

АНАЛІЗ ЙМОВІРНОСТІ КОМПРОМЕТАЦІЇ ФРАГМЕНТА ЛОКАЛЬНОЇ МЕРЕЖІ

Барилко Д.О.

Харківський національний університет радіоелектроніки,
Україна.

E-mail: dmytro.barylko@nure.ua

Abstract

One of the key issues in creating a local network is ensuring its security. Information networks are becoming increasingly complex every day, which makes them more vulnerable to cyber threats. When designing a local network, it is necessary to assess the likelihood of threats at every stage of its development, which defines the relevance of this work. Thus, one of the key indicators of security is the assessment of the probability of compromising a fragment of the local network. To achieve this, analytical modelling must be conducted to evaluate the probability of compromising the route between a pair of nodes — the sender and the receiver — within the local network.

Одним з ключових питань при створенні локальної мережі є питання забезпечення захисту мережі. С кожним днем інформаційні мережі стають все більш складними, що робить їх більш уразливими для кіберзагроз. Під час створення локальної мережі потрібно оцінювати її на ймовірність загроз при кожному етапі побудови, що й визначає актуальність роботи.

Так, одним з ключових оцінок захищеності є оцінка ймовірності компрометації фрагмента локальної мережі, для цього потрібно провести аналітичне моделювання щодо оцінювання ймовірності компрометації маршруту між парою вузлів відправника та отримувача в межах локальної мережі.

Для реалізації та тестування механізмів безпеки локальної мережі у роботі проведено дослідження мережі з топологією, яка складається з чотирьох маршрутизаторів (R1 – R4, IOSv), двох комутаторів (SW1, SW2, IOSvL2) і двох кінцевих пристроїв (PC1 – PC2), підключених до відповідних мережних вузлів. У топології реалізовано декілька логічно розділених підмереж, що дозволяє моделювати роботу VLAN, маршрутизації та безпечного розмежування трафіку. Крім базової маршрутизації, конфігурація враховуватиме аспекти мережної безпеки.

Компрометація – це процес розкриття, втрати або поширення конфіденційної інформації, унаслідок чого втрачається її конфіденційність, цілісність або доступність [1]. Схема маршруту локальної мережі для дослідження показана на рис. 1. Дослідження проведено в припущенні, що вузли мережі захищено з використанням налаштування механізму Port Security, налаштування віддаленого доступу SSH та налаштування алгоритму MD5 для здійснення автентифікації протоколу маршрутизації OSPF, тому найбільш вразливими елементами мережі є канали зв'язку.

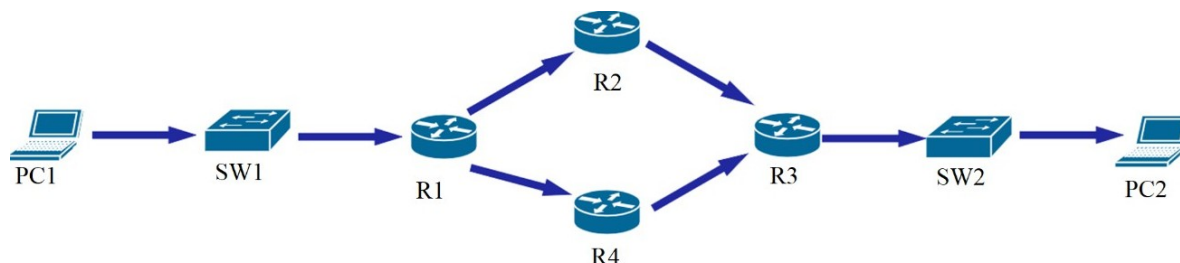


Рис. 1. Схема маршруту локальної мережі для дослідження

В роботі визначено ймовірність компрометації маршруту між PC1 і PC2 згідно методики, яку описано в [1, 2]. Згідно зі структурою, маршрут є композитним, тобто не може бути представлений виключно послідовним чи паралельним зв'язком каналів, а є їх комбінацією, що видно з рисунку 1.

Тоді, розділивши умовно цей маршрут на послідовні фрагменти, записано загальну формулу ймовірності його компрометації наступним чином:

$$P_{PC1-PC2} = 1 - (1 - P_1)(1 - P_2)(1 - P_3)(1 - P_4)(1 - P_5), \quad (1)$$

де P_1 – ймовірність компрометації каналу між PC1 і SW1;

P_2 – ймовірність компрометації каналу між SW і R1;

P_3 – ймовірність компрометації фрагменту між R1 і R2;

P_4 – ймовірність компрометації каналу між R3 і SW2;

P_5 – ймовірність компрометації каналу між SW2 і PC2.

Водночас фрагмент, якому співвідноситься ймовірність компрометації P_3 , є складним і містить послідовні і паралельні зв'язки між каналами. Отже, P_3 можна визначити так:

$$P_3 = P_{R1-R3} = (1 - (1 - P_{31})(1 - P_{32}))(1 - (1 - P_{33})(1 - P_{34})), \quad (2)$$

де P_{31} – ймовірність компрометації каналу між R1 і R2;

P_{32} – ймовірність компрометації каналу між R2 і R3;

P_{33} – ймовірність компрометації каналу між R1 і R4;

P_{34} – ймовірність компрометації каналу між R4 і R3.

Прийнято, що всі ймовірності компрометації каналів рівні й дорівнюють 0,2. Тоді, якщо маршрут буде простим і проходить напрям від R1 до R3, можна зробити розрахунок за формулою (1):

$$P_{PC1-PC2} = 1 - (1 - 0,2)(1 - 0,2)(1 - 0,2)(1 - 0,2)(1 - 0,2) = 0,67232.$$

Якщо маршрут композитний, тоді спочатку потрібно розрахувати фрагмент, що містить паралельні гілки $R1 \rightarrow R2 \rightarrow R3$ та $R1 \rightarrow R4 \rightarrow R3$ за формулою (2):

$$P_3 = P_{R1-R3} = (1 - (1 - 0,2)(1 - 0,2))(1 - (1 - 0,2)(1 - 0,2)) = 0,1296.$$

Тепер після визначення ймовірності компрометації фрагменту можна порахувати ймовірність компрометації маршруту між PC1 і PC2 за формулою (1):

$$P_{PC1-PC2} = 1 - (1 - 0,2)(1 - 0,2)(1 - 0,1296)(1 - 0,2)(1 - 0,2) = 0,6435.$$

З розрахунків можна побачити, що композитний маршрут кращий за простий (послідовний) і зменшує ймовірність компрометації на 4,29%, що підвищує безпеку та надійність даного маршруту.

Побудовано графіки залежності ймовірності компрометації простого маршруту при зміні P_3 від 0,1 до 0,9 (рис.2 (а)). Водночас залежність ймовірності компрометації композитного маршруту від зміни, наприклад, P_{31} від 0,1 до 0,9, виглядає, як показано на рисунку 2 (б).

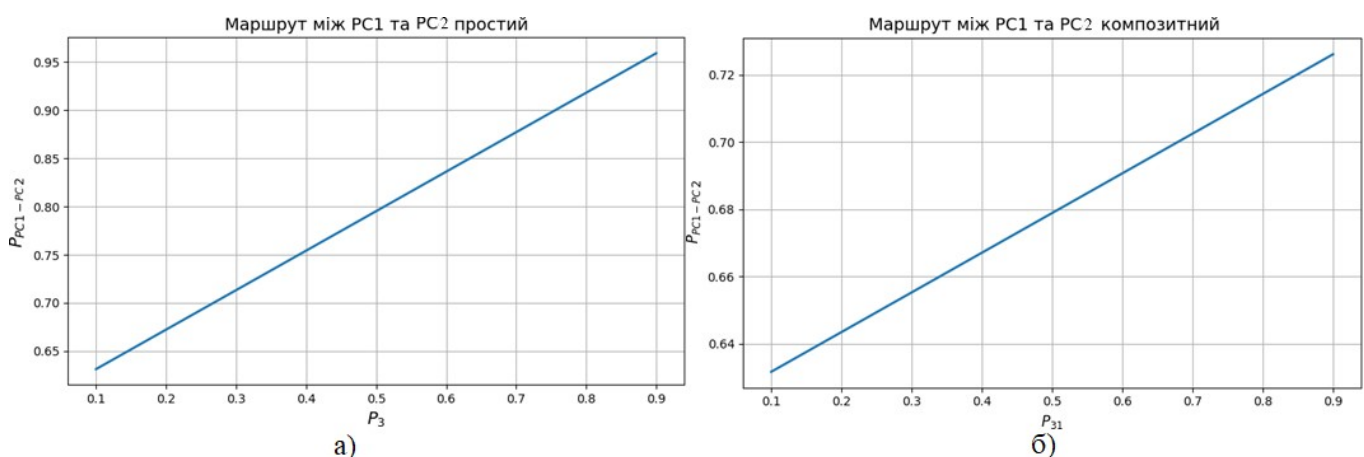


Рис. 2. Ймовірність компрометації простого маршруту при зміні (а) P_3 і (б) P_{31} від 0,1 до 0,9

Для зручності порівняння отриманих значень результати розрахунків представлено в таблиці 1 і таблиці 2.

Таблиця 1. Імовірність компрометації простого маршруту

P_3	$P_{PC1-PC2}$
0,1	0,63136
0,2	0,67232
0,3	0,71328
0,4	0,75424
0,5	0,7952
0,6	0,83616
0,7	0,87712
0,8	0,91808
0,9	0,95904

Таблиця 2. Імовірність компрометації композитного маршруту

P_{31}	P_3	$P_{PC1-PC2}$
0,1	0,1008	0,63169
0,2	0,1296	0,64348
0,3	0,1584	0,65528
0,4	0,1872	0,66708
0,5	0,216	0,67887
0,6	0,2448	0,69067
0,7	0,2436	0,70247
0,8	0,3024	0,71426
0,9	0,3312	0,72606

Результати розрахунків показали, що використання композитних маршрутів дозволяє знизити їх загальну ймовірність компрометації завдяки наявності фрагментів з паралельними гілками. Зі зростанням ймовірності компрометації окремих каналів прості маршрути демонструють вищу вразливість, тоді як композитні шляхи забезпечують значно нижчу ймовірність компрометації. Отже, використання композитних маршрутів у структурі локальної мережі підвищує її загальну надійність та безпеку шляхом зменшення ймовірності компрометації.

Література

1. Лемешко О. В., Єременко О. С., Невзорова, О. С. Потоківі моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ. 2020. 308 с.
2. Лемешко О.В., Єременко О.С., Євдокименко М.О., Шаповалова А.С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах // монографія. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків: ХНУРЕ. 2022. 198 с.