РОЗДІЛ 3
МОДЕЛІ ТА МЕТОДИ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

3.1. Характеристика засобів мережної безпеки в інфокомунікаціях

Як показав проведений аналіз [1–19], одним з найважливіших завдань, що регламентується стандартами побудови ІКМ, є реалізація функцій інформаційної безпеки. За стандартом ITU-T X-805 [20] в архітектурі безпеки (рис. 3.1) ІКМ умовно виокремлюють такі площини та рівні:

– функціональні площини безпеки:

- контролю (для передачі службової інформації для моніторингу стану ресурсів ІКМ);
- управління (для передачі службової інформації з метою поточного управління ресурсами ІКМ);
- користувача (для передачі інформації);

– рівні безпеки:

- інфраструктури, яка складається з елементів ІКМ (каналів зв'язку, маршрутизаторів, серверів тощо);
- сервісів (послуг), що надаються кінцевим користувачам ІКМ та провайдерам;
- застосунків, які беруть участь у комунікаційному процесі та генерують трафік користувачів, який циркулює в мережі.

Відповідно до цих площин і рівнів формуються модулі захисту ІКМ, які характеризуються такими параметрами: управління доступом; автентифікація; збереження інформації; конфіденційність даних; безпека зв'язку; цілісність даних; доступність; секретність.

За вимогами стандартів ITU, забезпечення інформаційної безпеки здійснюється в межах трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки застосунків (рис. 3.1) [20]. У цьому випадку ефективність роботи верхніх двох рівнів цілком і повністю визначається ефективністю функціонування засобів рівня безпеки інфраструктури, основними завданнями якого є: забезпечення безпеки на рівні мережних елементів (комутаторів, маршрутизаторів, серверів), каналів зв'язку та маршрутів загалом, які з них складаються.

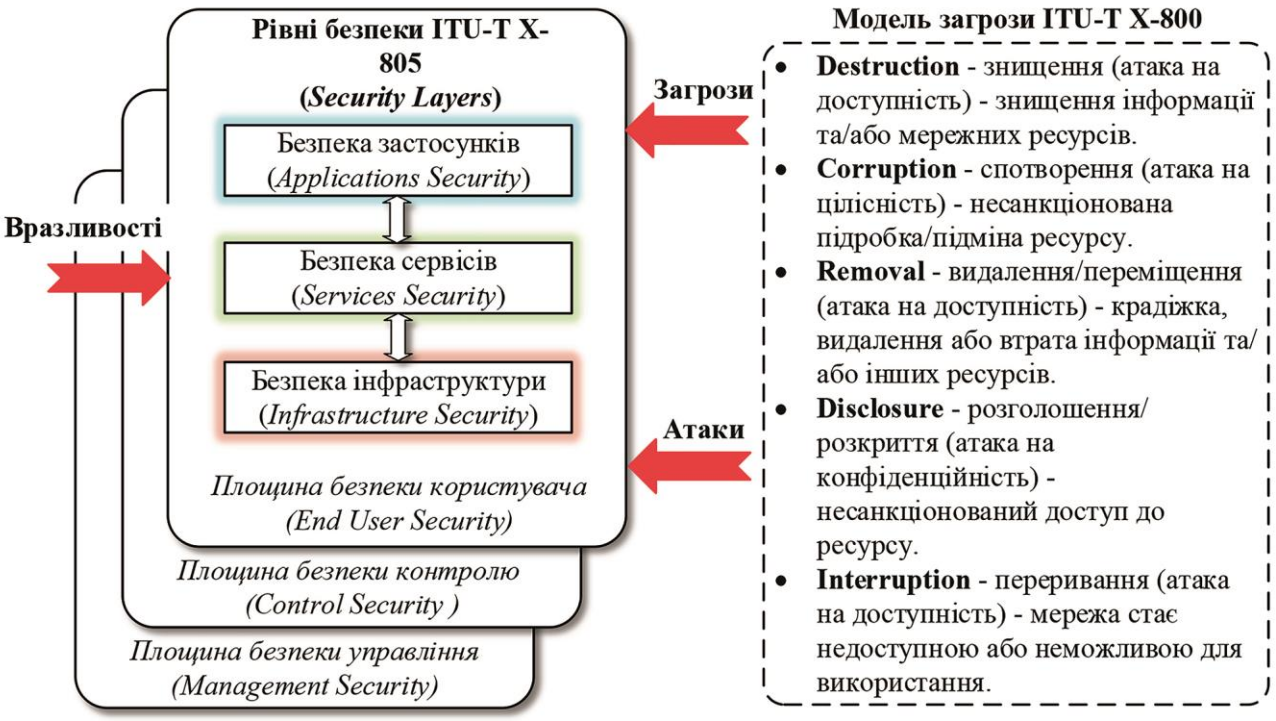


Рис. 3.1. Архітектура безпеки відповідно до стандарту ITU-T X-805

Якщо розглядати забезпечення мережної безпеки з точки зору рівнів моделі EMBBC (Open Systems Interconnection, OSI) і стандарту ISO 7498-1, а також архітектури безпеки згідно з ISO 7498-2 [21–23], то відповідність їх рівнів може бути представлена у вигляді схеми (рис. 3.2). Зокрема сервіси безпеки мають забезпечуватися протоколами відповідних рівнів моделі взаємодії відкритих систем. У свою чергу безпека на мережному рівні повинна підтримуватися і забезпечуватися також протоколами маршрутизації.

До засобів забезпечення мережної безпеки, як правило, належать автентифікація; криптографічний захист; системи аналізу та аудиту; виконання політик безпеки; використання міжмережних екранів; застосування систем виявлення та протидії атакам; управління трафіком і контроль доступу [24, 25]. Важливе значення в управлінні трафіком під час конфігурування мережного обладнання відводиться завданням формування списків доступу (Access Control List, ACL) [12, 13, 24]. Списки доступу можна використовувати для контролю над потоками пакетів, їх ідентифікації, для обмеження поширення оновлень маршрутизації, але однією з найбільш важливих причин застосування списків доступу є забезпечення мережної безпеки. Списки доступу є складниками функціональних можливостей «брандмауера» (міжмережного екрана, Firewall) маршрутизаторів, які часто розташовані між LAN і WAN мережами. Можна також використовувати списки доступу для управління трафіком на маршрутизаторах, розміщених між двома мережами.

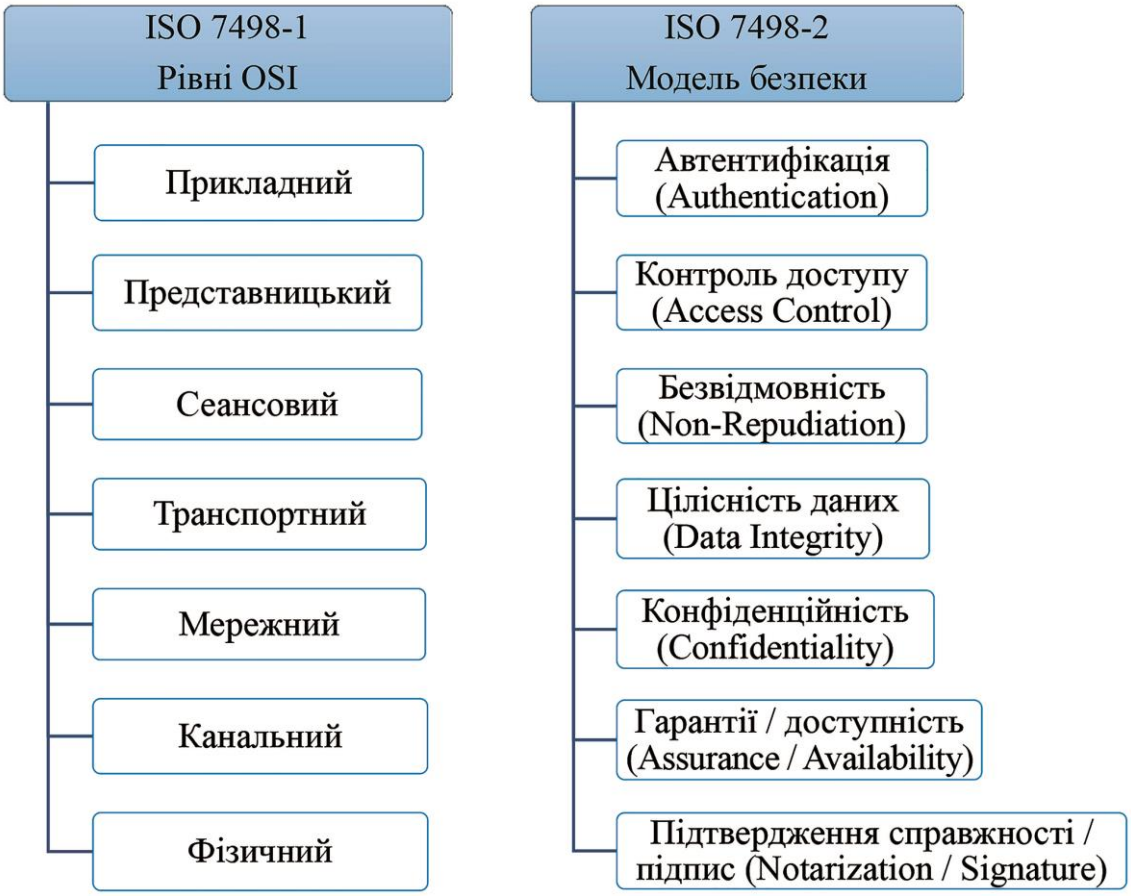


Рис. 3.2. Відповідність рівнів OSI та моделі безпеки

ACL дозволяють фільтрувати мережний трафік шляхом заборони або дозволу передачі пакетів, що надходять на вхідні та/або вихідні інтерфейси маршрутизатора. У процесі фільтрації трафіку маршрутизатор перевіряє кожен пакет і приймає рішення про те, передати його або відкинути, ґрунтуючись на ACL. Крім того, у розподілі канального ресурсу ІКМ під час конфігурування механізмів PQ, CQ, CBWFQ і LLQ за допомогою посилань на ACL можна конкретизувати, яким саме пакетам (потокам) виділяється та чи інша черга та пропускна здатність інтерфейсу. Стандартні ACL використовуються для фільтрації пакетів винятково на основі IP-адреси відправника пакетів на мережному рівні моделі OSI, тоді як розширені ACL можуть оперувати інформацією про ймовірного відправника та/або отримувача пакетів, що належить мережному та транспортному рівням моделі OSI: IP-адреси, номери портів транспортних протоколів TCP та UDP, значення полів пріоритету пакетів тощо.

Основним недоліком технологій фільтрації трафіку, основаних на використанні ACL, є те, що їх налаштування на маршрутизаторі здійснюється вручну адміністратором мережі, як правило, у режимі командного рядка. Це, з одного боку, негативно позначається на оперативності реакції на

можливі загрози безпеці мережі та комутаційного обладнання, а з іншого, – установлює пряму залежність між рівнем підготовки, досвіду та кваліфікації адміністраторів мережі загалом та рівнем її безпеки. Крім того, у разі виходу з ладу мережного обладнання на відновлення раніше налаштованих списків доступу можуть знадобитися тижні, тому в SDN-мережах ACL, як правило, зберігаються на серверах мережної операційної системи, а в перспективі завдання формування та коригування ACL мають бути автоматизовані.

Ключове значення в забезпеченні мережної безпеки також мають криптографічні засоби захисту інформації, які широко реалізуються в сучасних ІКМ. Наприклад, за умови порогової криптографії на стороні відправника конфіденційне повідомлення (секрет) розбивається на декілька частин, які загалом мають доставлятись отримувачу незалежно одна від одної. Зокрема повідомлення може бути дешифровано лише за наявності в отримувача більш ніж заданої порогової кількості його частин. Таким чином, у використанні порогової криптографії зловмисник має скомпрометувати не менше за порогову кількість частин повідомлення. Слід зазначити, що порогова криптографія вважається однією з найбезпечніших криптосистем та використовується в сучасних рішеннях, наприклад, таких як RSA (алгоритм Рівеста–Шаміра–Алдемана), криптосистема Пейє, криптосистема Дамгорда–Юрика, схема Ель-Гамаля, алгоритм електронного цифрового підпису із застосуванням еліптичних кривих [26–28].

Концепція порогової криптографії широко використовується та має різне застосування для побудови сучасних ІКМ і реалізується в технологіях хмарних обчислень, механізмах автентифікації, управлінні ключами, технології Інтернету речей (Internet of Things, IoT), мобільних самоорганізованих мережах (Mobile Ad hoc Network, MANET), сенсорних мережах, електронних цифрових підписах, застосунках електронного голосування, візуальній криптографії тощо (табл. 3.1) [27].

Схеми розділення секрету (secret sharing schemes) можна класифікувати таким чином [28]:

- проактивне розділення секрету;
- динамічне розділення секрету;
- розділення секрету з можливостями вето;
- робастне розділення секрету;
- поліноміальне розділення секрету;
- схеми, основані на китайській теоремі про остачі (Chinese Remainder Theorem, CRT);

- анонімне розділення секрету;
- розділення секрету на основі систематичних блокових кодів;
- розділення секрету у вигляді «чорної скрині» (black box secret sharing);
- візуальне розділення секрету.

Таблиця 3.1

Напрями застосування різних порогових схем в ІКМ

Напрям застосування	Схема порогового розділення секрету	Переваги використання
Хмарні обчислення	Схема Шаміра	Зменшення кількості ключів; забезпечення конфіденційності приватних даних; безпечне та надійне зберігання даних; безпечна передача даних.
Автентифікація	Схема Шаміра, криптосистема Пейє	Швидка групова автентифікація користувачів; стійкість до масиву атак, масштабованість, гнучкість; легковагова, масштабована групова автентифікація в IoT; анонімна автентифікація в IoT.
Ad-Hoc мережі	Схема Шаміра, порогова криптографія на основі еліптичних кривих (ECC)	Стійкість до сертифікатів фальшивих відкритих ключів, захист від уразливостей, спричинених шкідливими вузлами; високий рівень безпеки, доступний сервіс керування ключами.
Електронний цифровий підпис	Схема Шаміра, схема Шаміра з криптосистемою Ель-Гамаля	Відстежуваність підписів, множина політик підпису; відсутність потреби в довіреній третій стороні.
Електронне голосування	Схема Шаміра, схема Асмута–Блума, криптосистема Пейє	Зменшення порушення цілісності даних, відсутність потреби в довіреній третій стороні; надійність, конфіденційність; підтримка множинного та нульового вибору, ієрархічність; використання властивості гомоморфності.
Цифрове оброблення зображень	Схема Шаміра	Безпечна передача зображення через незахищені мережі.

Так, наприклад, схема Шаміра належить до схем поліноміального розділення секрету, тоді як схема Асмута–Блума основана на використанні теореми CRT. У схемі візуального розділення секрету візуальне зображення було як конфіденційне повідомлення. До прикладів забезпечення мережної безпеки також може належати концепція безпечної маршрутизації, яка реалізована в ІКМ, наприклад, за допомогою механізму SPREAD [29–33]. Це рішення основане на багатошляховій передачі частин конфіденційного повідомлення, які сформовані відповідно до схеми Шаміра. Зокрема чим більше шляхів буде використано та чим менше вони будуть перетинатися, тим з меншою ймовірністю компрометації повідомлення буде доставлено отримувачу. Подібні особливості у свою чергу накладають додаткові вимоги на використовувані математичні моделі та методи маршрутизації в ІКМ.

3.2. Аналіз методів безпечної маршрутизації в ІКМ

У роботі [34] було запропоновано новий евристичний підхід щодо безпечної міждоменної маршрутизації *Secure Multi-Party Computation* (*SMPC*). У цьому випадку міждоменна маршрутизація передбачає координацію між взаємно «недовірливими» сторонами, що призводить до виникнення вимог, відповідно до яких протокол BGP забезпечує автономність, гнучкість і конфіденційність шляхом розподіленого виконання рішень на основі політик під час процесу ітеративного обчислення маршруту. Цей підхід має слабку збіжність і робить планування та забезпечення відмовостійкості складним завданням. У зв’язку з цим у [34] запропоновано принципово інший підхід до обчислення міждоменного маршруту на основі SMPC, який забезпечує кращу гарантію конфіденційності, ніж BGP, і дозволяє розгортати нові парадигми політик.

У праці [35] отримав подальшого розвитку алгоритм безпечної оверлейної маршрутизації на основі схеми ймовірнісного передрозподілу ключів, яка набула широкого застосування в безпроводових мережах. Запропоновано масштабоване рішення для мереж високої розмірності з кількістю вузлів більшою ніж тисяча, що базується на детерміністському алгоритмі на основі алгоритму Дейкстри (Deterministic Dijkstra-based Algorithm, DDA), який дозволяє розраховувати оптимальні безпечні шляхи в оверлейних безпроводових мережах за умови часової складності, значно нижчій, ніж в оригінальному алгоритмі. Також у [35] запропоновано відповідну апроксимацію для знаходження шляху, близького до оптимального, з точністю до 1 % порівняно з DDA.

У роботах [29, 30] представлено та досліджено механізми SPREAD (Secure Protocol for Reliable dAta Delivery) та H-SPREAD (Hybrid Secure Protocol for Reliable dAta Delivery) посилення безпечної передачі повідомлень у MANET (рис. 3.3). Основна ідея полягає в тому, щоб розділити конфіденційне повідомлення на кілька фрагментів – частин, а потім передавати ці частини від відправника до отримувача множиною шляхів, які не перетинаються, так, щоб навіть якщо певну кількість частин повідомлення буде скомпрометовано, секретне повідомлення загалом залишиться нескомпрометованим. Запропоновано загальну архітектуру системи: математичну модель для створення та реконструкції частин повідомлення, оптимальний розподіл його частин за декількома шляхами з точки зору безпеки, а також підходи щодо розрахунку мультишляху в мережах MANET.

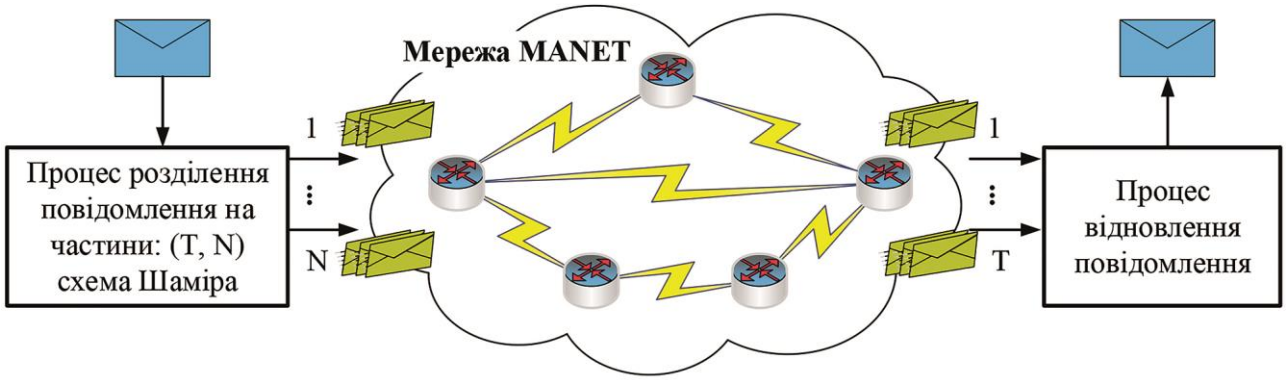


Рис. 3.3. Загальна архітектура роботи механізму SPREAD

Порівняно з проводовими мережами забезпечення безпеки в MANET пов’язано з виявленням і запобіганням множини наявних уразливостей та атак [36]. По-перше, радіоканали більш сприйнятливі до атак як пасивного прослуховування, так і активного втручання в сигнали та здійснення завад. По-друге, більшість протоколів маршрутизації в MANET припускають довірчі взаємодії між вузлами для здійснення передачі пакетів. Залежність від такої взаємодії робить передачу даних більш уразливою щодо несанкційного доступу, підміни даних та атак типу «відмова в обслуговуванні». По-третє, відсутність фіксованої інфраструктури та централізованого управління ускладнює застосування більшості традиційних рішень щодо забезпечення мережної безпеки.

Унаслідок використання механізму SPREAD вдається знизити ймовірність компрометації переданого повідомлення, тому що помітно ускладнюється завдання зловмисника: йому необхідно скомпрометувати не один маршрут, яким передається нерозділене повідомлення, а всі шляхи, якими передаються його частини. Зокрема під компрометацією повідомлення розуміється подія, пов’язана з несанкційним доступом до його вмісту.

Для забезпечення безпечної маршрутизації повідомлення в мережі відповідно до механізму SPREAD необхідно вирішити такі завдання [29, 30]:

1. Розрахунок множини маршрутів, що не перетинаються, між заданими вузлами «відправник» і «отримувач».
2. Розділення конфіденційного повідомлення, що передається, на множину частин відповідно до обраної схеми Шаміра.
3. Розподіл множини частин повідомлення між множиною маршрутів, визначених у процесі вирішення першого завдання.

Варто окремо зазначити, що ймовірність компрометації шляху багато в чому залежить як від кількості складників його вузлів і каналів зв'язку, так і від параметрів їх безпеки, тобто кожен елемент (вузол, канал) шляху може бути скомпрометований з певною ймовірністю. У загальному випадку шляхи, які використовуються для передачі частин розділеного відповідно до схеми Шаміра [29, 30, 33] повідомлення, можуть мати різні значення ймовірності компрометації. На жаль, у межах відомих рішень, присвячених реалізації механізму SPREAD, не враховуються параметри безпеки (зокрема ймовірність компрометації) цих шляхів. Крім того, подібні рішення орієнтовані на використання лише шляхів, які не перетинаються, що негативно впливає на ефективність використання доступного мережного ресурсу.

У роботах [37, 38] пропонується під час вибору маршруту в ІКМ враховувати ризики інформаційної безпеки. Це забезпечується шляхом відповідного формування маршрутних метрик, коли в них сумісно з QoS-показниками враховується і показник ризику інформаційної безпеки елементів системи маршрутизації. Цей підхід дозволяє динамічно вибрати найбільш безпечний маршрут потоків, що передаються, як в умовах активних атак, так і в разі пасивного аналізу ризиків у системі маршрутизації.

3.3. Удосконалення методу безпечної маршрутизації повідомлень шляхами, що не перетинаються: проактивний підхід

3.3.1. Метод безпечної маршрутизації повідомлень шляхами, що не перетинаються в ІКМ

Як показав проведений аналіз [29–33, 37, 38], можливість аналітичного розрахунку ймовірності компрометації повідомлення, що передається в мережі, багато в чому визначається особливостями структурної побудови ІКМ і типами використовуваних маршрутів. Відомо, що множину шляхів у мережі можна

умовно поділити на дві підмножини: підмножина шляхів, що не перетинаються, та підмножина шляхів, які допускають вузловий або канальний перетин [39–42].

Одним з напрямів забезпечення заданого рівня мережної безпеки в ІКМ є реалізація механізму SPREAD, основаного на багатошляховій маршрутизації повідомлення, що передається, попередньо розділеного на частини відповідно до схеми Шаміра [26–32]. Унаслідок застосування такої схеми вдається знизити ймовірність компрометації переданого повідомлення, тому що зловмисник для його компрометації повинен скомпрометувати, як правило, усі шляхи, якими передаються частини розділеного повідомлення.

У межах відомого методу безпечної маршрутизації використовуються такі позначення:

Константи

S_{msg} і D_{msg} — вузли «відправник» та «отримувач» для повідомлення, що передається;

M — кількість використовуваних шляхів, що не перетинаються, у разі маршрутизації частин повідомлення;

M_i — кількість каналів зв'язку в i-му шляху, які можуть бути скомпрометовані $\left(i = \overline{1, M}\right)$;

p_i^j — імовірність компрометації j-го каналу зв'язку i-го шляху $\left(i = \overline{1, M},\ j = \overline{1, M_i}\right)$;

(T, N) — параметри схеми Шаміра, де N – загальна кількість частин, на які розділяється повідомлення, що передається, унаслідок застосування схеми Шаміра; T – мінімальна кількість частин, за якими можливо відновити повідомлення, що передається $\left(T \le N\right)$;

γ_P — допустима ймовірність компрометації повідомлення в мережі.

Кількісні показники

p_i — імовірність компрометації i-го шляху $\left(i = \overline{1, M}\right)$;

P_{msg} — імовірність компрометації повідомлення загалом за умови його передачі частинами мережею.

Змінні

n_i — цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м шляхом $\left(i = \overline{1, M}\right)$.

У механізмі SPREAD у процесі багатошляхової маршрутизації та балансування кількості частин конфіденційного повідомлення шляхами необхідно забезпечити заданий рівень мережної безпеки, представленої, наприклад, імовірністю компрометації переданого повідомлення:

$$P_{msg} \le \gamma_P . \tag{3.1}$$

Під час подальших міркувань передбачається, що відправник та отримувач безпечні, тобто ймовірності компрометації вузла-відправника та вузла-отримувача дорівнюють нулю. Крім того, вважається [29, 30], якщо елемент (вузол, канал) шляху скомпрометовано, то всі фрагменти, що передаються через цей елемент, також будуть скомпрометовані. Тоді ймовірність компрометації i-го шляху, що складається з M_i елементів, можна розрахувати за допомогою формули

$$p_i = 1 - \left(1 - p_i^1\right)\left(1 - p_i^2\right)\ldots\left(1 - p_i^{M_i}\right) = 1 - \prod_{j=1}^{M_i}\left(1 - p_i^j\right). \tag{3.2}$$

Крім того, для розрахунку керуючих змінних n_i $\left(i = \overline{1, M}\right)$, що регламентують процес розподілу фрагментів повідомлення, яке передається, шляхами, що не перетинаються, має виконуватися така умова [29]:

$$\sum_{i=1}^{M} n_i = N . \tag{3.3}$$

У разі використання схеми Шаміра з параметрами $T < N$ мають виконуватися умови

$$N - n_i < T , \left(i = \overline{1, M}\right), \tag{3.4}$$

тоді як у разі використання схеми без надмірності, якщо $T = N$, мають місце такі умови:

$$1 \le n_i \le T - 1, \left(i = \overline{1, M}\right). \tag{3.5}$$

Виконання умови (3.5) гарантує, що у випадку компрометації всіх маршрутів, крім i-го, зловмисникові не вдасться відновити повідомлення загалом.

Однією з основних умов, яка в обов'язковому порядку має виконуватися в процесі безпечної маршрутизації, є те, що ймовірність компрометації повідомлення в разі його передачі мережею не повинна перевищувати заданого допустимого значення (3.1). Тоді ймовірність компрометації повідомлення, розділеного на N частин відповідно до схеми Шаміра $\left(N, N\right)$ і переданого за M шляхами, визначається виразом [29]

$$P_{msg} = \prod_{i=1}^{M} p_i . \tag{3.6}$$

Перевагами описаного методу є те, що використання множини шляхів, що не перетинаються, у процесі передачі частин конфіденційного повідомлення дуже спрощує розрахунок імовірності його компрометації в мережі за допомогою виразів (3.2)–(3.6).

3.3.2. Дослідження методу безпечної маршрутизації повідомлень шляхами, що не перетинаються

Розглянемо окремо задачу розподілу кількості частин повідомлення, що передається, між множиною маршрутів, які не перетинаються. Вона буде представлена як оптимізаційна у застосуванні виразів (3.1)–(3.6). Проведемо порівняльний аналіз її розв'язань з використанням чотирьох моделей з різними критеріями оптимальності отримуваних рішень [43, 44].

Першою моделлю (*Модель* 1) була раніше запропонована в роботах [29, 30] модель, що використовується в механізмі SPREAD і представлена виразами (3.1)–(3.6). Друга модель (*Модель* 2) (3.1)–(3.3), (3.5), (3.6), яка підлягає порівнянню, відрізнялася від першої тим, що критерієм оптимальності був мінімум цільової функції, представленої таким виразом:

$$J = \sum_{i=1}^{M} p_i n_i \,. \tag{3.7}$$

Використання критерію (3.7) дозволяє забезпечити такий порядок безпечної маршрутизації повідомлення в мережі, коли максимальна кількість його частин буде передаватися шляхом з мінімальною ймовірністю компрометації. І навпаки, шляхом з максимальною ймовірністю компрометації буде передаватися мінімальна кількість частин того самого повідомлення.

Модель 3 для забезпечення оптимального балансування кількості частин повідомлення множиною маршрутів передбачає введення додаткових умов:

$$n_i \le \beta \ \left(i = \overline{1, M}\right), \tag{3.8}$$

де β – верхній динамічно керований поріг кількості частин повідомлення, які передаються в мережі шляхами, що не перетинаються.

У цій же моделі критерієм оптимальності маршрутних рішень обрано мінімум такої цільової функції:

$$J = \beta + \sum_{i=1}^{M} p_i n_i \,. \tag{3.9}$$

Мінімізація виразу (3.9) має здійснюватися у виконанні умов (3.3) та (3.8), що дозволить забезпечити балансування кількості частин повідомлення, які передаються в кожному з обраних шляхів. Уведення в цільову функцію (3.9)

доданку $\sum_{i=1}^{M} p_i n_i$ спрямовано на досягнення такої мети: у випадку, якщо загальна кількість частин N не кратна кількості обраних шляхів M, то більша кількість фрагментів буде передаватися кращим з точки зору ймовірності компрометації маршрутом. Це є важливою перевагою запропонованого рішення від попередньо відомих [29, 30].

У свою чергу *Модель* 4 представлена умовами-обмеженнями (3.1)–(3.3), (3.6) у разі використання критерію оптимальності

$$J = \sum_{i=1}^{M} \left(p_i n_i \right)^2 . \qquad (3.10)$$

Особливості описаних моделей 1÷4 будуть продемонстровані на такому прикладі. Припустимо, що задано пару вузлів відправника й отримувача, між якими існують три доступні шляхи, що не перетинаються, з різною кількістю елементів: вузлів і каналів зв'язку між ними (рис. 3.4).

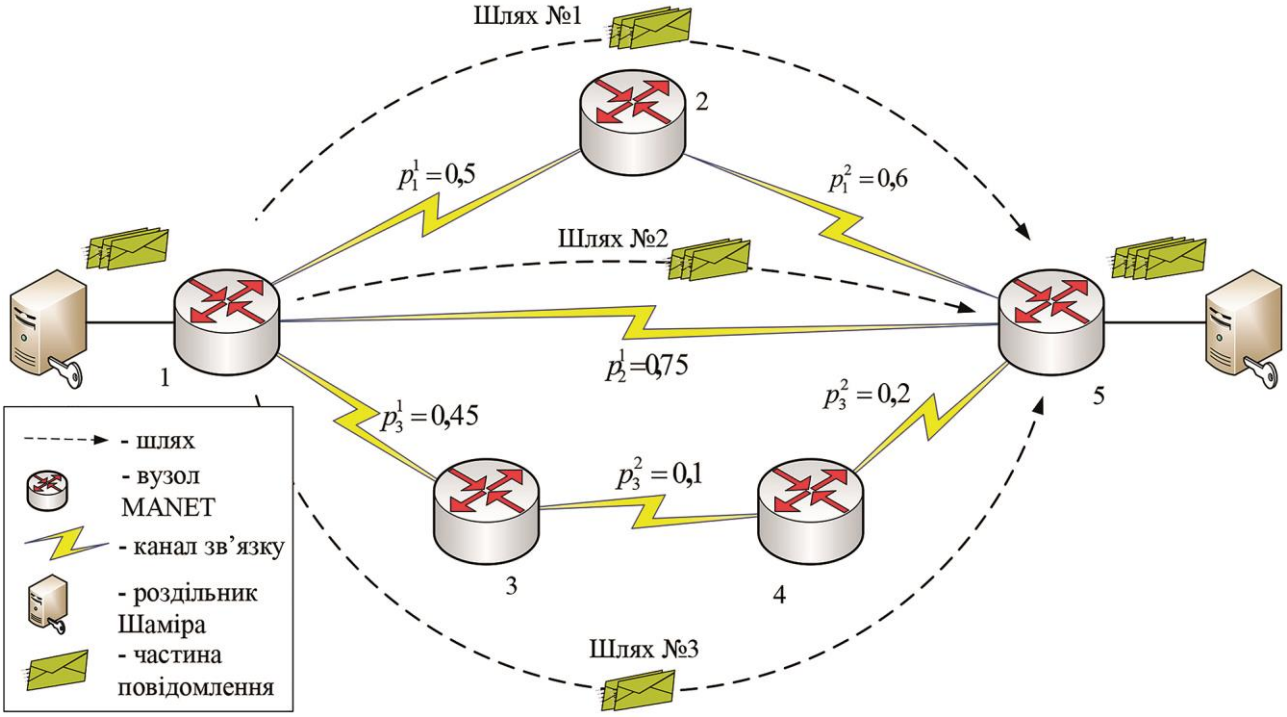


Рис. 3.4. Вихідна структура MANET

Нехай у цьому прикладі до компрометації схильні лише канали зв'язку, що є досить справедливим для MANET. У процесі розрахунків вихідними будуть такі дані:

– для розділення повідомлення на частини реалізується два випадки схеми Шаміра, а саме (10, 10) без надмірності та (8, 10) з надмірністю;

– імовірності компрометації каналів зв'язку відповідно до їх нумерації і належності до шляхів, що не перетинаються (рис. 3.4), приймають такі значення: $p_1^1 = 0,5$; $p_1^2 = 0,6$; $p_2^1 = 0,75$; $p_3^1 = 0,45$; $p_3^2 = 0,1$; $p_3^3 = 0,2$.

Тоді ймовірності компрометації шляхів, отримані в процесі використання виразу (3.2), такі: $p_1 = 0,8$, $p_2 = 0,75$, $p_3 = 0,604$. Крім того, у табл. 3.2 показано допустимі рішення задачі розподілу кількості частин шляхами, що не перетинаються, які були отримані під час використання раніше описаних чотирьох моделей.

Таблиця 3.2

Порівняння моделей розподілу кількості частин повідомлення між множиною маршрутів, що не перетинаються, з їх оптимальним балансуванням

Номер моделі	Кількість частин повідомлення в окремому шляху залежно від методу балансування			
	Модель 1	Модель 2	Модель 3	Модель 4
Номер шляху	Схема Шаміра без надмірності (10, 10)			
1	8	1	2	3
2	1	1	4	3
3	1	8	4	4
Номер шляху	Схема Шаміра з надмірністю (8, 10)			
1	4	1	2	3
2	3	1	4	3
3	3	8	4	4

Розглянемо випадок з використанням схеми Шаміра без надмірності, наприклад (10, 10). Аналіз результатів розрахунків та порівняння отриманих значень кількості частин повідомлення, які передавалися різними шляхами, показали, що всі чотири моделі можуть дати задовільні рішення. Це можна пояснюється тим, що для компрометації всього повідомлення всі три шляхи повинні бути скомпрометовані. Однак найкращі моделі – це *Моделі* 3 та 4, оскільки вони передбачають адаптацію до параметрів безпеки елементів мережі, коли максимальна кількість частин повідомлення передається найкращим шляхом за рівнем ймовірності компрометації (табл. 3.2).

У використанні *Моделі* 1 (табл. 3.2) одним з можливих рішень розподілу частин повідомлення за шляхами є рішення, коли максимальна кількість фрагментів $(n_1 = 8)$ буде передаватися найгіршим шляхом з точки зору ймовірності компрометації $(p_1 = 0,8)$, що є недоліком цієї моделі (рис. 3.5).

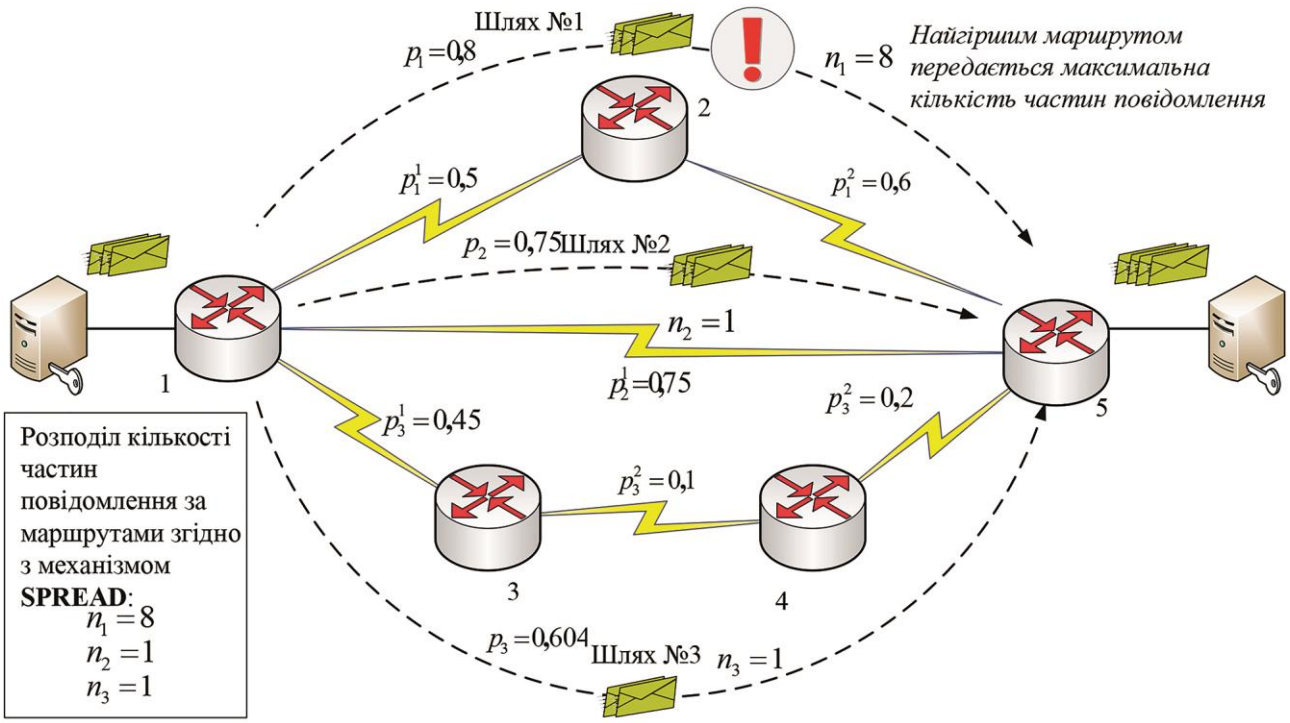


Рис. 3.5. Розподіл кількості частин повідомлення за маршрутами згідно з механізмом SPREAD (*Модель* 1)

Відповідно до *Моделі* 2 за допомогою схеми Шаміра (10, 10) розподіл частин повідомлення за шляхами мережі показав, що максимальна кількість фрагментів $(n_3 = 8)$ передавалася найкращим з точки зору ймовірності компрометації шляхом $(p_3 = 0,604)$, а їх мінімальна кількість $(n_1 = 1)$ передавалася найгіршим шляхом $(p_1 = 0,8)$.

Розглянемо приклад використання схеми Шаміра з надмірністю, наприклад, (8, 10). Найкращі рішення були надані *Моделями* 1 і 4, оскільки для компрометації всього повідомлення всі три шляхи мали бути скомпрометовані. Хоча у *Моделі* 2 зловмисник повинен скомпрометувати лише один шлях для реконструкції повідомлення, що передається $(n_3 = 8,\ T = 8)$, тоді як у *Моделі* 3 треба скомпрометувати два шляхи $(n_2 = 4,\ n_3 = 4,\ T = 8)$.

Модель 1 у цьому випадку забезпечує досить ефективне рішення з точки зору оптимального розподілу частин повідомлення (табл. 3.2). *Модель* 4 на основі умов обмежень (3.1)–(3.3), (3.6) та критерію оптимальності (3.10) дає найкраще рішення (рис. 3.6) порівняно з усіма іншими моделями. Використовуючи цю модель, можна забезпечити, з одного боку, оптимальне балансування частин повідомлення, переданих через окремі шляхи в мережі, що не перетинаються, а з іншого, – адаптацію до параметрів безпеки

(імовірності компрометації) окремих елементів мережі: каналів зв'язку та маршрутів загалом. У цьому випадку мінімальна кількість фрагментів $(n_1 = 3)$ передається найгіршим шляхом з точки зору ймовірності компромісу, а їх максимальна кількість $(n_3 = 4)$ передається найкращим шляхом (табл. 3.2).

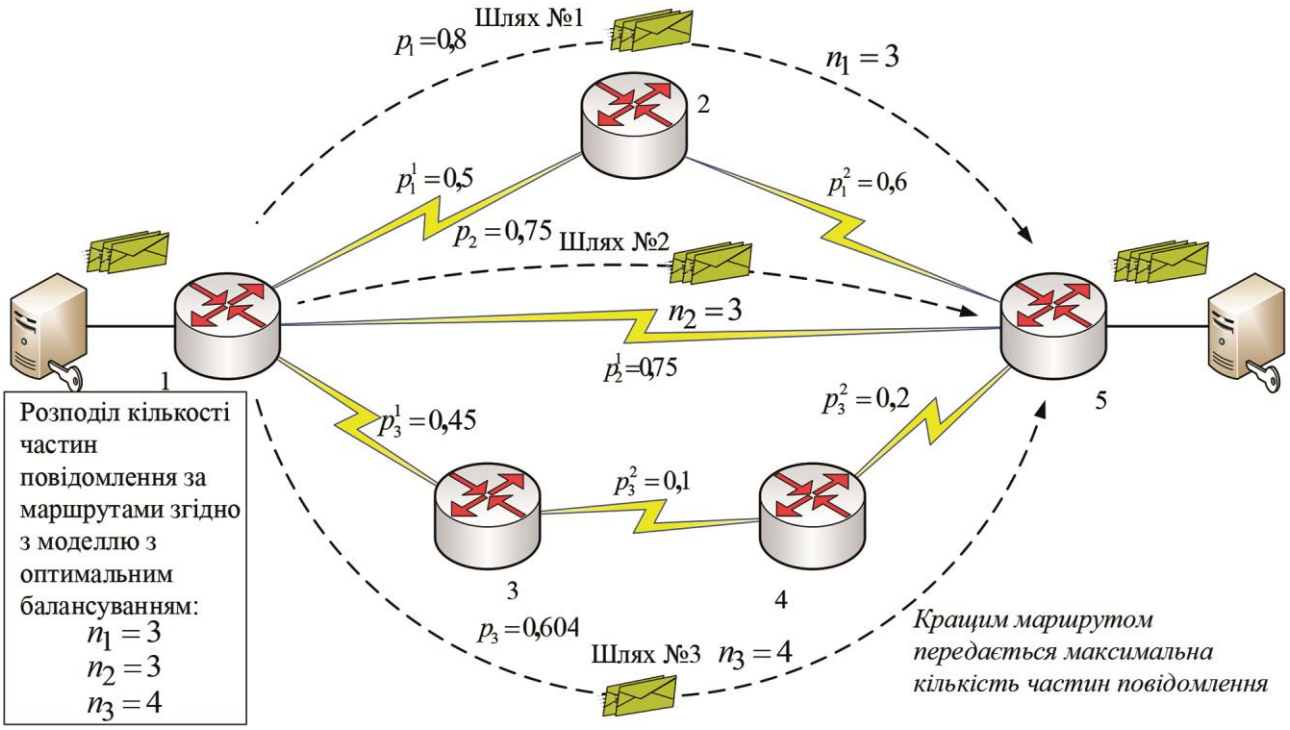


Рис. 3.6. Розподіл кількості частин повідомлення за маршрутами згідно з *Моделлю* 4

Таким чином, реалізація *Моделі* 4 передбачає метод безпечної багатошляхової маршрутизації з оптимальним балансуванням частин повідомлення в MANET, який містить такі етапи:

1. Аналіз архітектури MANET (кількість елементів мережі, вимоги щодо якості обслуговування та безпеки, сигнально-завадова обстановка тощо).

2. Розрахунок множини шляхів, що не перетинаються, між заданими вузлами відправника та отримувача відповідно до умови (3.1).

3. Фрагментація повідомлення, що передається, за обраною схемою Шаміра з надлишковістю або без надлишковості.

4. Оптимальний розподіл частин повідомлення за множиною шляхів, що не перетинаються, на основі моделі, яка містить вирази (3.1)–(3.3), (3.6) та критерій оптимальності (3.10).

3.4. Метод безпечної маршрутизації повідомлень шляхами, що перетинаються: проактивний підхід

У розглянутих у підрозділі 3.3 рішеннях щодо безпечної маршрутизації, зокрема в механізмі SPREAD, виконання умови (3.1) цілком і повністю визначається параметрами використовуваних шляхів, що не перетинаються, а завдання балансування частин повідомлення цими шляхами полягає у виконанні умов (3.3)–(3.5). Тому якщо використання множини шляхів, які не перетинаються, не дозволяє задовольнити вимогу (3.1), то поставлене завдання щодо забезпечення заданого рівня мережної безпеки залишається невирішеним.

У цьому випадку інтуїтивно можна припустити, що використання на тій же мережній топології шляхів, які перетинаються, могло б сприяти поліпшенню шуканої ймовірності компрометації переданого повідомлення і, як наслідок, до успішного вирішення поставленого завдання. Як показав проведений аналіз, у разі використання шляхів, що перетинаються, процедура числової оцінки ймовірності компрометації повідомлення, яке передається, помітно ускладнюється, а в низці випадків стає неможливою (в аналітичному вигляді) [30]. У зв'язку з цим актуальним є завдання пошуку компромісного рішення, пов'язаного з визначенням такого класу маршрутів, що перетинаються, для яких можливо в аналітичному вигляді розрахувати, а отже, і контролювати ймовірність компрометації конфіденційного повідомлення, яке передається.

У цьому підрозділі зроблено спробу розширення класу шляхів, що перетинаються, у використанні яких усе ще можливо здійснити аналітичну оцінку ймовірності компрометації повідомлення, яке передається. Це дозволить створити умови для контролю за виконанням вимог щодо рівня мережної безпеки (3.1) в умовах використання шляхів, які перетинаються [45–48].

У цьому контексті необхідно додатково ввести ще два типи шляхів: простий і композитний. Простий шлях завжди утворений послідовним з'єднанням каналів зв'язку мережі, а ймовірність його компрометації розраховується за допомогою формули (3.2). У свою чергу композитні шляхи є більш складними структурними формами, що містять перетин простих шляхів. У зв'язку з цим уточнимо раніше введені та введемо додаткові позначення [47]:

Константи

$\tilde{M}$ кількість використовуваних композитних шляхів, що не перетинаються, які можуть використовуватися в процесі маршрутизації частин повідомлення;

$\tilde{M}_i$ кількість фрагментів в i-му композитному шляху, які можуть бути скомпрометовані $\left(i=\overline{1,\tilde{M}}\right)$;

M_i кількість каналів зв'язку в i-му композитному шляху, які можуть бути скомпрометовані $\left(i=\overline{1,\tilde{M}}\right)$;

p_i^j імовірність компрометації j-го каналу зв'язку i-го композитного шляху $\left(i=\overline{1,\tilde{M}},\ j=\overline{1,M_i}\right)$.

Кількісні показники

$\tilde{p}_i^j$ імовірність компрометації j-го фрагмента i-го композитного шляху $\left(i=\overline{1,\tilde{M}},\ j=\overline{1,\tilde{M}_i}\right)$;

$\tilde{p}_i$ імовірність компрометації i-го композитного шляху $\left(i=\overline{1,\tilde{M}}\right)$;

$\tilde{P}_{msg}$ імовірність компрометації повідомлення загалом за умови його передачі частинами за композитними шляхами.

Змінні

n_i цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним шляхом $\left(i=\overline{1,\tilde{M}}\right)$.

Для того щоб забезпечувалася можливість формулювання в аналітичному вигляді виразу для розрахунку ймовірності компрометації композитного шляху в процесі безпечної маршрутизації, він повинен містити два типи фрагментів, що складаються з послідовного (рис. 3.7, а) або з паралельного з'єднання каналів зв'язку (рис. 3.7, б). На рис. 3.7, в наведено приклад композитного шляху з послідовним з'єднанням двох фрагментів мережі. Перший фрагмент представлений паралельним з'єднанням каналів зв'язку, а другий – послідовним.

На рис. 3.7, в показано структуру мережі, яка містить один композитний шлях, що складається з каналів двох простих шляхів, які перетинаються між собою. Перший простий шлях представлений вузлами 1→2→3→4, а другий – 1→3→4. З іншого боку, цей композитний шлях містить два послідовно з'єднаних фрагменти. Перший фрагмент складається з паралельно з'єднаних каналів зв'язку 1→3 та послідовності каналів 1→2 та 2→3. Тоді як другий фрагмент представлений каналом зв'язку 3→4.

Тоді ймовірність компрометації композитного шляху (рис. 3.7, в) розраховується відповідно до виразу

$$\tilde{p}_1 = 1 - \left(1 - \tilde{p}_1^1\right)\left(1 - \tilde{p}_1^2\right). \qquad (3.11)$$

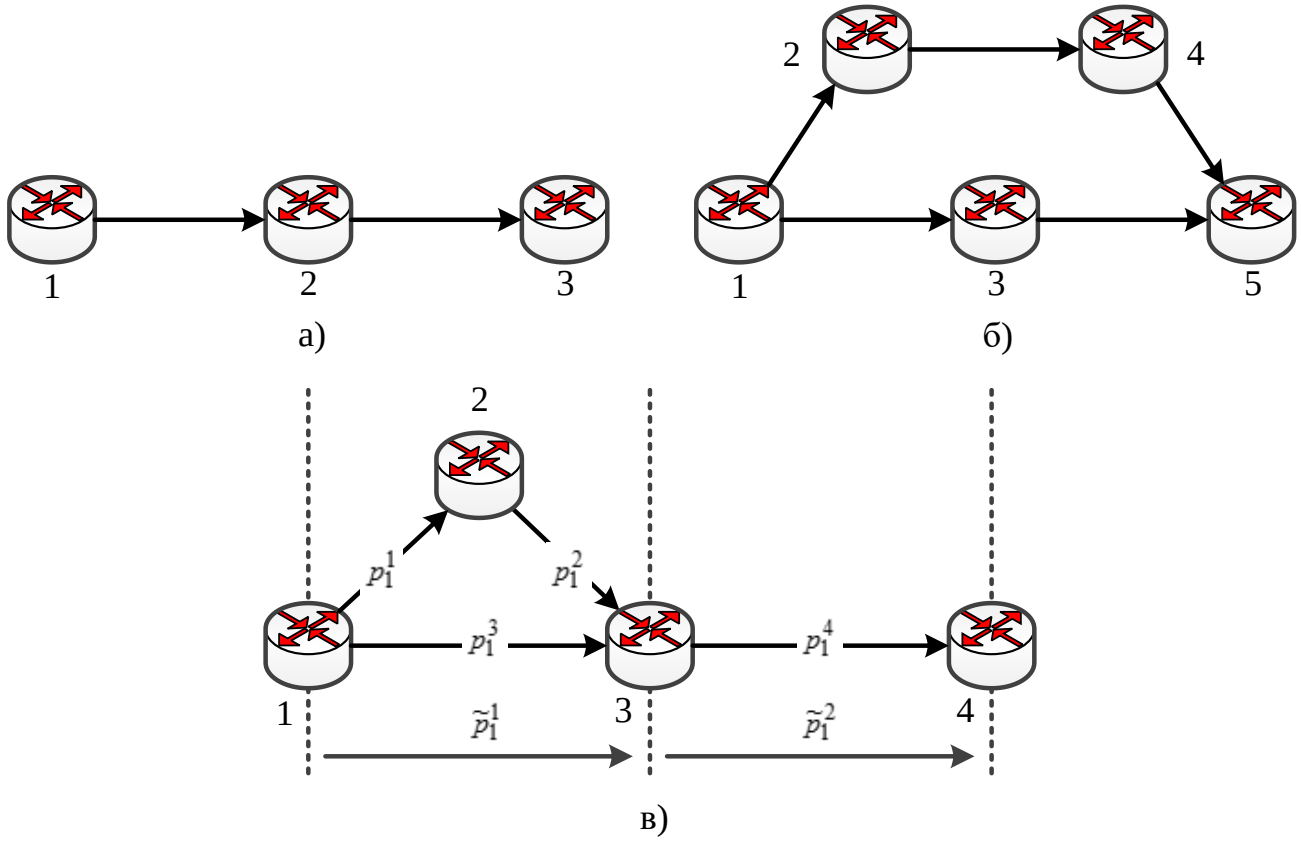


Рис. 3.7. Приклади типів фрагментів і композитного шляху:
а – послідовне з'єднання каналів зв'язку;
б – паралельне з'єднання каналів зв'язку; в – композитний шлях

У виразі (3.11) імовірності компрометації першого та другого фрагментів визначаються через імовірності компрометації каналів зв'язку, які вони містять:

$$\tilde{p}_1^1 = \left[1 - \left(1 - p_1^1\right)\left(1 - p_1^2\right)\right] p_1^3, \; \tilde{p}_1^2 = p_1^4.$$

Отже, у загальному випадку ймовірність компрометації i-го композитного шляху, що складається з $\tilde{M}_i$ фрагментів, може бути розрахована відповідно до такого виразу [47]:

$$\tilde{p}_i = 1 - \prod_{j=1}^{\tilde{M}_i} \left(1 - \tilde{p}_i^j\right). \qquad (3.12)$$

Якщо для доставки повідомлення використовується єдиний композитний шлях, то ймовірність компрометації цього повідомлення визначається

ймовірністю компрометації цього композитного шляху. У більш загальному випадку, коли частини повідомлення передаються за множиною композитних шляхів, що не перетинаються, для розрахунку ймовірності компрометації повідомлення необхідно використовувати такий вираз [47]:

$$\tilde{P}_{msg} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i \,, \tag{3.13}$$

який є модифікацією формули (3.6).

Приклад подібного випадку показано на рис. 3.8, коли для передачі частин повідомлення використовуються два шляхи, що не перетинаються:

– перший шлях є композитним і складається з таких каналів зв'язку 1→2, 2→3, 2→4, 3→5, 4→5, 5→7;

– другий шлях є простим і містить канали зв'язку 1→6 і 6→7.

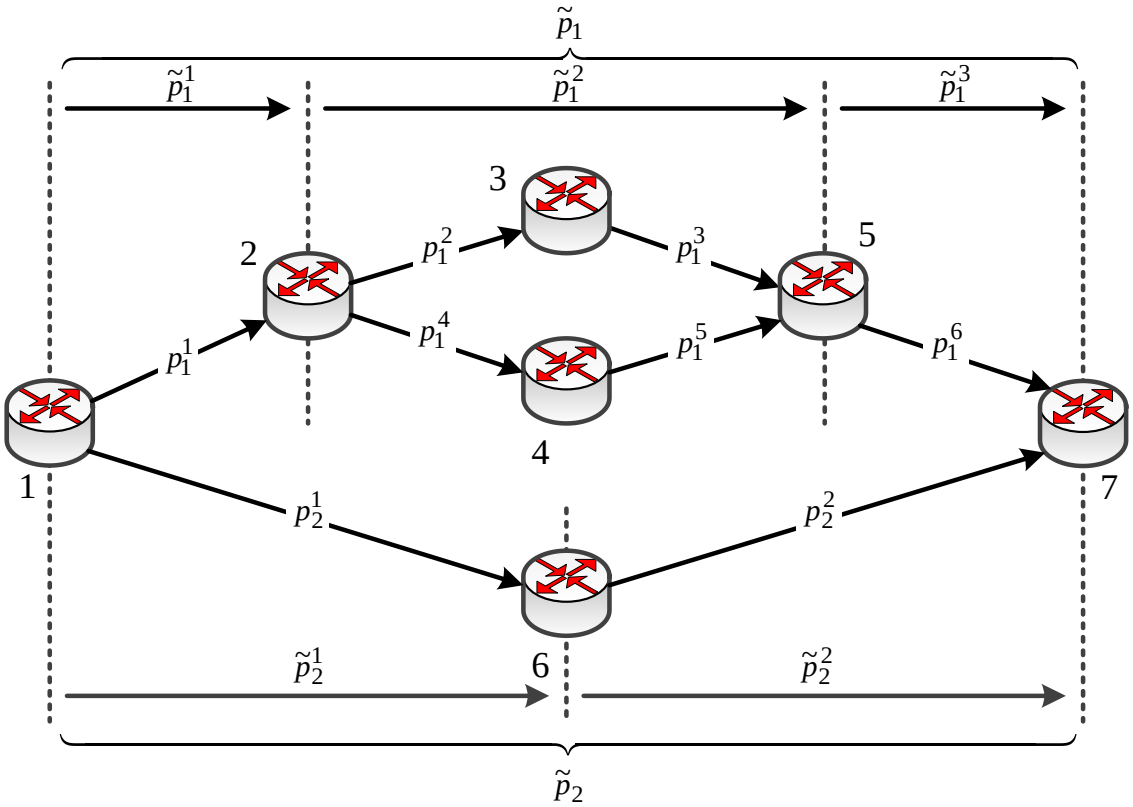


Рис. 3.8. Приклад використання двох шляхів: композитного та простого

У свою чергу перший (композитний) шлях складається з трьох послідовно з'єднаних мережних фрагментів:

– перший фрагмент представлений каналом зв'язку 1→2;

– другий фрагмент оснований на паралельному з'єднанні таких каналів зв'язку: 2→3, 3→5 і 2→4, 4→5;

– третій фрагмент представлений каналом зв'язку 5→7.

Тоді для цієї мережної структури (рис. 3.8) імовірність компрометації повідомлення у використанні двох різнотипних описаних вище шляхів буде визначатися таким чином:

$$P_{msg} = \tilde{p}_1 \cdot \tilde{p}_2 . \tag{3.14}$$

У виразі (3.14) імовірності компрометації композитного та простого шляхів (першого та другого відповідно) виражаються через імовірності компрометації їх фрагментів і каналів зв'язку як

$$\tilde{p}_1 = 1 - \left(1 - \tilde{p}_1^1\right)\left(1 - \tilde{p}_1^2\right)\left(1 - \tilde{p}_1^3\right) =$$

$$= 1 - \left(1 - p_1^1\right)\left(1 - \left[1 - \left(1 - p_1^2\right)\left(1 - p_1^3\right)\right] \times \left[1 - \left(1 - p_1^4\right)\left(1 - p_1^5\right)\right]\right)\left(1 - p_1^6\right); \tag{3.15}$$

$$\tilde{p}_2 = 1 - \left(1 - \tilde{p}_2^1\right)\left(1 - \tilde{p}_2^2\right) = 1 - \left(1 - p_2^1\right)\left(1 - p_2^2\right). \tag{3.16}$$

У загальному випадку один композитний шлях може містити кілька послідовно з'єднаних фрагментів з паралельним з'єднанням каналів зв'язку. Позначимо через h_i максимальну кількість паралельно з'єднаних каналів зв'язку за всіма фрагментами i-го композитного шляху. Тоді умова (3.5) набуде вигляду [47]

$$h_i \le n_i \le T - 1, \ \left(i = \overline{1, \tilde{M}}\right), \tag{3.17}$$

а її виконання дозволить таким чином розподілити частини повідомлення за паралельно з'єднаними каналами мережних фрагментів композитних шляхів, щоб у кожному з них передавалося ненульове число таких частин повідомлення та були справедливі вирази (3.12) і (3.13).

Крім того, умова (3.4) з урахуванням композитного характеру використовуваних шляхів набуде вигляду

$$N - n_i < T, \ \left(i = \overline{1, \tilde{M}}\right). \tag{3.18}$$

У зв'язку з цим в основу запропонованого методу безпечної маршрутизації частин повідомлення, яке передається за множиною шляхів, що перетинаються, може бути покладено розв'язання оптимізаційної задачі, пов'язаної з використанням критерію оптимальності

$$\min_{n_i} \prod_{i=1}^{\tilde{M}} \tilde{p}_i\left(n_i\right), \tag{3.19}$$

що гарантує мінімізацію ймовірності компрометації переданого повідомлення [47]. Крім того, на керуючі змінні залежно від використовуваної схеми Шаміра накладаються обмеження (3.12), (3.17) або (3.18), а також аналог умови (3.3), представлений рівністю

$$\sum_{i=1}^{\tilde{M}} n_i = N . \tag{3.20}$$

Сформульована оптимізаційна задача належить до класу задач нелінійного цілочисельного програмування (Nonlinear Integer Programming), тому що змінні, які підлягають розрахунку, є цілочисельними, а критерій оптимальності (3.19) є нелінійним.

Запропонований метод безпечної маршрутизації повідомлень за множиною шляхів, які перетинаються, є засобом проактивного підходу щодо поліпшення рівня мережної безпеки. Це визначається тим, що на основі постійного аналізу стану мережі, її структури та параметрів безпеки каналів зв'язку, а також у процесі оптимального балансування частин конфіденційних повідомлень шляхами, які перетинаються, реалізуються всі доступні можливості для того, щоб максимально знизити ймовірність компрометації даних, які передаються.

3.5. Аналіз запропонованого методу безпечної маршрутизації повідомлень шляхами, що перетинаються

3.5.1. Дослідження методу безпечної маршрутизації повідомлень шляхами, що перетинаються, у разі використання єдиного композитного шляху

Під час дослідження запропонованого методу буде проведено аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих каналів зв'язку та фрагментів мережі. Крім того, оцінимо виграш за ймовірністю компрометації, отримуваний за умови використання запропонованого в підрозділі 3.4 методу, порівняно з раніше відомим, описаним у пункті 3.3.1. Особливості розрахунку ймовірності компрометації повідомлення будуть продемонстровані на мережній структурі, показаній на рис. 3.7, в. Вихідними даними були значення, представлені в табл. 3.3. В останньому рядку табл. 3.3 наведено результат розв'язання поставленої оптимізаційної задачі, пов'язаної з мінімізацією виразу (3.19) у разі обмежень (3.12), (3.17), (3.20) у процесі реалізації схеми Шаміра (10, 10) та $h_1 = 2$.

Таблиця 3.3

Вихідні дані для дослідження
в разі використання єдиного композитного шляху

Канал зв'язку	1→2	2→3	1→3	3→4
№ каналу зв'язку в шляху	1	2	3	4
Імовірність компрометації каналу зв'язку	0,1	0,2	0÷1	0÷1
Кількість частин повідомлення	5	5	5	10

У процесі передачі повідомлення від першого до четвертого вузла його частини прямували за двома маршрутами, що перетинаються: 1→2→3→4 і

1→3→4, тобто канал 3→4 в них був спільним. У дослідженні передбачалося, що ймовірності компрометації першого та другого каналів були фіксованими та становили 0,1 і 0,2 відповідно, а ймовірності компрометації третього та четвертого каналів змінювалися в межах від 0 до 1.

Розрахунок імовірності компрометації проводився для двох випадків:

– у першому випадку для розрахунку ймовірності компрометації повідомлень $\left(\tilde{P}_{msg}\right)$ використовувався підхід, описаний у підрозділі 3.4 і оснований на виразах (3.11)–(3.13), (3.18);

– у другому випадку в розрахунках застосовувався підхід (3.2)–(3.6), викладений у пункті 3.3.1, який передбачає використання лише шляхів, що не перетинаються. Щодо рис. 3.7, в це передбачає використання або шляху 1→3→4, якому відповідала ймовірність компрометації P_{msg}^1, або шляху 1→2→3→4, компрометація якого оцінювалася ймовірністю P_{msg}^2.

Тоді на рис. 3.9 показано характер залежності ймовірності компрометації повідомлення, переданого шляхами різних типів для мережної структури, наведеної на рис. 3.7, в, від значень імовірності компрометації четвертого каналу p_1^4 (відкладені по осі абсцис).

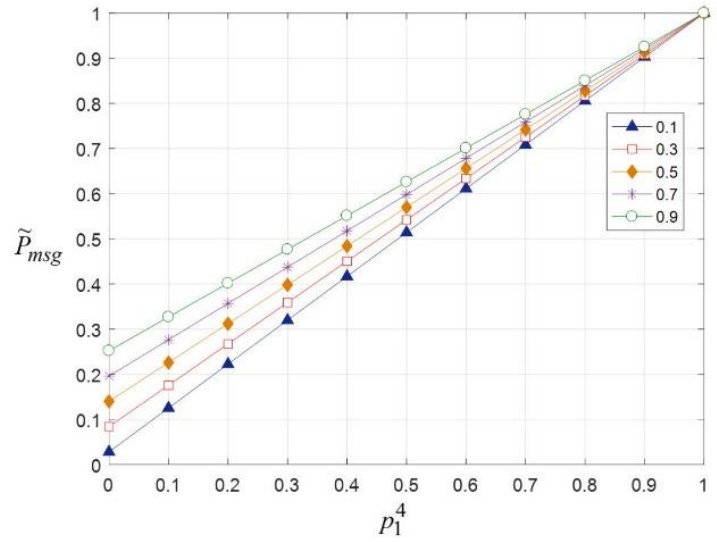
Кожній з множини прямих відповідало своє значення ймовірності компрометації третього каналу $\left(p_1^3\right)$. Як показано на рис. 3.9, зі зростанням p_1^3 та p_1^4 ймовірність компрометації повідомлення, що передається за умови використання композитного шляху та простого шляху 1→3→4, завжди зростала, але характер залежності в разі використання шляхів різних типів (що перетинаються та не перетинаються) істотно відрізнявся. З огляду на те, що простий шлях 1→2→3→4 не містив третій канал (рис. 3.7, в), то ймовірність його компрометації залежала лише від p_1^4 і не залежала від p_1^3 (рис. 3.9, в).

Для кількісної оцінки виграшу за ймовірністю компрометації повідомлень від застосування запропонованого методу, основаного на використанні шляхів, що перетинаються, порівняно з раніше відомими рішеннями використовувалися вирази:

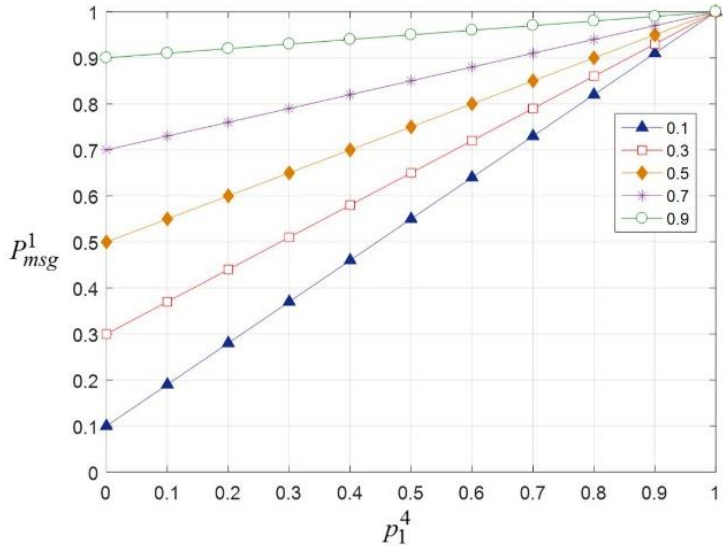
$$\Delta_1 = \frac{P_{msg}^1 - \tilde{P}_{msg}}{P_{msg}^1} \cdot 100\%, \tag{3.21}$$

а також

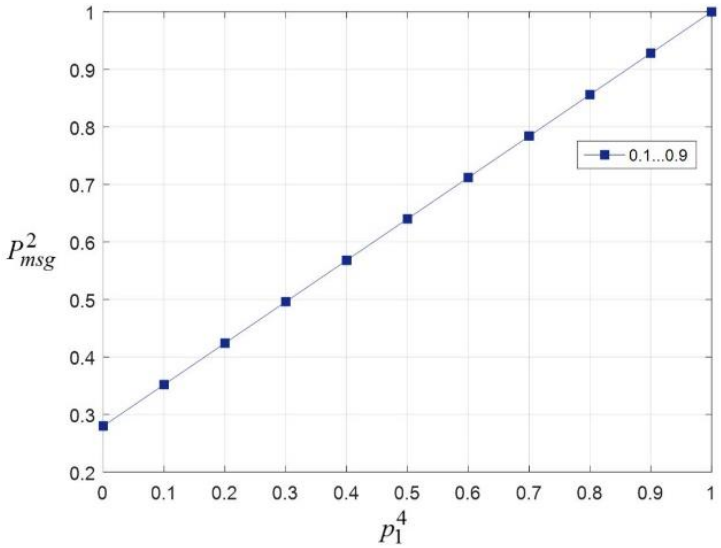
$$\Delta_2 = \frac{P_{msg}^2 - \tilde{P}_{msg}}{P_{msg}^2} \cdot 100\%. \tag{3.22}$$



а)



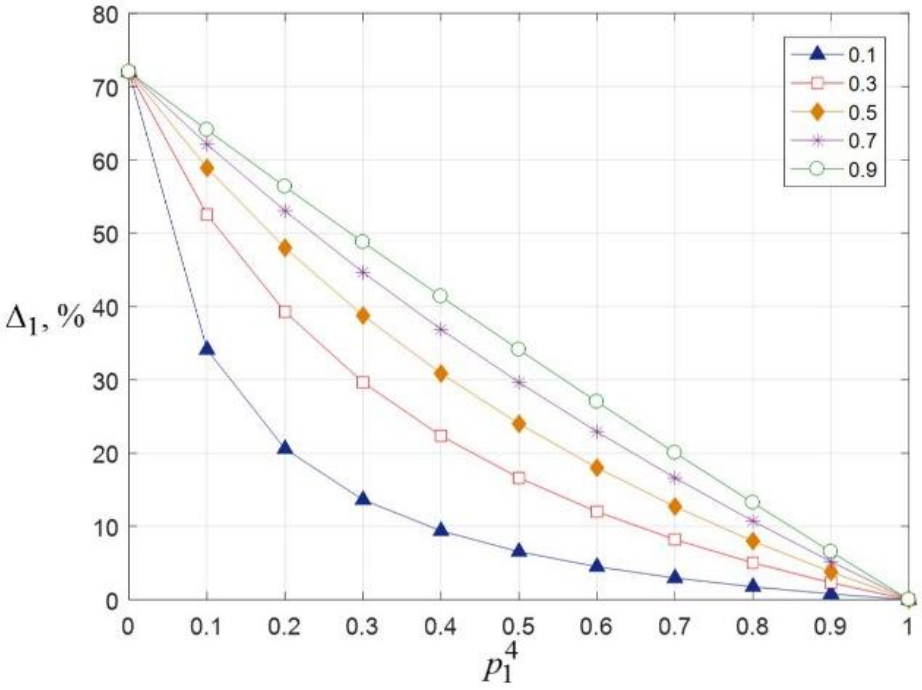
б)



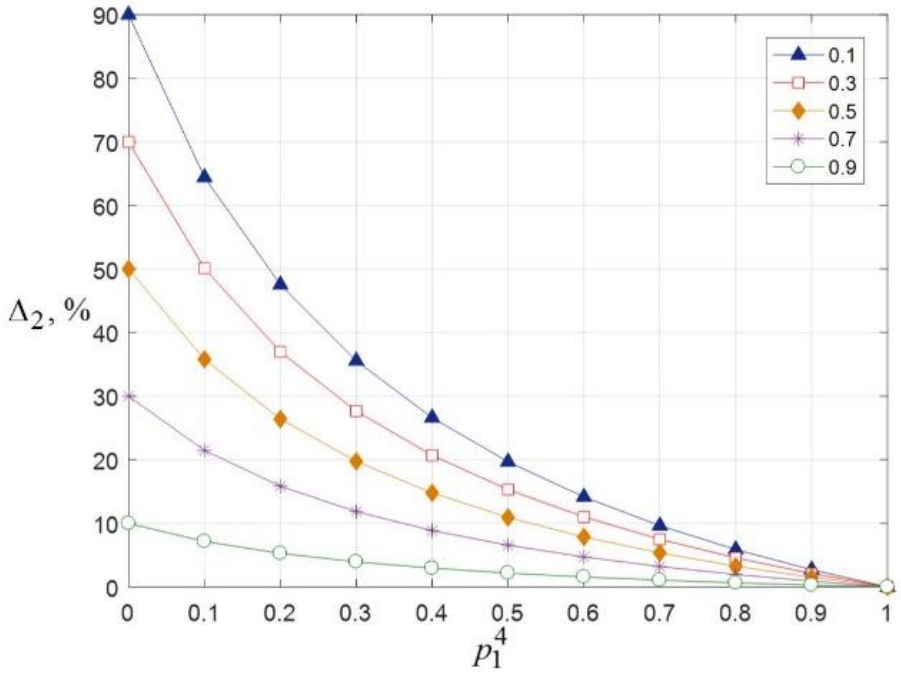
в)

Рис. 3.9. Залежність імовірності компрометації повідомлення, яке передається шляхами різних типів для мережної структури, наведеної на рис. 3.7, в

Відповідно до цих виразів отримані графіки, зображені на рис. 3.10. За результатами, представленими на рис. 3.10, можна зробити висновок, що використання запропонованого методу безпечної маршрутизації частин повідомлення двома простими шляхами, які перетинаються, об'єднаних в єдиний композитний шлях, сприяло поліпшенню рівня мережної безпеки.



а)



б)

Рис. 3.10. Залежність виграшу за ймовірністю компрометації від використання запропонованого методу порівняно з раніше відомими рішеннями для мережної структури, наведеної на рис. 3.7, в

У цьому випадку вдалося знизити ймовірність компрометації повідомлення:

– порівняно з використанням одного простого шляху $1\to3\to4$ в середньому на 20–55 %, якщо $p_1^4 = 0{,}1 \div 0{,}3$ та на 5–20 % за умови $p_1^4 = 0{,}5 \div 0{,}9$ (рис. 3.10, а);

– порівняно з використанням одного простого шляху $1\to2\to3\to4$ в середньому на 5–50 % у разі $p_1^4 = 0{,}1 \div 0{,}3$ та на 3–15 %, якщо $p_1^4 = 0{,}5 \div 0{,}9$ (рис. 3.10, б).

Виграш за ймовірністю компрометації повідомлення, що передається, знижувався, якщо $p_1^4 \to 1$, оскільки будь-який з розглянутих маршрутів, і простий, і композитний, проходили через цей канал.

3.5.2. Дослідження методу безпечної маршрутизації повідомлень у разі використання двох різнотипних шляхів, що не перетинаються

Аналогічно проведемо порівняльний аналіз ефективності запропонованого методу (див. підрозділ 3.4) та раніше відомих рішень (див. пункт 3.3.1) для структури мережі, представленої на рис. 3.8. За допомогою запропонованого в підрозділі 3.4 методу оцінювалася ймовірність компрометації повідомлення $\left(\tilde{P}_{msg}\right)$, яке передається з використанням усіх доступних каналів зв'язку, що містяться в одному композитному й одному простому шляху.

З використанням раніше відомого методу (3.2)–(3.6) оцінювалася ймовірність компрометації повідомлення, частини якого передавалися з використанням двох простих шляхів, які не перетинаються. Зокрема розглядалися два можливі випадки комбінації вибору таких шляхів. У першому випадку використовувалися шляхи $1\to2\to4\to5\to7$ та $1\to6\to7$, якому відповідала ймовірність компрометації повідомлення P_{msg}^1. У другому випадку частини повідомлення передавалися іншою парою шляхів, що не перетинаються: $1\to2\to3\to5\to7$ та $1\to6\to7$. Цьому рішенню відповідало значення ймовірності компрометації P_{msg}^2.

Показником ефективності безпечної маршрутизації знову була ймовірність компрометації повідомлень, які передаються, а в процесі досліджень аналізувався вплив на неї ймовірностей компрометації, наприклад,

каналів 2→4 та 1→6, які змінювалися від 0 до 1. Канал 2→4 розміщувався у композитному шляху під четвертим номером, а канал 1→6 мав перший номер у структурі простого шляху (табл. 3.4).

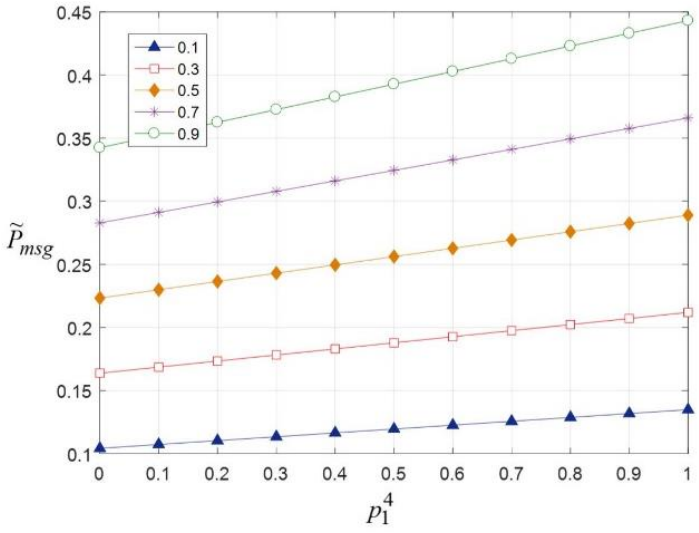
Таблиця 3.4

Вихідні дані для дослідження випадку використання двох різнотипних шляхів, що не перетинаються

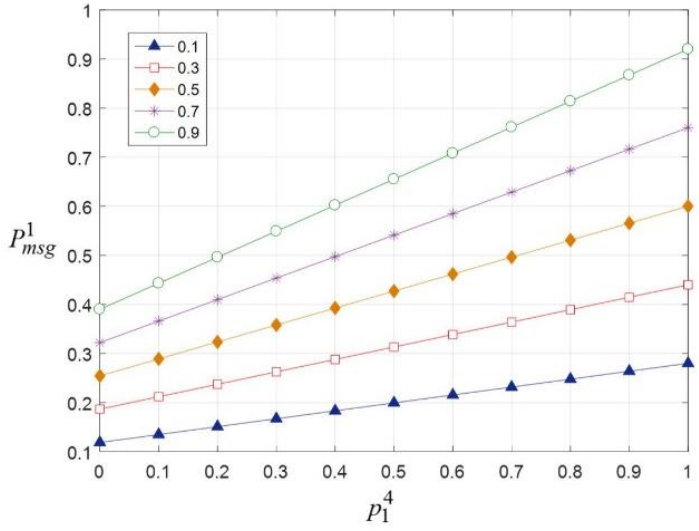
Номер шляху	1 (композитний)						2 (простий)	
Канал зв'язку	1→2	2→3	3→5	2→4	4→5	5→7	1→6	6→7
№ каналу зв'язку в шляху	1	2	3	4	5	6	1	2
Імовірність компрометації каналу зв'язку	0,2	0,1	0,1	0÷1	0,1	0,2	0÷1	0,2
Кількість частин повідомлення	5	3	3	2	2	5	5	5

У табл. 3.4 також наведені значення ймовірностей компрометації всіх каналів, що містяться в цих двох шляхах. Останнім рядком у табл. 3.4 вказано результат розв'язання оптимізаційної задачі, пов'язаної з мінімізацією (3.19) за умови обмежень (3.12), (3.17) або (3.18), (3.20) у разі реалізації схеми Шаміра (10, 10) та $h_1 = 2$, $h_2 = 1$. Першим (композитним) шляхом і другим (простим) шляхами передавалося по 5 частин вихідного повідомлення, тобто $n_1 = n_2 = 5$.

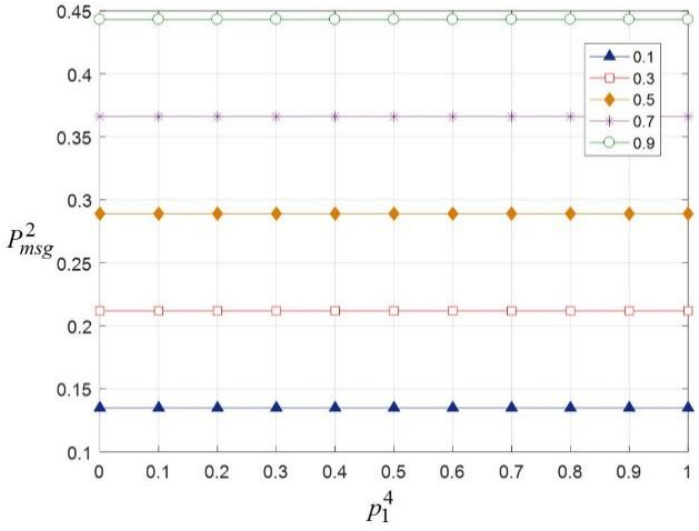
На рис. 3.11 показано залежність імовірності компрометації повідомлення, яке передається шляхами різних типів для структури, наведеної на рис. 3.8, від значень імовірності компрометації четвертого каналу композитного шляху (відкладені по осі абсцис). Кожній з множини прямих на рис. 3.11 відповідало своє значення ймовірності компрометації першого каналу простого шляху $\left(p_2^1\right)$. Як показано на рис. 3.11, а та б, зі зростанням p_2^1 та p_1^4 імовірність компрометації повідомлення, яке передається у разі використання композитного шляху та простого шляху 1→2→4→5→7 завжди зростала. З огляду на те, що прості шляхи 1→2→3→5→7 і 1→6→7, не містили канал 2→4 (рис. 3.8), то ймовірність їх компрометації залежала лише від p_2^1 і не залежала від p_1^4 (рис. 3.11, в).



а)



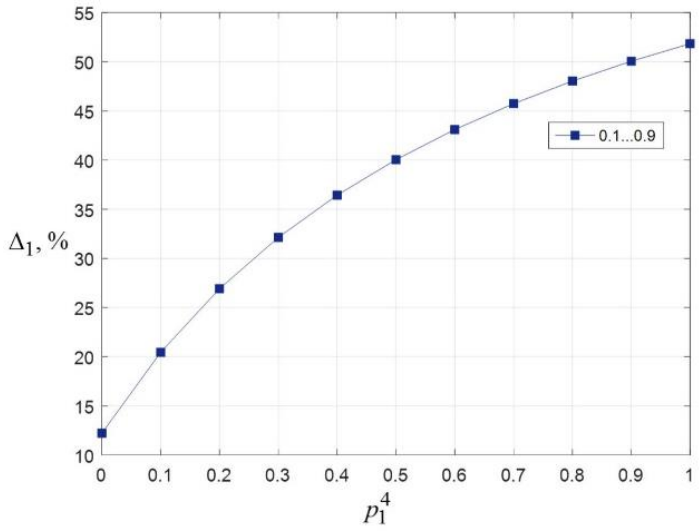
б)



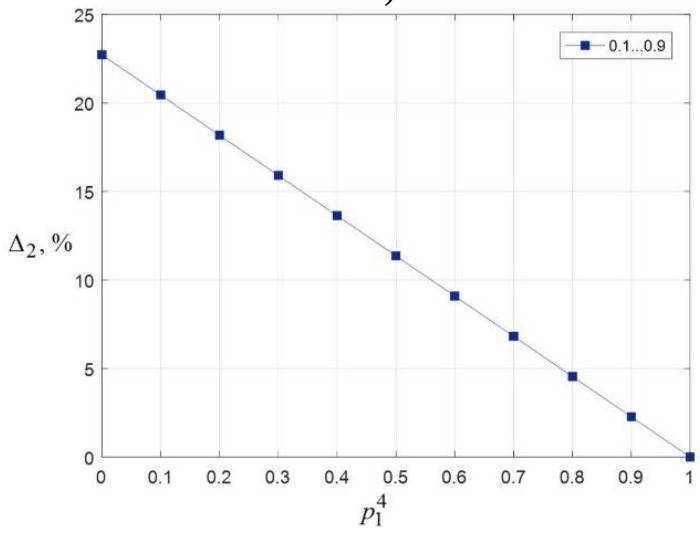
в)

Рис. 3.11. Залежність імовірності компрометації повідомлення, яке передається шляхами різних типів, для мережної структури, наведеної на рис. 3.8

Проведено кількісний аналіз виграшу за ймовірністю компрометації повідомлень (рис. 3.12) від використання запропонованого методу, основаного на використанні шляхів, що перетинаються, порівняно з раніше відомими рішеннями з використанням виразів (3.21) і (3.22). Як показано на рис. 3.12, аналізований за формулами (3.21) і (3.22) виграш за ймовірністю компрометації повідомлення, яке передається за шляхами різних типів, залежить лише від параметрів безпеки каналів, що містяться в композитному шляху. У цьому випадку це канал зв'язку $2\to4$, який є четвертим каналом першого (композитного) шляху з імовірністю компрометації p_1^4. Від значень імовірності компрометації каналу $1\to6$ $\left(p_2^1=0{,}1\div0{,}9\right)$, який є першим каналом другого (простого) шляху, виграш (3.21) і (3.22) не залежав (рис. 3.12).



а)



б)

Рис. 3.12. Залежність виграшу за ймовірністю компрометації від використання запропонованого методу порівняно з раніше відомими рішеннями для мережної структури, наведеної на рис. 3.8

За результатами, представленими на рис. 3.12, також можна зробити висновок, що використання запропонованого методу безпечної маршрутизації призвело до зниження ймовірності компрометації повідомлення, яке передається:

– порівняно із застосуванням двох простих шляхів $1\to2\to4\to5\to7$ і $1\to6\to7$, що не перетинаються, у середньому на 20–33 %, якщо $p_1^4 = 0{,}1 \div 0{,}3$, і на 40–50 % у разі $p_1^4 = 0{,}5 \div 0{,}9$ (рис. 3.12, а);

– порівняно з використанням двох простих шляхів $1\to2\to3\to5\to7$ і $1\to6\to7$, що не перетинаються, у середньому на 16–20 % за умови $p_1^4 = 0{,}1 \div 0{,}3$ і на 3–12 %, якщо $p_1^4 = 0{,}5 \div 0{,}9$ (рис. 3.12, б).

Таким чином, у процесі зростання ймовірності компрометації каналу, що міститься в композитному шляху, тобто якщо $p_1^4 \to 1$, виграш за ймовірністю компрометації повідомлення, яке передається, підвищувався порівняно з використанням простих шляхів, що містять той самий канал (рис. 3.12, а).

Якщо $p_1^4 = 1$, весь простий шлях $1\to2\to4\to5\to7$ буде скомпрометований, а використання композитного шляху, що містить мережний фрагмент з паралельним з'єднанням каналів, дозволяє цього уникнути.

З іншого боку, якщо канал $2\to4$ був скомпрометований, тобто $p_1^4 = 1$, то композитний шлях фактично втрачав свою перевагу, перетворюючись де-факто в простий шлях $1\to2\to3\to5\to7$. Це і призводило до зниження виграшу за ймовірністю компрометації повідомлення від застосування запропонованого методу порівняно з методом безпечної маршрутизації шляхами, що не перетинаються (рис. 3.12, б).

3.6. Метод безпечної швидкої перемаршрутизації повідомлень композитними шляхами: проактивний і реактивний підходи

З метою розширення функціональних можливостей засобів безпечної маршрутизації важливо, щоб запропонований метод реалізував принципи не тільки проактивного, але й реактивного підходу. Іншими словами, у структурі методу безпечної маршрутизації важливо передбачити процедури оперативної реакції на можливі порушення рівня мережної безпеки. У цей час протоколи маршрутизації реагують на можливі зміни стану мережі в масштабі часу десятків секунд, що не є прийнятним з точки зору необхідного рівня мережної безпеки.

У зв’язку з цим усе частіше на практиці застосовуються методи та протоколи швидкої перемаршрутизації, під час яких попередньо розраховуються два типи шляхів: основний і резервний. У цьому випадку використання окремо кожного типу шляхів має сприяти задоволенню вимог щодо рівня мережної безпеки. Тоді в разі відмови основного шляху повідомлення практично миттєво (із затримкою в десятки мілісекунд) будуть передаватися з використанням резервних маршрутів. Очевидно, що основний і резервний маршрути не повинні перетинатися за елементами мережі, які скомпрометовані (маршрутизаторами, каналами зв’язку або маршрутами загалом) [49–52].

Тоді в межах безпечної швидкої перемаршрутизації (Secure Fast ReRouting, S-FRR) використання множини основних шляхів належить до рішень проактивного підходу щодо забезпечення заданого рівня мережної безпеки, а застосування резервних шляхів відповідає вимогам реактивного підходу. Зокрема в межах запропонованого методу розрахунок множини основних і резервних шляхів повинен здійснюватися максимально погоджено для підвищення ефективності кінцевих рішень.

Поділ шляхів на основні та резервні має на увазі, що частини повідомлення будуть передаватися не всіма доступними композитними та простими шляхами, а лише їхньою обмеженою кількістю, але з виконанням вимог щодо ймовірності компрометації (3.1). З огляду на те, що для підвищення рівня мережної безпеки повідомлень, які передаються, необхідно реалізувати багатошляхову маршрутизацію їх частин, то основними та резервними будуть не окремі композитні або прості шляхи, а утворені ними мультишляхи. У цьому випадку у складі як основного, так і резервного мультишляху можуть міститися кілька композитних та (або) простих шляхів.

Для розрахунку резервного мультишляху пропонується реалізувати такі дві схеми захисту основного мультишляху:

– схема захисту основного мультишляху загалом, за якої основний і резервний мультишляхи не перетинаються ні за вузлами, ні за каналами;

– схема захисту окремого шляху (композитного або простого) основного мультишляху, у разі якої резервний мультишлях не повинен містити канали та вузли шляху, що захищається.

Реалізація кожної зі схем захисту орієнтована на відновлення заданого рівня мережної безпеки за рахунок відмови від основного мультишляху та переходу до використання резервного мультишляху. У зв’язку з цим уточнимо раніше введені та введемо додаткові позначення [47]:

Кількісні показники

$\tilde{p}_i^{pr}$ імовірність компрометації i-го композитного або простого шляху основного мультишляху $\left(i=\overline{1,\tilde{M}}\right)$;

$\tilde{p}_i^{b}$ імовірність компрометації i-го композитного або простого шляху резервного мультишляху $\left(i=\overline{1,\tilde{M}}\right)$;

$\tilde{P}_{msg}^{pr}$ імовірність компрометації повідомлення загалом у разі його передачі частинами композитними або простими шляхами основного мультишляху;

$\tilde{P}_{msg}^{b}$ імовірність компрометації повідомлення загалом у випадку його передачі частинами композитними або простими шляхами резервного мультишляху.

Змінні

n_i цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються i-м композитним або простим шляхом, з якого складається основний мультишлях $\left(i=\overline{1,\tilde{M}}\right)$;

$\overline{n}_i$ цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються i-м композитним або простим шляхом, з якого складається резервний мультишлях $\left(i=\overline{1,\tilde{M}}\right)$.

З огляду на введені позначення для розрахунку ймовірності компрометації повідомлення, яке передається частинами множиною композитних шляхів, необхідно за аналогією до формул (3.1) і (3.13) використовувати відповідно вирази:

$$\tilde{P}_{msg}^{pr}=\prod_{i=1}^{\tilde{M}}\tilde{p}_i^{pr} \quad \text{і} \quad \tilde{P}_{msg}^{b}=\prod_{i=1}^{\tilde{M}}\tilde{p}_i^{b}\,. \tag{3.23}$$

Варто зазначити, що ймовірності компрометації мережних фрагментів $\tilde{p}_i^{pr}$ і $\tilde{p}_i^{b}$ є функціями від кількості частин повідомлення, що передаються ними, тобто від n_i і $\overline{n}_i$. Тоді з урахуванням (3.12) мають місце умови [47]:

$$\tilde{p}_i^{pr}=\begin{cases}1-\prod\limits_{j=1}^{\tilde{M}_i}\left(1-\tilde{p}_i^{\,j}\right), n_i>0;\\ 1, n_i=0,\end{cases} \text{ і } \tilde{p}_i^{b}=\begin{cases}1-\prod\limits_{j=1}^{\tilde{M}_i}\left(1-\tilde{p}_i^{\,j}\right), \overline{n}_i>0;\\ 1, \overline{n}_i=0.\end{cases} \tag{3.24}$$

Системи (3.24) можуть бути записані як

$$\tilde{p}_i^{pr} = 1 - H_0(n_i) \prod_{j=1}^{\tilde{M}_i} \left(1 - \tilde{p}_i^{\,j}\right) \quad \text{і} \quad \tilde{p}_i^{b} = 1 - H_0(\overline{n}_i) \prod_{j=1}^{\tilde{M}_i} \left(1 - \tilde{p}_i^{\,j}\right), \tag{3.25}$$

де H_0 – функція Хевісайда, що з урахуванням виразу (3.24) розраховується таким чином:

$$H_0(n) = \begin{cases} 0, n = 0; \\ 1, n > 0. \end{cases}$$

Умова (3.20) з огляду на реалізацію S-FRR доповнюються виразом

$$\sum_{i=1}^{\tilde{M}} \overline{n}_i = N. \tag{3.26}$$

У свою чергу для захисту основного мультишляху, за аналогією з [53], необхідно забезпечити виконання такої умови:

$$\sum_{i=1}^{\tilde{M}} n_i \, \overline{n}_i = 0. \tag{3.27}$$

За необхідності захисту окремого i-го композитного шляху важливо забезпечити виконання умови

$$n_i \, \overline{n}_i = 0, \tag{3.28}$$

яка також є нелінійною (білінійною).

Для того щоб у використанні й основного, і резервного мультишляху виконувалися вимоги щодо ймовірності компрометації повідомлення, яке за ними передається, уводиться за аналогією з (3.1) така умова [47]:

$$P_{msg}^{pr} \le P_{msg}^{b} \le \gamma_P. \tag{3.29}$$

Тоді в основу розроблюваного методу S-FRR може бути покладено рішення оптимізаційної задачі нелінійного цілочисельного програмування (Nonlinear Integer Programming) з критерієм оптимальності

$$J = \sum_{i=1}^{\tilde{M}} \tilde{p}_i n_i + \sum_{i=1}^{\tilde{M}} \tilde{p}_i \overline{n}_i \tag{3.30}$$

і обмеженнями, що відповідають умовам (3.17), (3.18), (3.20), (3.26), (3.27), (3.28) та (3.29). Зокрема обмеження (3.27)–(3.29) є нелінійними, а змінні n_i й $\overline{n}_i$ мають цілочисельний характер [47]. У критерії (3.30) значення $\tilde{p}_i$, розраховані відповідно до виразів (3.12), є вартісними ваговими коефіцієнтами. Цим забезпечується безпечна маршрутизація в мережі, коли максимальна кількість частин повідомлення буде передаватися шляхом з мінімальною ймовірністю компрометації. Навпаки, шляхом з найвищою ймовірністю компрометації передаватиметься мінімальна кількість частин повідомлення або не буде передано жодної.

3.7. Дослідження методу безпечної швидкої перемаршрутизації повідомлень композитними шляхами

Продемонструємо особливості функціонування запропонованого методу безпечної швидкої перемаршрутизації конфіденційних повідомлень. Вихідна структура мережі представлена на рис. 3.13, а відповідні ймовірності компрометації каналів зв'язку наведені в табл. 3.5.

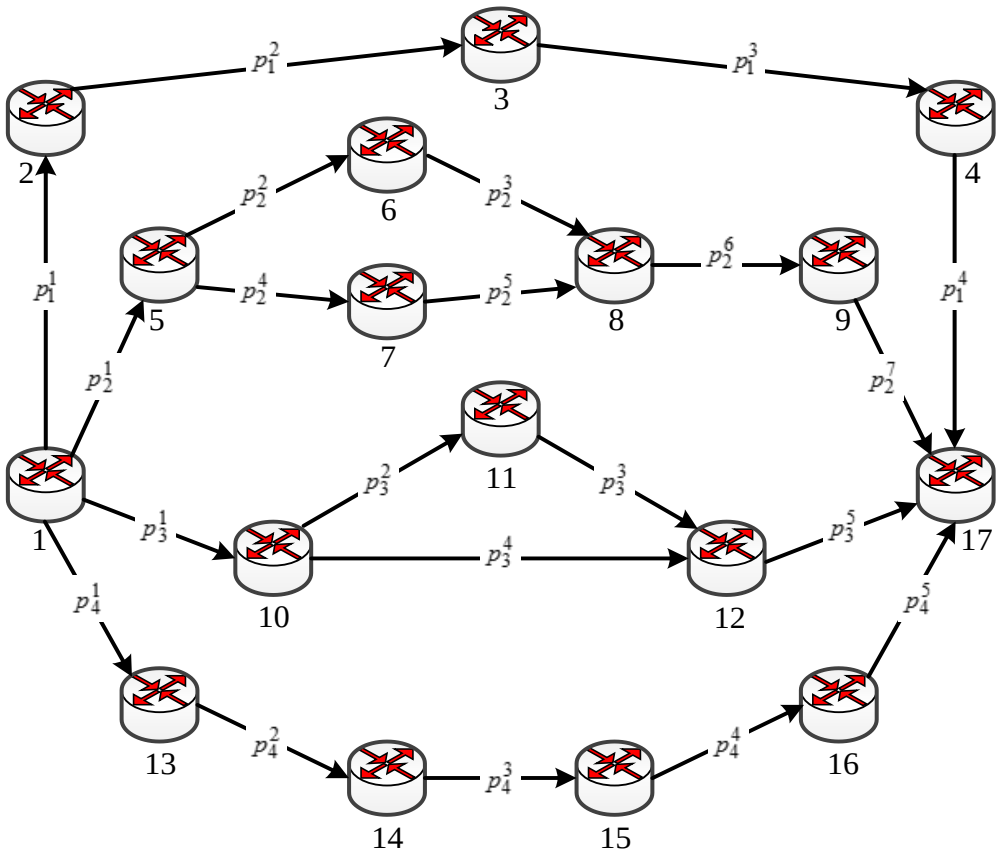


Рис. 3.13. Вихідна структура мережі

Відправником повідомлення є перший вузол, а отримувачем – сімнадцятий вузол. Суцільними лініями на рис. 3.13 показані канали зв'язку, що використовуються для формування основного та резервного мультишляхів для передачі повідомлення. Нехай за умови безпечної швидкої перемаршрутизації реалізується схема Шаміра (10, 10) і відповідно до структури шляхів, наведених на рис. 3.13, $h_1 = 1$, $h_2 = 2$, $h_3 = 2$ та $h_4 = 1$, а допустиме значення ймовірності компрометації повідомлення, що передається, яке визначається параметром γ_P, так само 0,3. Тоді в процесі дослідження розглянуто два випадки, що демонструють особливості реалізації описаних у підрозділі 3.6 схем захисту:

– перший випадок пов'язаний зі схемою захисту другого (композитного) шляху;

– другий випадок описує схему захисту основного мультишляху загалом.

Розглянемо докладніше перший випадок. Тоді, відповідно до наведених у табл. 3.5 вихідних даних, ґрунтуючись на запропонованому в підрозділі 3.6 методі розрахунку, основний мультишлях містить два композитних шляхи: другий і третій, які мають найменші ймовірності компрометації: 0,5339 і 0,4061 відповідно. Параметри цих шляхів і послідовність балансування ними частин повідомлення, яке передається, наведені в табл. 3.6.

Таблиця 3.5

Вихідні дані для дослідження безпечної швидкої перемаршрутизації

Номер шляху	1 (простий)						
Канал зв'язку	1→2	2→3	3→4	4→17			
№ каналу зв'язку в шляху	1	2	3	4			
Імовірність компрометації каналу зв'язку	0,15	0,19	0,17	0,2			
Номер шляху	2 (композитний)						
Канал зв'язку	1→5	5→6	6→8	5→7	7→8	8→9	9→17
№ каналу зв'язку в шляху	1	2	3	4	5	6	7
Імовірність компрометації каналу зв'язку	0,2	0,2	0,1	0,2	0,2	0,19	0,2
Номер шляху	3 (композитний)						
Канал зв'язку	1→10	10→11	11→12	10→12	12→17		
№ каналу зв'язку в шляху	1	2	3	4	5		
Імовірність компрометації каналу зв'язку	0,2	0,2	0,2	0,2	0,2		
Номер шляху	4 (простий)						
Канал зв'язку	1→13	13→14	14→15	15→16	16→17		
№ каналу зв'язку в шляху	1	2	3	4	5		
Імовірність компрометації каналу зв'язку	0,2	0,18	0,1	0,15	0,1		

За третім (композитним) шляхом передавалося вісім частин повідомлення, тому що ймовірність його компрометації мінімальна та дорівнює 0,4061. За другим (композитним) шляхом передавалося дві частини повідомлення, оскільки ймовірність його компрометації була вже 0,5339, а нижній поріг для n_2 відповідно до умов (3.17) становив $h_2 = 2$. Використання даних двох шляхів як основного мультишляху відповідно до виразу (3.23) забезпечує ймовірність компрометації повідомлення, рівну 0,2168, що задовольняє вимозі $(\gamma_P = 0{,}3)$.

У разі захисту другого (композитного) шляху основного мультишляху у складі розрахованого резервного мультишляху будуть уже перший (простий) і третій (композитний) шляхи, параметри яких наведені в табл. 3.7.

Таблиця 3.6

Параметри основного мультишляху

Номер шляху	2 (композитний)						
Імовірність компрометації шляху	0,5339						
Кількість частин повідомлення в шляху	2						
Канал зв’язку	1→5	5→6	6→8	5→7	7→8	8→9	9→17
№ каналу зв’язку в шляху	1	2	3	4	5	6	7
Кількість частин повідомлення в каналі зв’язку	2	1	1	1	1	2	2
Номер шляху	3 (композитний)						
Імовірність компрометації шляху	0,4061						
Кількість частин повідомлення в шляху	8						
Канал зв’язку	1→10	10→11	11→12	10→12	12→17		
№ каналу зв’язку в шляху	1	2	3	4	5		
Кількість частин повідомлення в каналі зв’язку	8	4	4	4	8		

Таблиця 3.7

Параметри резервного мультишляху (перший випадок)

Номер шляху	1 (простий)				
Імовірність компрометації шляху	0,5428				
Кількість частин повідомлення в шляху	1				
Канал зв’язку	1→2	2→3	3→4	4→17	
№ каналу зв’язку в шляху	1	2	3	4	
Кількість частин повідомлення в каналі зв’язку	1	1	1	1	
Номер шляху	3 (композитний)				
Імовірність компрометації шляху	0,4061				
Кількість частин повідомлення в шляху	9				
Канал зв’язку	1→10	10→11	11→12	10→12	12→17
№ каналу зв’язку в шляху	1	2	3	4	5
Кількість частин повідомлення в каналі зв’язку	9	5	5	4	9

За третім (композитним) шляхом передаватиметься дев’ять частин повідомлення, а за першим (простим) усього одна, тому що ймовірність

компрометації першого шляху становила 0,5428 за умови $h_1 = 1$. Використання резервного мультишляху також задовольняє вимоги щодо ймовірності компрометації переданого повідомлення (3.29), яка становила 0,2204.

Розглянемо докладніше другий випадок, у межах якого необхідно було захистити основний мультишлях загалом. Застосування запропонованого методу S-FRR залишило незмінним основний мультишлях (табл. 3.6). Тоді відповідно до наведених у табл. 3.5 вихідних даних резервний мультишлях містить два простих шляхи – перший і четвертий (табл. 3.8).

Таблиця 3.8

Параметри резервного мультишляху (другий випадок)

Номер шляху	1 (простий)			
Імовірність компрометації шляху	0,5428			
Кількість частин повідомлення в шляху	9			
Канал зв'язку	1→2	2→3	3→4	4→17
№ каналу зв'язку в шляху	1	2	3	4
Кількість частин повідомлення в каналі зв'язку	9	9	9	9
Номер шляху	4 (простий)			
Імовірність компрометації шляху	0,5483			
Кількість частин повідомлення в шляху	1			
Канал зв'язку	1→13	13→14	14→15	15→16	16→17
№ каналу зв'язку в шляху	1	2	3	4	5
Кількість частин повідомлення в каналі зв'язку	1	1	1	1	1

Імовірність компрометації четвертого (простого) шляху становила 0,5483. Тоді використання резервного мультишляху дозволило забезпечити значення ймовірності компрометації повідомлення, яке передається, в 0,2977 у разі $\gamma_P = 0,3$. За першим шляхом передавалося дев'ять частин повідомлення, тому що його ймовірність компрометації була нижчою, ніж у четвертого шляху, за яким передавалася одна частина повідомлення за умови $h_4 = 1$.

Висновки до третього розділу

1. Визначено, що залежно від часу реакції на можливу компрометацію каналів зв'язку та фрагментів мережі для забезпечення заданого рівня мережної

безпеки на практиці можуть використовуватися як проактивні, так і реактивні засоби, що повинні взаємно доповнювати один одного. Проактивні засоби застосовуються, як правило, на етапі запобігання компрометації повідомлень або мінімізації ймовірності її виникнення. Реактивні засоби використовуються тоді, коли безпека даних, що передаються, уже порушена і мережними засобами важливо оперативно відновити необхідний рівень безпеки.

2. Установлено, що одним з ефективних проактивних засобів забезпечення заданого рівня мережної безпеки є багатошляхова маршрутизація конфіденційних повідомлень, розділеного на частини відповідно до схеми Шаміра з балансуванням кількості таких частин маршрутами, що не перетинаються. На основі аналізу недоліків наявного механізму SPREAD запропоновано вдосконалення моделі розподілу фрагментів, яка була зведена до задачі оптимального балансування кількості частин повідомлення, що передається, маршрутами, які не перетинаються. Запропоновано низку критеріїв оптимальності, пов'язаних з вирішенням завдання балансування. У процесі порівняльного аналізу обґрунтований до використання на практиці критерій оптимальності, що забезпечує, з одного боку, мінімізацію верхнього динамічно керованого порога кількості частин повідомлення, які передаються окремими непересічними шляхами в мережі, а з іншого, – адаптацію до параметрів безпеки (імовірності компрометації) окремих елементів мережі: вузлів, каналів і шляхів. Представлено числові приклади реалізації моделей з різними критеріями оптимальності отримуваних рішень, і проведено їх порівняльний аналіз. Результати порівняння (табл. 3.2) підтвердили ефективність запропонованої моделі, коли гіршим, з точки зору ймовірності компрометації, шляхом передається мінімальна кількість частин повідомлення, а кращим шляхом – їх максимальна кількість.

3. У розділі запропоновано використання особливого класу шляхів, що перетинаються, які становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі, що орієнтує на зниження ймовірності компрометації конфіденційних повідомлень, які передаються в ІКМ. Розроблено метод безпечної маршрутизації повідомлень шляхами, що перетинаються, який належить до класу проактивних рішень щодо забезпечення мережної безпеки. Новизна методу полягає в тому, що він, по-перше, допускає використання шляхів, які перетинаються, становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку, а по-друге, оснований на оптимізації процесу вибору множини композитних

шляхів і балансування ними частин повідомлення, що передається, із забезпеченням допустимих значень його ймовірності компрометації. Проведений аналіз показав (рис. 3.10 та 3.12), що використання запропонованого методу в межах наведених розрахункових прикладів дозволяє знизити ймовірність компрометації переданих повідомлень у середньому від 5–10 % до 25–50 % з огляду на можливості використання композитних шляхів, які є одним з підкласів шляхів, що перетинаються.

4. Зазначено, що за умови зміни стану мережі, викликаного порушенням рівня безпеки конфіденційних повідомлень, що передаються в ІКМ, важливо визначити оперативну послідовність зміни множини шляхів, які використовуються для передачі його частин. Тому рішення щодо швидкої перемаршрутизації з локальним чи глобальним захистом елементів ІКМ можуть розглядатися як реалізація реактивного підходу щодо забезпечення безпечної маршрутизації. Синтезовано метод безпечної швидкої перемаршрутизації повідомлень у мережі, який орієнтує на реалізацію як проактивної, так і реактивної безпечної маршрутизації конфіденційних повідомлень. Новизна методу безпечної швидкої перемаршрутизації полягає в тому, що в разі порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, які містяться в основному мультишляху, багатошляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень імовірності його компрометації буде здійснюватися вже заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху загалом, або одного чи декількох заздалегідь заданих композитних шляхів, що містить основний мультишлях.

5. У межах запропонованого методу безпечної швидкої перемаршрутизації повідомлень закладено можливість захисту як основного мультишляху загалом, так і одного або декількох заздалегідь заданих композитних шляхів, що містить цей основний мультишлях. Застосування методу S-FRR дозволяє в реальному часі забезпечувати задані значення такого важливого показника мережної безпеки, як імовірність компрометації повідомлень, що передаються, навіть в умовах динамічної зміни стану мережі (імовірності компрометації каналів і шляхів) на підставі розрахунку й оперативного переходу на використання резервних композитних шляхів за умови багатошляхової передачі частин конфіденційного повідомлення.

6. Розроблені методи безпечної маршрутизації можуть бути покладені в основу нових мережних протоколів маршрутизації та швидкої перемаршрутизації

для багатошляхової передачі частин конфіденційного повідомлення із заданими вимогами щодо граничної ймовірності його компрометації в мережі.

Перелік джерел посилання до третього розділу

1. ITU-T Rec. Y.2701. Security requirements for NGN release 1. April 2007. 44 p. URL: https://www.itu.int/rec/T-REC-Y.2701-200704-I/en.

2. ITU-T Rec. Y.2704. Security mechanisms and procedures for NGN. January 2010. 58 p. URL: https://www.itu.int/rec/T-REC-Y.2704-201001-I/en.

3. ITU-T Rec. Y.2705. Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS). March 2013. 24 p. URL: https://www.itu.int/rec/T-REC-Y.2705-201303-I/en.

4. ITU-T Rec. Y.2720. NGN identity management framework. January 2009. 34 p. URL: https://www.itu.int/rec/T-REC-Y.2720-200901-I.

5. ITU-T Rec. Y.2770. Requirements for deep packet inspection in next generation networks. December 2012. 38 p. URL: https://www.itu.int/rec/T-REC-Y.2770-201211-I/en.

6. Телекомунікаційні системи та мережі. Структура та основні функції / В.В. Поповський та ін. Харків: СМІТ, 2011. Т. 1. URL: http://www.znanius.com/3534.html.

7. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах: в 2 т. Харьков: СМИТ, 2006.

8. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах: в 2 т. Харьков: СМИТ, 2010.

9. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. 464 с.

10. Оксіюк О.Г., Гаврилов Д.С., Гуржій П.М., Демідов Б.О. Метод забезпечення безпеки відеоінформаційного ресурсу на основі багаторівневої селективної обробки в телекомунікаційних системах. Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 1. С. 46–48.

11. Оксіюк О.Г. Методика розрахунку часу затримки інформації управління в інформаційно-комунікаційних мережах. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. 2015. № 3. С. 133–140.

12. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015. 398 p.

13. Stallings W. Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2016. 768 p.

14. Новиков С.Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи. Москва: Горячая линия – Телеком, 2015. 128 с.

15. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience-fundamentals for a definition. New Contributions in Information Systems and Technologies. 2015. Vol. 353. Springer, Cham. P. 311–316. DOI: https://doi.org/10.1007/978-3-319-16486-1_31.

16. Fink G.A., Griswold R.L., Beech Z.W. Quantifying cyber-resilience against resource-exhaustion attacks. Resilient Control Systems (ISRCS) 2014: Proceedings of the 7th International Symposium, Denver, CO, USA, 19–21 August, 2014. IEEE, 2014. P. 1–8. DOI: 10.1109/ISRCS.2014.6900093.

17. Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A. Comprehensive approach to increase cyber security and resilience. Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24–27 August, 2015. IEEE, 2015. P. 686–692. DOI: 10.1109/ARES.2015.30.

18. Musman S. Assessing prescriptive improvements to a system's cyber security and resilience. Systems Conference (SysCon) 2016: Proceedings of the Annual IEEE Conference. Orlando, FL, USA, 18–21 April, 2016. IEEE, 2016. P. 1–6. DOI: 10.1109/SYSCON.2016.7490660.

19. Galinec D., Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. Informatics 2017: Proceedings of the IEEE 14th International Scientific Conference. Poprad, Slovakia, 14–16 November, 2017. IEEE, 2017. P. 87–93. DOI: 10.1109/INFORMATICS.2017.8327227.

20. ITU-T X-805. Security architecture for systems providing end-to-end communications. October 2003. 28 p. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en.

21. ISO 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. International Standard ISOIEC, 74981, 1994. 59 p.

22. ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989. 32 p.

23. ITU-T X-800. Security architecture for Open Systems Interconnection for CCITT applications. March 1991. 48 p. URL: https://www.itu.int/rec/T-REC-X.800-199103-I.

24. Santos O., Kampanakis P., Woland A. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. 1 edition. Cisco Press, 2016. 368 p.

25. Al-Kuwaiti M., Kyriakopoulos N., Hussein S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. IEEE Communications Surveys & Tutorials. 2009. Vol. 11, No. 2. P. 106–124. DOI: 10.1109/SURV.2009.090208.

26. Kaur R., Kashmira P., Meena K., Mohapatra A. K. Survey on Different Techniques of Threshold Cryptography. Journal of Electronics and Communication Engineering (IOSR-JECE). 2017. P. 114–119.

27. Venukumar V., Pathari V. A survey of applications of threshold cryptography – proposed and practiced. Information Security Journal: A Global Perspective. 2016. Vol. 25, No. 4–6. P. 180–190. DOI: 10.1080/19393555.2016.1251996.

28. Sarma K.S., Lamkuche H.S., Umamaheswari S. A Review of Secret Sharing Schemes. Research Journal of Information Technology. 2013. Vol. 5. P. 67–72. DOI: 10.3923/rjit.2013.67.72.

29. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. IEEE Transactions on Vehicular Technology. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.

30. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.

31. Alouneh S., En-Nouaary A., Agarwal A. A Multiple LSPs Approach to Secure Data in MPLS Networks. Journal of Networks. 2007. Vol. 2, No. 4. P. 51–58. DOI: 10.4304/jnw.2.4.51–58.

32. Alouneh S., Agarwal A., En-Nouaary A. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing. Computer Networks: The International Journal of Computer and Telecommunications Networking. 2009. Vol. 53, No. 9. P. 1530–1545. DOI: 10.1016/j.comnet.2009.02.001.

33. Кулаков Ю.А., Лукашенко В.В., Левчук А.В. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности. Захист інформації. 2011. Том 13, № 2(51). С. 5–10. DOI: 10.18372/2410-7840.13.2018.

34. Gupta D., Segal A., Panda A., Segev G., Schapira M., Feigenbaum J., Rexford J., Shenker S. A new approach to interdomain routing based on secure multi-party computation. Hot Topics in Networks: Proceedings of the 11th ACM Workshop. October, 2012. ACM, 2012. P. 37–42. DOI: 10.1145/2390231.2390238.

35. Gharib M., Yousefizadeh H., Movaghar A. Secure Overlay Routing for Large Scale Networks. IEEE Transactions on Network Science and Engineering. 2018. Vol. 1. P. 1–12. DOI: 10.1109/TNSE.2018.2812830.

36. Чевардін В.Є., Романюк В.А., Шевченко В.С. Модель загроз безпеки інформації в сучасних телекомунікаційних мережах з динамічною топологією. Збірник наукових праць ВІТІ НТУУ «КПІ». 2012. № 2. С. 90–95.

37. Снегуров А.В., Чакрян В.Х. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности. Системи управління, навігації та зв'язку. 2012. № 4(24). С. 105–110.

38. Snihurov A., Chakrian V. Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters. Scholars Journal of Engineering and Technology. 2015. Vol. 3, No. 8. C. 707–714.

39. Gomes T., Martins L., Ferreira S., Pascoal M., Tipper D. Algorithms for determining a node-disjoint path pair visiting specified nodes. Optical Switching and Networking. 2017. Vol. 23. P. 189–204. DOI: https://doi.org/10.1016/ j.osn.2016.05.002.

40. Myslitski K., Rak J., Kuszner Ł. Toward fast calculation of communication paths for resilient routing. Networks. 2017. Vol. 70, No. 4. P. 308–326. DOI: https://doi.org/10.1002/net.21789.

41. Natarajan M. Graph Theory Algorithms for Mobile Ad Hoc Networks. Informatica – An International Journal of Computing and Informatics. 2012. Vol. 36. P. 185–200.

42. Suurballe J. W. Disjoint paths in a network. Neworks. 1974. Vol. 4, No. 2. P. 125–145.

43. Лемешко А.В., Еременко А.С. Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам. Захист інформації. 2015. Т. 17. № 2. С. 135-142. DOI: 10.18372/2410-7840.17.8776.

44. Yeremenko O.S., Ali S.A. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET. Radioelectronics and Informatics. 2015. № 1(68). С. 26–29.

45. Еременко А.С. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-

параллельной или комбинированной структурой. Наукові записки Українського науково-дослідного інституту зв'язку. 2015. № 6(40). С. 64–71.

46. Yeremenko O., Lemeshko O., Persikov A. Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in Communication Network. Computer Sciences and Information Technologies (CSIT): Proceedings of the XIIth International Scientific and Technical Conference, Lviv, Ukraine, 5–8 Sept. 2017. IEEE, 2017. P. 87–90. DOI: 10.1109/STC-CSIT.2017.8098743.

47. Yeremenko O., Lemeshko O., Persikov A. Secure Routing in Reliable Networks: Proactive and Reactive Approach. Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 689. P. 631–655. DOI: 10.1007/978-3-319-70581-1_44.

48. Yeremenko O., Yevdokymenko M., Persikov A. Flow-aware approach of evaluating probability of compromise in combined structure network. Advanced Information and Communication Technologies (AICT): Proceedings of the 2nd International Conference, Lviv, Ukraine, 4–7 July, 2017. IEEE, 2017. P. 258–261. DOI: 10.1109/AIACT.2017.8020114.

49. Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A. Quality of resilience as a network reliability characterization tool. IEEE network. 2009. Vol. 23, No. 2. P. 11–19. DOI: 10.1109/MNET.2009.4804331.

50. Tipper D. Resilient network design: challenges and future directions. Telecommunication Systems. 2014. Vol. 56, No. 1. P. 5–16. DOI: 10.1007/s11235-013-9815-x.

51. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 181 p.

52. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. Optical Switching and Networking, 2017. Vol. 23, Part 2. P. 156–178. DOI: https://doi.org/10.1016/j.osn. 2016.06.002.

53. Lemeshko O., Romanyuk A., Kozlova H. Design schemes for MPLS Fast ReRoute. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) 2013: Proceedings of the 12th International Conference. Polyana Svalyava, Ukraine, 19-23 February, 2013. IEEE, 2013. P. 202–203.