*), \quad X^* = X \setminus X_j, \quad Y^* = Y \setminus Y_j.$$

Якщо для графа G^* :

$$\left(k_{u_i} \geq k_{u_i}^{(2)} \ \& \ |X^*| \leq N_u^a + \varepsilon^a \right) \vee \left(k_{u_i} < k_{u_i}^{(2)} \ \& \ |X^*| \leq N_u^a + \varepsilon^a \right),$$

то закінчити.

(Гут ε^0 позначено допустиме перевищення розміру куска, яке задається для того, щоб не вводити зайву зону управління, коли число вершин, що залишилося, не перевищує ε^0).

В протилежному випадку слід перейти до п.2, використовуючи як початкове граф G^* .

До переваг послідовного алгоритму відноситься його простота, результат можна отримати при невеликих витратах машинного часу. Проте в загальному випадку даний алгоритм може привести до неоптимальних результатів.

Кращі результати можуть бути отримані при розбитті мережі на зони з використанням ітераційних алгоритмів.

Розглянемо ітераційний алгоритм виділення зон управління, суть якого полягає в тому, що спочатку знаходиться (наприклад, за допомогою описаного вище алгоритму) деяке початкове розбиття графа $G = \{G_1^i, \dots, G_i^i\}$.

Потім обчислюється величина, на яку зміниться вага розбиття V при обміні вершинами (або групами вершин) між двома кусками G_i^i і G_j^i . Якщо вага розбиття зменшиться, то вершини (групи вершин) міняються місцями.

Процес продовжується до тих пір, поки не будуть виконані всі можливі перестановки. В алгоритмі, розробленому в даному параграфі, проводиться обмін одиничними вершинами.

Визначимо умови, при яких проводиться обмін вершинами між кусками. Розглянемо два куски з розбиття – A і B .

Нехай зовнішня і внутрішня ваги розбиття відповідно рівні

$$E_a = \sum_{y \in B} r_{ay}; \quad I_a = \sum_{y \in B} r_{ax}$$

Позначимо $D_z = E_z - I_z$. При обміні вершинами a і b вага розбиття V змінюється на величину $\Delta V = D_a - 2r_{ab}$. Отже, мінятися місцями повинні лише ті вершини, для яких $\Delta V > 0$.

Крім того, оскільки при обміні вершинами може змінитися значення коефіцієнта централізації зони, необхідно ввести поняття допустимого обміну.

Обмін вершинами a і b назвемо допустимим, якщо при обміні значення коефіцієнта централізації кожного з кусків розбиття не переходить через граничне значення $k_u^{(2)}$, тобто якщо до обміну виконувалася нерівність $k_u \leq k_u^{(2)}$, то вона повинна виконуватися і після обміну; аналогічно, якщо до обміну виконувалася нерівність $k_u > k_u^{(2)}$, то вона повинна виконуватися і після обміну.

Ітераційний алгоритм складається з таких кроків:

1. Визначити початкове розбиття графа мережі G з використанням послідовного алгоритму.

2. Зафіксувати пару кусків розбиття G_i і G_j . Обчислити D_{x_k} для всіх $x_k \in X_i$ для всіх $x_l \in X_j$.

3. Вибрати пару вершин $x_k \in X_i$, $x_l \in X_j$ таких, що

$$\begin{cases} \Delta V = \max_{(x_k, x_l)} \Delta V, \\ \Delta V > 0. \end{cases}$$

Якщо така пара знайдена і обмін допустимий, то поміняти вершини місцями. В протилежному випадку перейти до п. 5.

4. Сформувати множини $X_i = X_i \setminus x_k$ і $X_j = X_j \setminus x_l$, перейти до п. 3.

5. Якщо є не розглянуті пари G_i і G_j , то перейти до п. 2, якщо таких пар немає, то закінчити.

Даний ітераційний алгоритм дозволяє значно поліпшити результати розбиття графа інформаційної в порівнянні з послідовним алгоритмом. Подальше зменшення ваги розбиття може бути досягнуто ціною значного ускладнення даного алгоритму, що полягає в перестановці груп вершин.

III. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Дослідження запропонованих евристичних алгоритмів для реалізації методу виділення зон управління в захищеній інформаційній мережі було проведено на ряді топологічних структур захищених інформаційних мереж, які генерувалися випадковим чином, з використанням комп'ютерного моделювання.

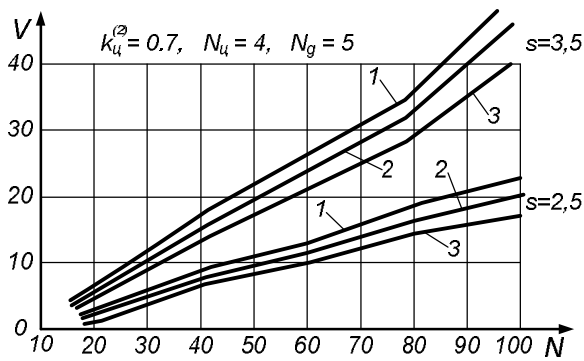
Результати отриманих результатів дослідження залежно від числа вузлів в мережі N і середньої зв'язаності мережі $\nu = M/N$, де M – число каналів зв'язку (КЗв), приведено на рис.1.

Крива 1 характеризує залежність ваги розбиття від числа вузлів в мережі при розподілі вузлів по зонах випадковим чином; крива 2 – залежність, відповідна послідовному алгоритмі розбиття; крива 3 – залежність, відповідна ітераційному алгоритму розбиття.

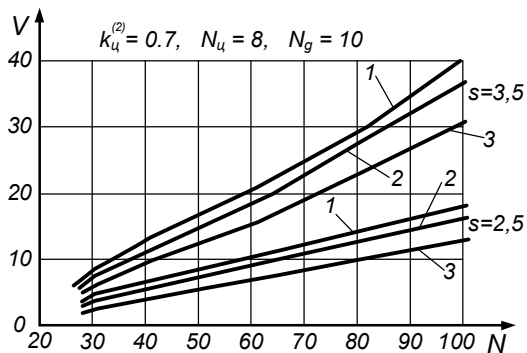
На рис.2 приведено графіки залежності відносного зменшення ваги розбиття при використанні розроблених алгоритмів від числа вузлів мережі.

Крива 1 – відповідає ітераційному алгоритму; крива 2 – послідовному алгоритму. Значення Δ обчислюється за формулою $\Delta = (V_c - V_i)/V_c$, де V_c – вага розбиття при випадковому розподілі вузлів інформаційної мережі по зонах; V_i – вага розбиття при використуванні

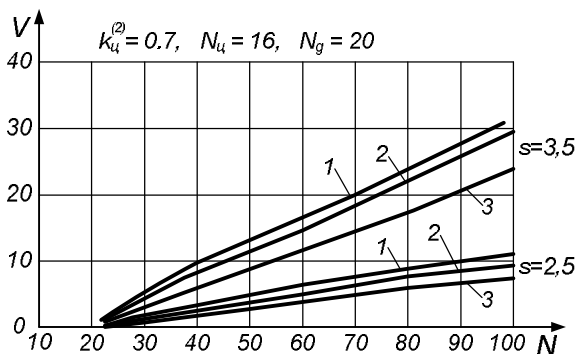
одного з алгоритмів розбиття (послідовного при $i = 1$ або ітераційного при $i = 2$).



а)



б)



в)

Рис. 1. Результати дослідження розроблених алгоритмів на ряді топологічних структур захищених інформаційних мереж

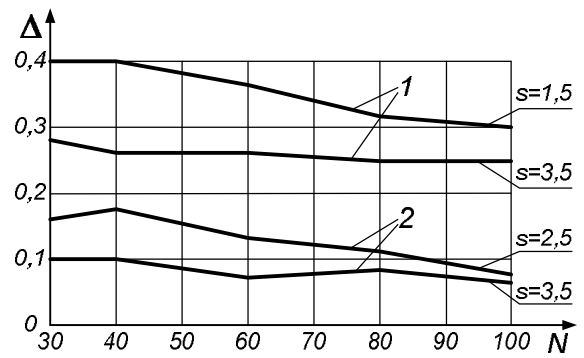


Рис. 2. Залежність відносного зменшення ваги розбиття при використанні розроблених алгоритмів від числа вузлів мережі

IV. ВИСНОВКИ

Запропоновані евристичні алгоритми для реалізації методу виділення зон управління в інформаційній мережі дозволяють оптимізувати обсяг трафіків в захищеній інформаційній мережі, а також збільшити пропускну здатність та швидкість інформаційної мережі.

Це є важливим фактором для роботи захищених інформаційних мереж спеціального призначення, особливо в екстремальних умовах та при надзвичайних ситуаціях, коли частина структури інформаційної мережі може бути пошкоджена чи зруйнована внаслідок агресивних дій супротивника.

Проведені дослідження та результати комп'ютерного моделювання підтверджують достатню ефективність запропонованих алгоритмів.

ЛІТЕРАТУРА REFERENCES

- [1] В.А. Кудинов, Л.Т. Пархуць, В.А. Хорошко, Оптимизация структуры информационной сети. Научно-технический журнал «Защит информации», № 3, 2004. – с.44-49.
- [2] К. Берг, Теория графов и ее применения. М.: Изд-во иностр.лит., 1962. -264с.
- [3] И.Р. Конеев, А.В. Беляева, Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. –752с.
- [4] Дж. Ирвин, Д. Харль, Передача данных в сетях: инженерный подход. – СПб.: БХВ-Петербург, 2003. –448с.
- [5] М.Ю. Костяк, Л.Т.Пархуць, Задача управления обмеженням інтенсивності потоків в захищеній інформаційній мережі. Системи обробки інформації. – Харків: ХУПС. – 2013. – Вып. 3(110), Том 2. – С. 105-107.
- [6] В.Б. Дудикевич, М.Ю. Костяк, Л.Т. Пархуць, В.О. Хорошко, Ієрархічна зонава адресація і маршрутизація в захищеній інформаційній мережі. Вісник Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 6 (136), Ч.1., – С.143-149.
- [7] М.Ю. Костяк, Алгоритми адаптивної внутрішньозонової маршрутизації в захищеній локальній мережі / М.Ю.Костяк, Л.Т.Пархуць // Інформаційна безпека Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 1, – С. 38-43.