РОЗДІЛ 2
ПОТОКОВІ МОДЕЛІ ТА МЕТОДИ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

У розділі пропонується система теоретичних рішень щодо розв'язання задач відмовостійкої маршрутизації в ІКМ, представлених відповідними математичними моделями та методами, які можуть бути покладені в основу перспективних маршрутних протоколів. Нові та вдосконалені математичні моделі та методи охоплюють два основні варіанти організації відмовостійкої маршрутизації – без та з резервуванням елементів ІКМ. Маршрутні рішення без резервування елементів ІКМ основані на реалізації багатошляхової маршрутизації без введення надлишковості в обсяги використаного мережного ресурсу, коли в разі відмови одного або декількох шляхів мережний трафік міг ще передаватися множиною працездатних маршрутів. Тому при розв'язанні задач відмовостійкої маршрутизації в цьому випадку накладаються додаткові обмеження на характер перетинання множини розрахованих шляхів, щоб відмова одного шляху мінімально впливала на працездатність інших маршрутів.

Моделі та методи відмовостійкої маршрутизації з резервуванням елементів ІКМ вводять надлишковість у використання мережного ресурсу. Тобто одночасно з множиною основних шляхів також розраховується і множина резервних маршрутів, на використання яких майже миттєво (50–60 мс) [1, 2] перемикаються потоки пакетів у разі відмови того чи іншого елемента мережі: шлюзу за замовчуванням, каналу, вузла або шляху, що підлягають захисту. У зв'язку з цим на рівні транспортної мережі подібні відмовостійкі рішення належать до засобів швидкої перемаршрутизації (Fast ReRoure, FRR). Запропоновані в розділі рішення для підвищення рівня QoS орієнтовані як на реалізацію вимог концепції Traffic Engineering (TE-FRR) щодо забезпечення збалансованого використання доступного мережного ресурсу, так і на захист рівня QoS за показником пропускної здатності (швидкості передачі пакетів).

2.1. Маршрутизація як засіб забезпечення відмовостійкості ІКМ

Незважаючи на постійне зростання надійності сучасного комунікаційного обладнання, проблема забезпечення заданого рівня відмовостійкості ІКМ також стоїть досить гостро. До основних глобальних причин відмов в ІКМ належать

масштабні катастрофи, соціально-політичні та економічні чинники, вторинні відмови, людський чинник (помилки людини-оператора), загрози мережній безпеці, екологічні проблеми тощо [3–12]. Крім того, серед основних технологічних чинників, що викликають відмови в обслуговуванні в мережі, виокремлюють збої фізичного рівня та перевантаження мережного обладнання в процесі його експлуатації, помилки під час конфігурації та оновлення термінального або мережного програмного забезпечення (рис. 2.1, табл. 2.1) [3–6]. У зв'язку з цим на сьогоднішній день надзвичайно актуальним є завдання, пов'язане з побудовою так званих відмовостійких мереж (Resilient Networks), здатних забезпечити високий рівень якості обслуговування та відмовостійкості (Quality of Resilience, QoR) [3, 4].

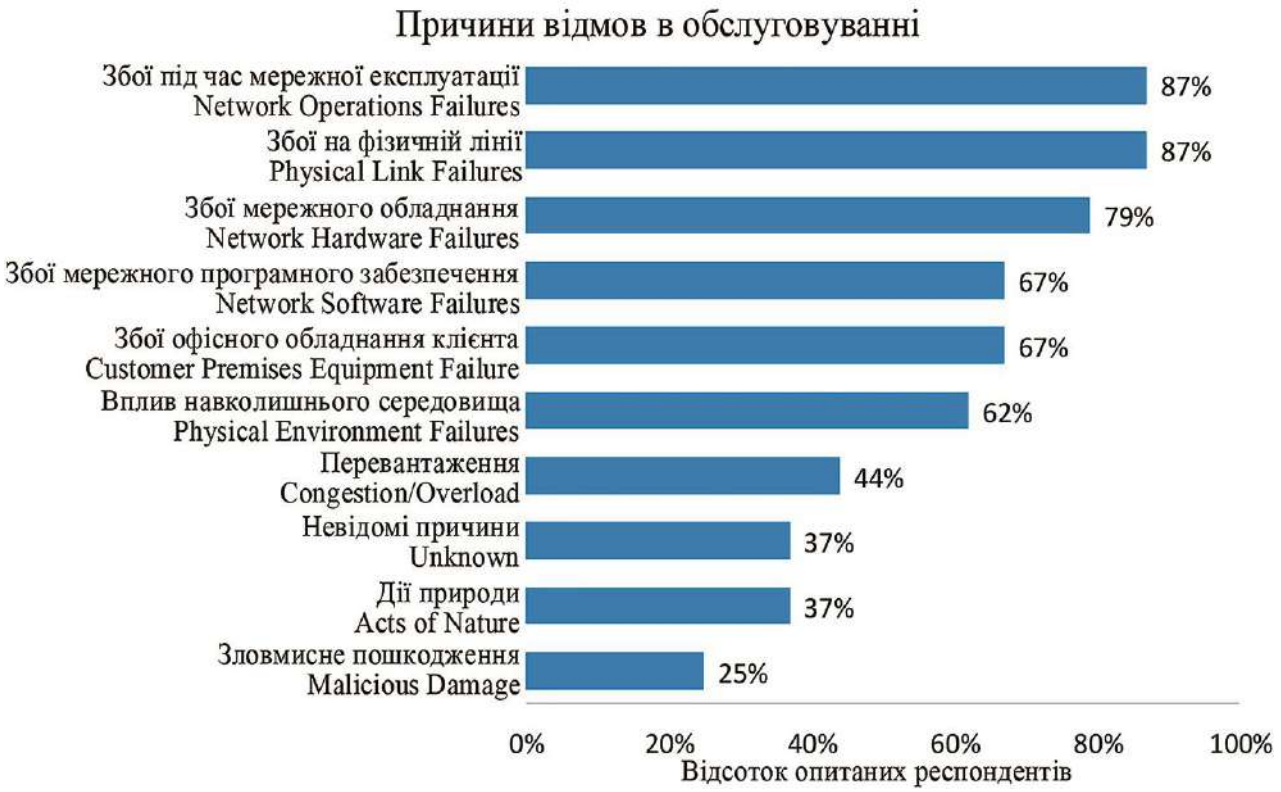


Рис. 2.1. Основні причини, що викликають відмови в обслуговуванні

Варто зазначити, що відмовостійкість мереж була визначена як окремий аспект забезпечення якості обслуговування, що зосереджує увагу на параметрах, пов'язаних із надійністю ІКМ. Надзвичайна важливість QoR обумовлена її значенням для функціонування мереж, а також випливає з широкого спектра технологій, що забезпечують диференційовану QoS кінцевим користувачам (рис. 2.2) [3, 5]. Вимірювані показники для кількісного визначення відмовостійкості вказані у відповідних стандартах ITU-T та IETF [13–16].

Таблиця 2.1

Типи відмов і відсоток їх появи

Типи виходу з ладу		Відсоток, %
Конфігурація оновлення	програмного забезпечення	22
	апаратного забезпечення	9
Збої програмного забезпечення	площина управління	15
	площина даних	5
	інші	5
Збій обладнання	управління	7
	карта введення/виведення	7
Відмови каналів зв'язку		20
Вимкнення електроенергії		1
Інші/невідомі		9

Рис. 2.2. Співвідношення вимог
щодо якості обслуговування та відмовостійкості [5]

Основними засобами забезпечення відмовостійкості ІКМ є:

– інженерні методики організації експлуатації, технічного обслуговування та ремонту комунікаційного обладнання;

– засоби діагностики (самодіагностики) та перевірки (оцінки) працездатності елементів мережі;

– протоколи моніторингу та збирання інформації про стан мережі;

– засоби превентивного виявлення відмов елементів мережі та аналізу ймовірних несправностей;

– протоколи резервування (дуплікації) елементів мережі та її сегментів;

– протоколи маршрутизації та балансування навантаження;

– методи планування мережі з введенням структурної та функціональної надлишковості;

– методи реконфігурації мережі.

Отже, маршрутизація є одним з дієвих технологічних засобів забезпечення відмовостійкості ІКМ, що може реалізовуватися як у процесі визначення та використання найбільш надійних маршрутів (проактивне рішення), так і під час швидкої перемаршрутизації потоків у разі відмови та резервування елементів мережі (реактивне рішення).

2.2. Класифікація засобів відмовостійкої маршрутизації в ІКМ

На сьогоднішній день класифікацію засобів відмовостійкої маршрутизації в ІКМ можна провести за такими критеріями (рис. 2.3) [1, 17–32]:

– за рівнем забезпечення резервування (захисту) елементів мережі;

– за типом підтримуваної схеми захисту;

– за підтримкою захисту рівня QoS;

– за місцем реалізації відмовостійкої маршрутизації в мережі;

– за типом використовуваної схеми резервування.

У разі відсутності резервування (захисту) елементів мережі та реалізації стратегії багатошляхової маршрутизації можуть використовуватися шляхи наступних класів. У шляхів, які не перетинаються, спільними є лише вузли відправника та отримувача. Якщо шляхи містять хоча б один спільний вузол та (або) канал, то вони називаються такими, що перетинаються. Якщо шляхи мають спільні вузли, тоді вони називаються шляхами, що перетинаються за вузлами, а якщо спільні канали – шляхами, що перетинаються за каналами (рис. 2.4).

Для забезпечення резервування (захисту) елементів мережі в процесі відмовостійкої маршрутизації передбачається розрахунок одночасно з основним ще й резервного шляху. Тоді в разі відмови елемента мережі з метою зменшення часу переривання обслуговування важливо не тільки скоротити час для того, щоб переорієнтувати трафік на резервний шлях (тобто дії перемикання щодо відновлення інколи містять розрахунок резервних шляхів після збою), але також зосередити увагу на інших етапах процедури

відновлення, зображених на рис. 2.5, які зазвичай складаються з виявлення та локалізації відмов, повідомлення про них та перемикання на резервний шлях щодо відновлення обслуговування [5].

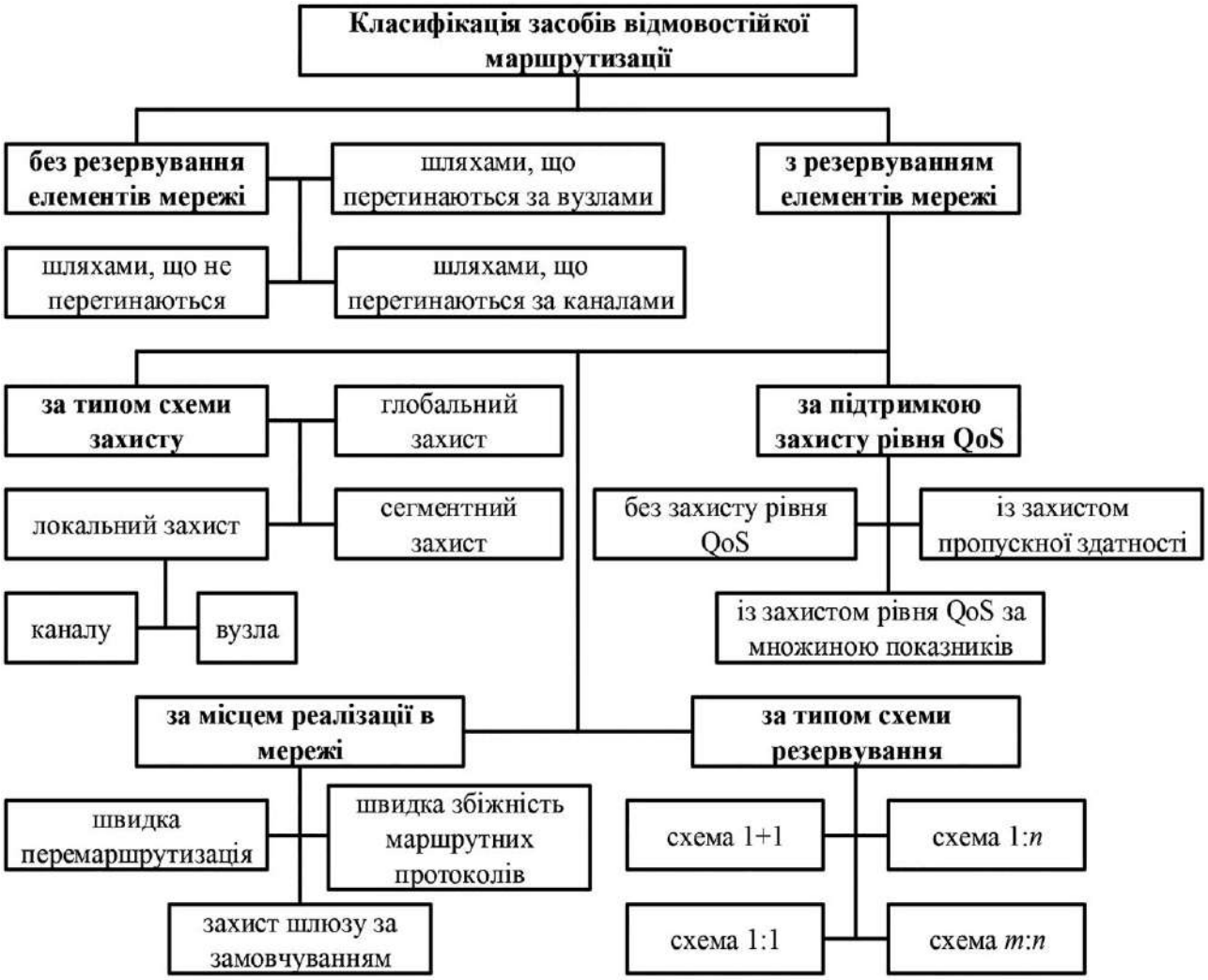


Рис. 2.3. Класифікація засобів відмовостійкої маршрутизації в ІКМ

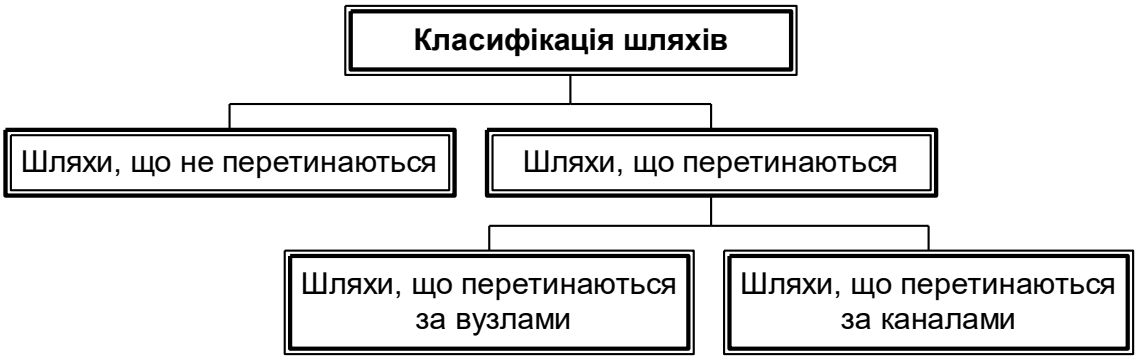


Рис. 2.4. Класифікація шляхів за умови багатошляхової маршрутизації

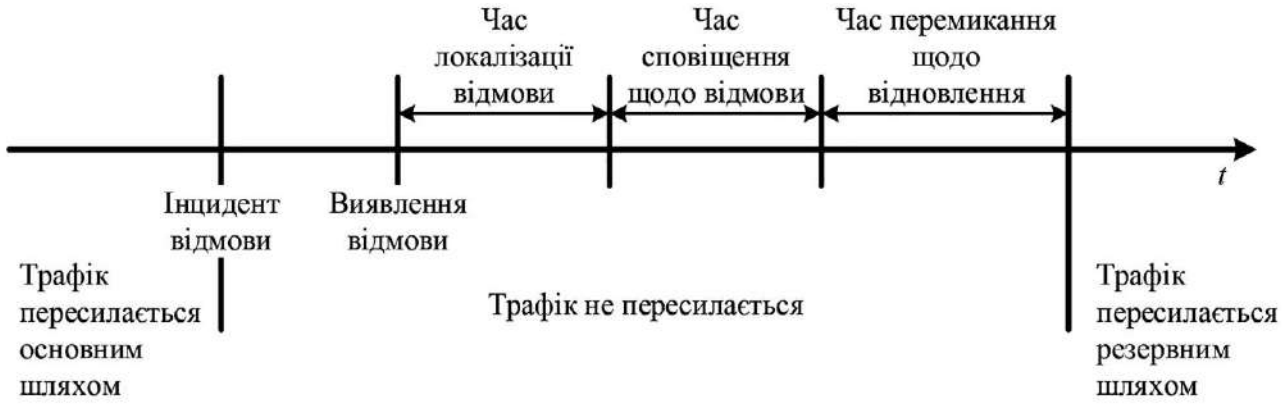


Рис. 2.5. Елементи процедури відновлення обслуговування

За типом підтримуваної схеми захисту в реалізації відмовостійкої маршрутизації в загальному випадку виокремлюють локальний захист (каналу, вузла), глобальний захист (шляху) та сегментний захист (множина елементів мережі) [5, 19, 20]. Схема захисту каналу (link protection) є найбільш простим рішенням і передбачає створення резервного маршруту в обхід аварійного каналу (рис. 2.6). За умови виявлення аварії маршрутизатор направляє потік пакетів на заздалегідь створений резервний маршрут. Пакети передаються резервним маршрутом до моменту розрахунку нового основного маршруту від відправника до отримувача.

Схема захисту вузла (node protection) використовується в разі відмови маршрутизатора (node failure). У цьому випадку резервний маршрут не повинен містити в собі вузол, який захищається. Фактично реалізація цієї схеми зводиться до захисту всіх каналів, безпосередньо підключених до вузла, який захищається (рис. 2.7). Схема захисту маршруту (path protection), наприклад, у мережах MPLS належить до глобальних механізмів захисту. У процесі реалізації захисту шляху основний і резервний маршрути можуть мати спільними лише вузли відправника та отримувача (рис. 2.8).

За підтримкою захисту рівня якості обслуговування виокремлюють засоби відмовостійкої маршрутизації без захисту рівня QoS, із захистом одного QoS-показника, як правило, пропускної здатності, та із захистом рівня QoS за множиною показників. У разі забезпечення захисту пропускної здатності відбувається резервування необхідного канального ресурсу, потрібного для успішної передачі пакетів як основним, так і резервним маршрутом [5]. Схема захисту рівня QoS реалізується в тому випадку, коли доступності резервного шляху недостатньо, а необхідно гарантувати, що уздовж цього шляху буде необхідний обсяг пропускної здатності. Це особливо важливо для потоків пакетів, чутливих до пропускної здатності, затримки та джитеру.

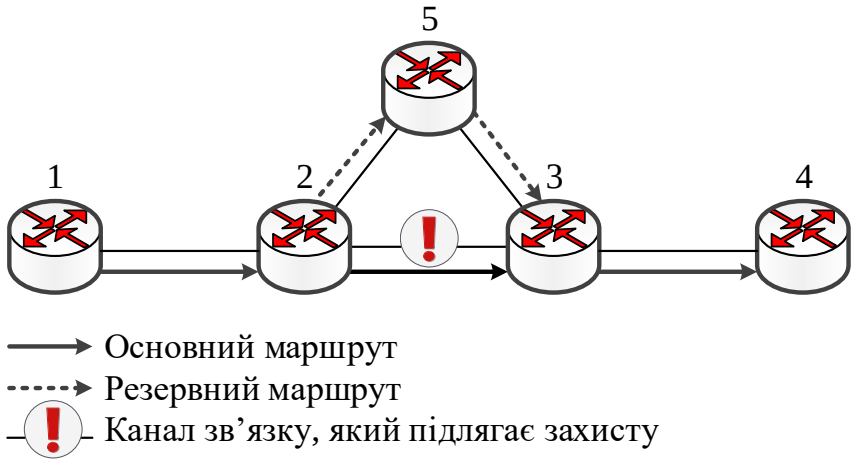


Рис. 2.6. Приклад реалізації схеми захисту каналу

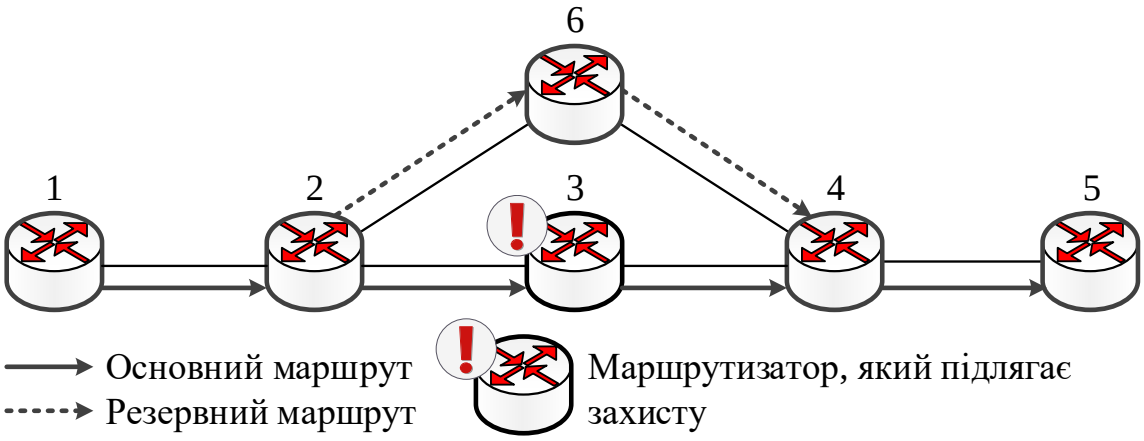


Рис. 2.7. Приклад реалізації схеми захисту вузла

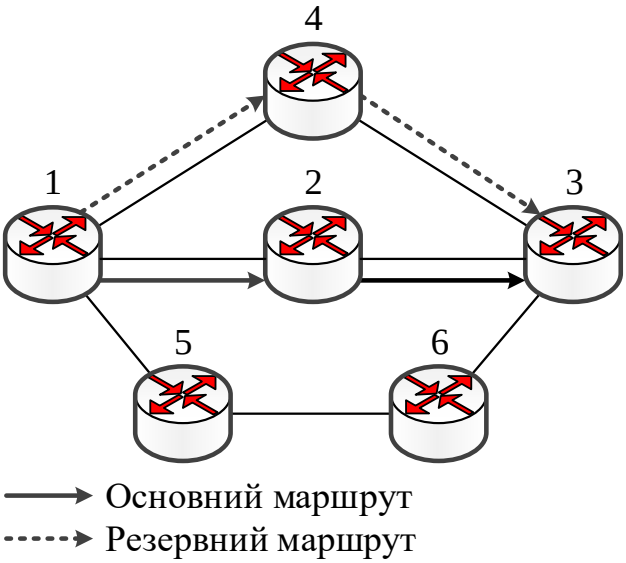


Рис. 2.8. Приклад реалізації схеми захисту маршруту

За місцем реалізації відповідно до багаторівневої архітектури сучасних ІКМ задачі відмовостійкої маршрутизації можуть розв’язуватись як на рівні доступу, так і на рівні ядра ІКМ або транспортної мережі (рис. 2.9) [33].

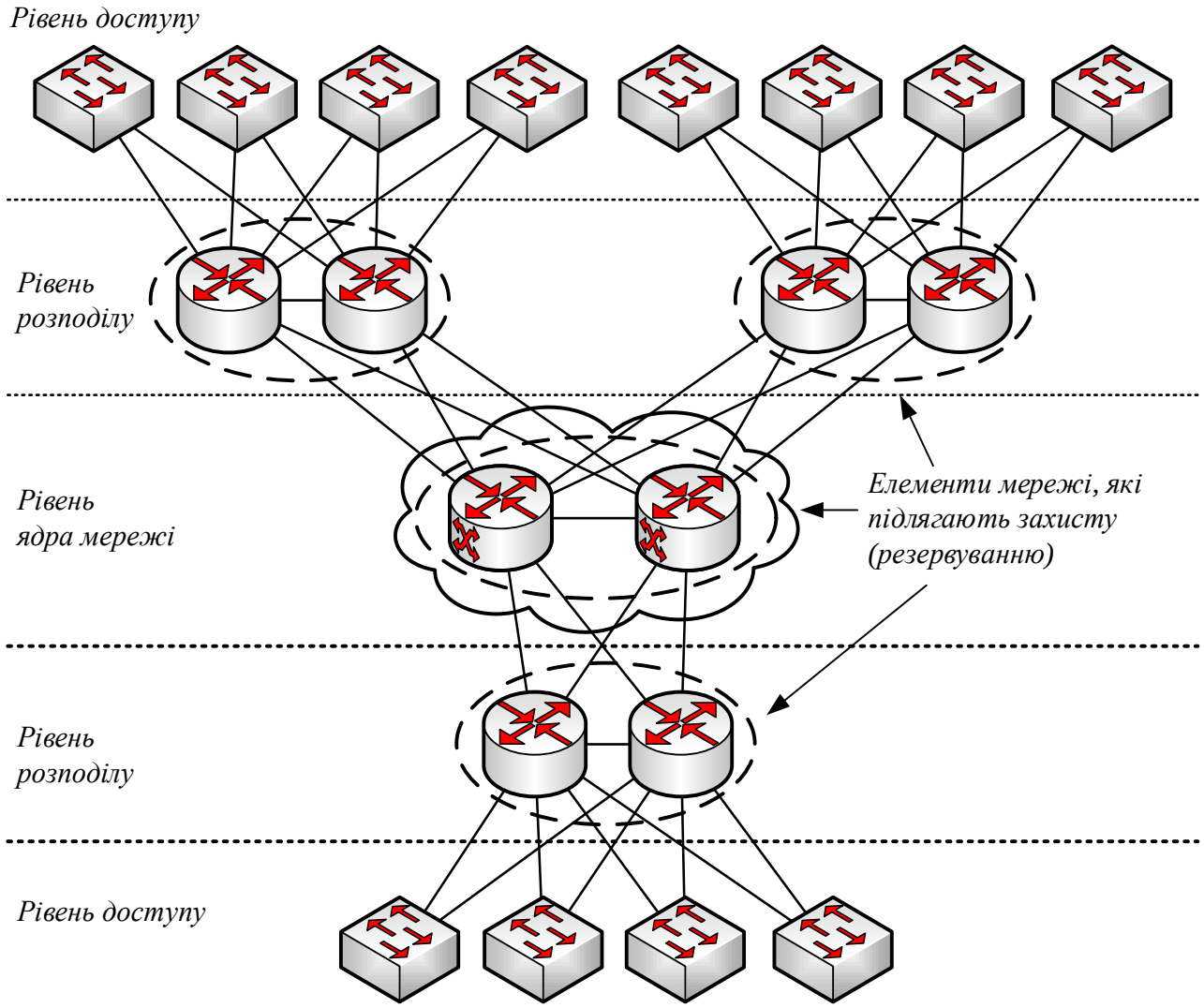


Рис. 2.9. Багаторівнева архітектура забезпечення відмовостійкості ІКМ

На рівні доступу задача відмовостійкої маршрутизації зводиться до захисту шлюзу за замовчуванням, тобто маршрутизатора, до якого комутується та чи інша мережа доступу. Це можливо організувати, коли мережі доступу комутуються одночасно до декількох пригранічних маршрутизаторів, інтерфейси яких конфігуруються відповідним протоколом як віртуальний шлюз за замовчуванням. В IP-мережах до таких протоколів належать Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), Common Address Redundancy Protocol (CARP) [24–27].

Для підвищення доступності приграничних маршрутизаторів у разі відмови основного шлюзу протокол в автоматичному режимі здійснює перемикання потоків на резервний шлюз. Так, наприклад, за умови застосування протоколу VRRP аналізується стан мережі та визначається інтерфейс віртуального маршрутизатора, який у подальшому використовується мережею доступу для підключення до транспортної мережі. Крім того, балансування навантаження за декількома інтерфейсами віртуального маршрутизатора здатне підвищити доступність і надійність з'єднання, однак така функціональність не властива всім протоколам (табл. 2.2) [24, 27].

Таблиця 2.2

Порівняння протоколів резервування шлюзу за замовчуванням

Характеристика	HSRP	VRRP	GLBP	CARP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary	Not a standard (BSD based OS)
Стандарт	RFC 2281	RFC 5798	Ні	Ні
Рівень моделі OSI	Мережний	Мережний	Канальний	Мережний
Балансування навантаження	Не підтримується	Підтримується	Підтримується	Підтримується
IPv6	Підтримується	Підтримується	Підтримується	Підтримується
Переваги	– легка конфігурація; – низьке навантаження мережі службовим трафіком.	– спрощене управління мережею; – висока адаптованість; – низьке навантаження мережі службовим трафіком; – балансування навантаження; – мінімізація обчислювальних витрат.	– ефективне використання мережних ресурсів; – висока доступність; – автоматичне балансування навантаження; – низькі витрати на адміністрування; – ефективне проектування рівня доступу.	– відкрита альтернатива HSRP і VRRP; – резервування для брандмауерів та маршрутизаторів; – балансування навантаження.
Недоліки	– неефективний для передачі трафіку реального часу; – слабкий рівень безпеки; – пропрієтарний протокол Cisco.	– слабкий рівень безпеки (не містить жодного типу автентифікації).	– пропрієтарний протокол Cisco; – висока складність управління мережею.	– несумісність з чинними стандартами; – слабкий рівень безпеки.

Найбільш суттєвими недоліками наявних рішень щодо відмовостійкої IP-маршрутизації вважаються такі:

– не враховується потоковий характер мережного трафіку;

– обмежені можливості для балансування навантаження з необхідністю адміністративної конфігурації;

– відсутність узгодженого рішення взаємопов'язаних завдань вибору шлюзу за замовчуванням і маршрутизації у транспортній мережі.

Наприклад, як показано в [24], для забезпечення балансування навантаження за інтерфейсами шлюзів за замовчуванням можуть використовуватися такі механізми: Round Robin та Weighted (зважене) в GLBP, Host-dependent у GLBP та VRRP.

Метод Round Robin передбачає рівномірне балансування навантаження за всіма інтерфейсами віртуального шлюзу, що є прийнятним рішенням лише у разі приблизно однакової доступності пригранічних маршрутизаторів транспортної мережі. В іншому випадку доцільно використовувати зважене балансування навантаження, у якому трафік, що надходить від мереж доступу, розподіляється між інтерфейсами віртуального маршрутизатора пропорційно їх адміністративній вазі. Третій механізм (host-dependent) реалізує псевдобалансування, коли певний віртуальний інтерфейс шлюзу для однієї мережі доступу є основним інтерфейсом, а для іншої мережі доступу – резервним. Таким чином, для забезпечення нерівномірного балансування навантаження між пригранічними маршрутизаторами транспортної мережі з різною доступністю необхідно адміністративно проводити додаткову конфігурацію обладнання.

Ці механізми балансування значно знижують швидкість реакції мережі на можливі збої та обмежують функціональність мережних рішень для захисту шлюзів (резервування). Крім того, навіть у разі оптимізації балансування навантаження для захисту шлюзу відсутня гарантія, що після вибору шлюзу за замовчуванням у транспортній мережі є маршрут, який має необхідну пропускну здатність для забезпечення QoS. Це пов'язано з тим, що відомі рішення захисту шлюзу за замовчуванням не узгоджуються з рішеннями маршрутизації в транспортній мережі та вирішуються послідовно та незалежно один від одного.

На рівні ядра мережі функціонал відмовостійкої маршрутизації, як правило, здійснюється в межах технологій швидкої IGP/BGP конвергенції (Fast IGP/BGP convergence) та швидкої перемаршрутизації (Fast ReRoute), які реалізуються в мережах IP та MPLS [1]. У межах технології Fast IGP/BGP convergence забезпечується мінімізація часу реакції ІКМ на можливі відмови

її елементів [1, 17–23, 28–30]. Цей процес ще називається збіжністю мережі (network convergence) або процесом синхронізації таблиць маршрутизації після зміни топології. У загальному випадку під час збіжності необхідно використати час на такі процеси:

– виявлення аварії в мережі;

– передача інформації про аварію, тобто поширення LSA (Link-state advertisement) у мережі;

– обчислення найкоротших шляхів на всіх маршрутизаторах у разі отримання нової інформації про стан ІКМ;

– оновлення маршрутних таблиць на всіх маршрутизаторах у мережі.

Скоротити час збіжності в межах технології IP Fast ReRoute (IP FRR) можна за рахунок зменшення часу виявлення аварії, таймера протоколу Hello; затримок у разі поширення інформації LSA (LSA/LSP flooding) на підставі використання алгоритму експоненційного відтермінування, який дозволяє динамічно розрахувати затримку для генерації LSA; затримок оброблення тощо. Адміністративне зменшення кожного з цих часових параметрів може негативно позначитися на обсягах службового трафіку, що циркулює в мережі, тобто спричинити його неконтрольоване зростання. Тому поряд з вибором у розумних межах значень перелічених параметрів необхідно реалізовувати і доступні схеми резервування ресурсів мережі.

Технологія Fast ReRoute застосовується в IP/MPLS-мережах для захисту елементів транспортної мережі – каналу, вузла, шляху та пропускної здатності мережі загалом. В IP-мережах для підвищення відмовостійкості використовується технологія IP FRR [18, 28], яка багато в чому аналогічна технології Fast ReRoute, що функціонує в мережах MPLS-TE. Метою технології IP FRR є знаходження альтернативного шляху передачі пакетів у разі можливої несправності каналу або вузла мережі без виникнення мікропетель (microloops). За умови швидкої перемаршрутизації застосовуються протоколи IP-мереж, такі як OSPF та I-IS-IS. Якщо маршрутизатор знає про декілька маршрутів з рівною метрикою (вартістю) (Equal Cost MultiPaths, ECMP) від відправника до отримувача, а деякі з них не мають аварійних каналів або вузлів, то такі шляхи можна використовувати як резервні. За відсутності таких шляхів маршрутизатор шукає безпосередньо підключеного сусіда, який має маршрут, що не містить аварійного каналу/вузла до отримувача. Такий шлях через безпосередньо підключеного сусіда називають альтернативним маршрутом без петель (Loop Free Alternate, LFA) [21].

У разі способу альтернативного U-обходу (U-turn Alternates), якщо шляхи ECMP/LFA недоступні, маршрутизатор може сформувати обхідний шлях за рахунок відправлення пакетів у напрямку відправника (джерела), але через інший маршрутизатор, у якого в таблиці маршрутизації може зберігатися альтернативний шлях до вузла призначення. Шляхи відновлення через такі маршрутизатори називають шляхами відновлення мультитранзитної ділянки, і стандартний спосіб такого відновлення представлений у RFC 5714 [28]. На цей час запропоновано декілька варіантів реалізації способів альтернативного U-обходу [1]:

– пряма вказівка в заголовку IP-пакета на заборону пересилання пакета маршрутизатора, у якого відмовив канал [34];

– відправлення пакета іншому маршрутизатору, який має альтернативні відношення зв'язності з ділянкою, у якій розміщений вузол-отримувач;

– використання маршрутизаторами декількох топологічних конфігурацій дерев найкоротших маршрутів (мультитопологій) з можливістю переходу між ними в разі відмови каналу [29];

– тунелювання трафіку в напрямку U-обходу елемента, що відмовив, до місця, де може бути продовжена його безаварійна передача.

Також слід зазначити, що технології IP/MPLS-мереж, як і більшість рішень, пов'язаних з підвищенням мережної надійності, основані на реалізації різноманітних схем резервування [1, 5, 35]:

– схема 1+1, за якої потік пакетів передається одночасно і основним, і резервним маршрутами;

– схема 1:1, коли для кожного робочого маршруту створюється резервний шлях, який не повинен містити проблемний елемент мережі (канал або вузол);

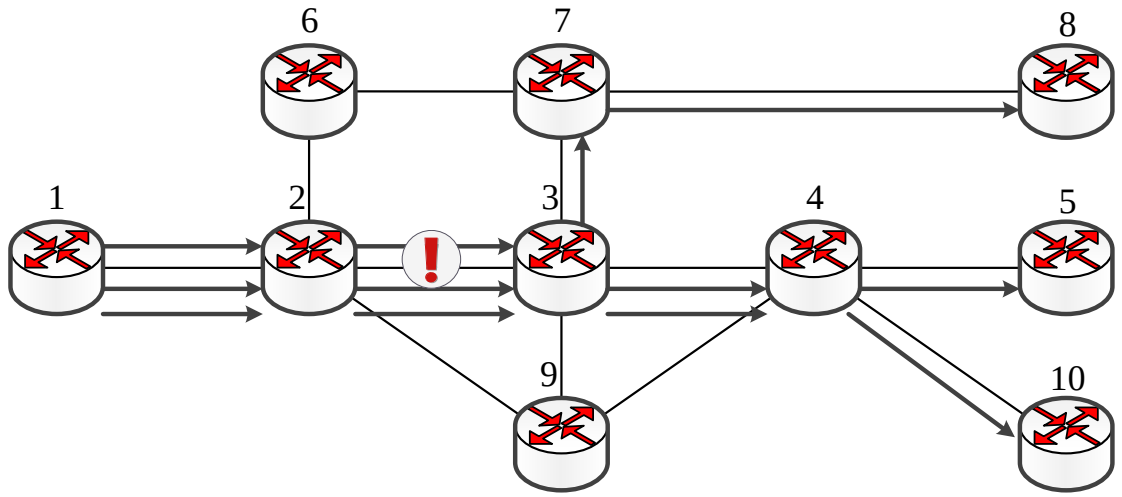
– схема 1:*n*, за якої створюється *один* резервний шлях для *n* основних шляхів (*facility backup*);

– схема *m*:*n*, коли створюється *m* резервних шляхів для *n* основних шляхів.

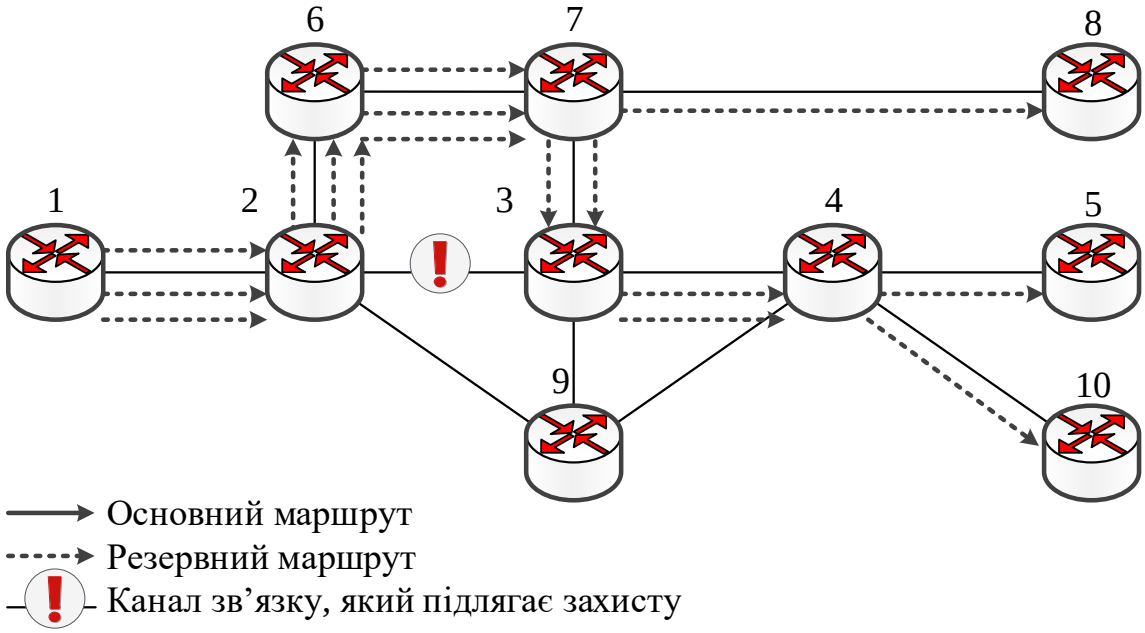
Приклад застосування схеми 1:1 у випадку необхідності захисту каналу зв'язку та вузла показано на рис. 2.10 і 2.11 відповідно.

З точки зору використання пропускної здатності політики щодо відмовостійкості класифікуються на виділені (*dedicated*) та спільні (*shared*) механізми. У виділеній схемі захисту певний обсяг пропускної здатності зарезервовано для перемаршрутизації кожного потоку. Навпаки, у разі застосування механізму спільного захисту резервна пропускна здатність може спільно використовуватися (ділитися) між потоками, на які не впливають одні й ті самі відмови. Це дозволяє зменшити обсяг необхідного для резерву мережного ресурсу, але призводить до ускладнення обчислювальних завдань. На вибір

схеми відновлення/захисту також впливає протокол маршрутизації, що застосовується. Наприклад, у технології MPLS дозволяється явно обирати шлях для кожного потоку пакетів, гарантуючи тим самим більш гнучку політику маршрутизації та дозволяючи використання схеми захисту шляху. Тоді відповідно до протоколу OSPF маршрутизація відбувається за допомогою дерев найкоротших шляхів, і зазвичай застосовується саме схема відновлення.



а) застосування основного шляху



б) використання резервного шляху

Рис. 2.10. Приклад реалізації схеми захисту каналу зв’язку в разі використання схеми резервування 1:1

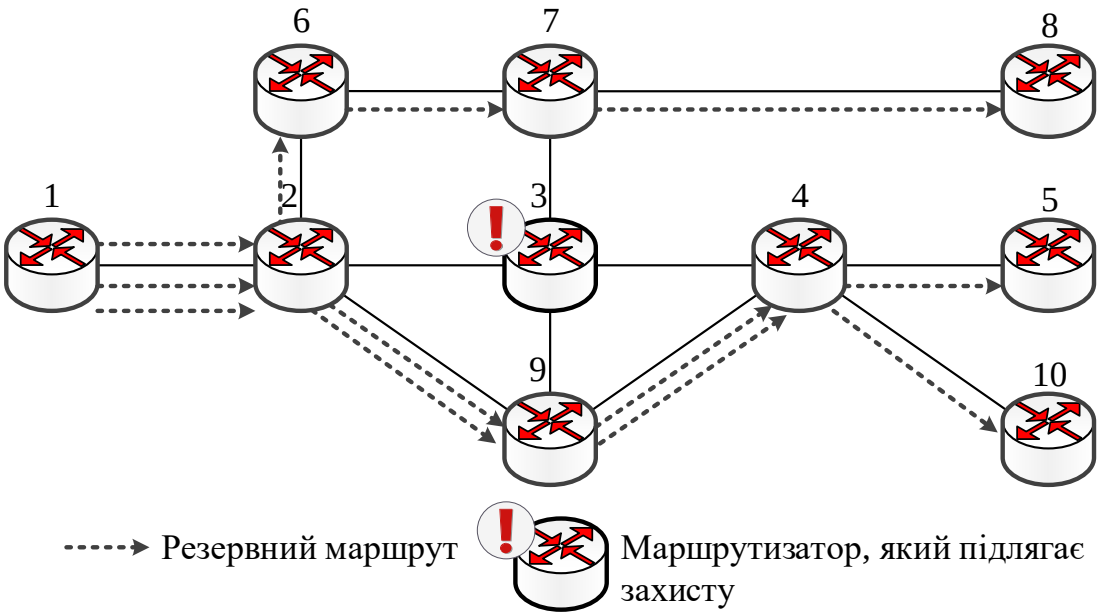


Рис. 2.11. Приклад визначення резервного шляху
під час захисту вузла з використанням схеми резервування 1:1

Застосування механізму спільного захисту продемонстровано для реалізації схеми резервування 1:*n* на рис. 2.12. У цьому випадку розраховується один резервний шлях для *n* основних шляхів і реалізується так звана схема *facility backup*, за рахунок чого підвищується масштабованість отримуваних рішень щодо відмовостійкої маршрутизації.

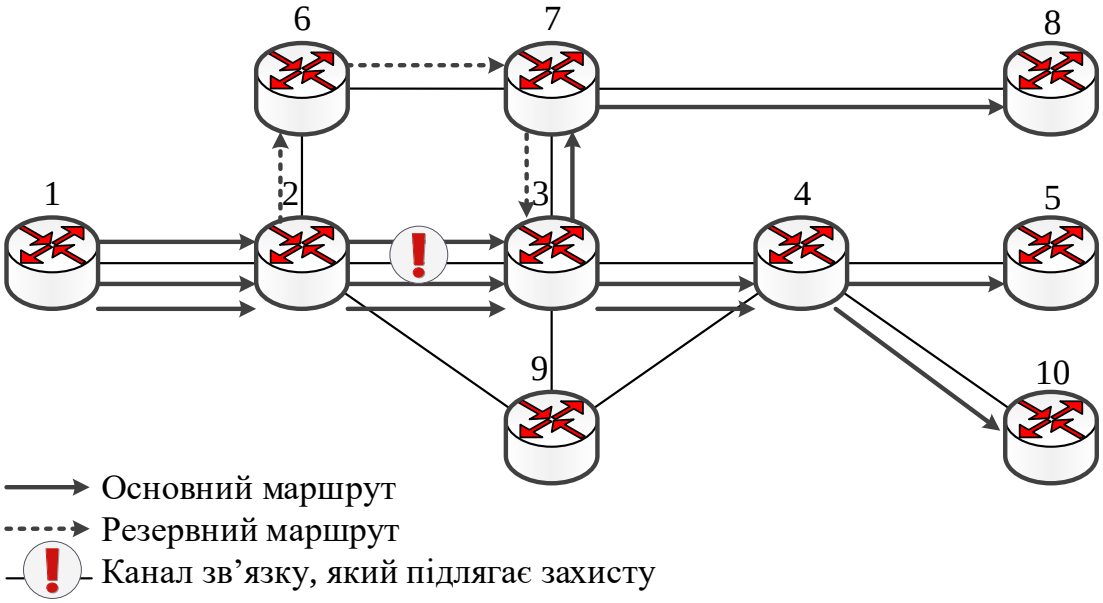


Рис. 2.12. Приклад захисту каналу зв'язку
за умови використання схеми 1:*n*

У випадку відмови вузла схема 1:*n* його захисту залежно від топології мережі може бути більш складною, що показано на рис. 2.13. Тут резервними (обхідними) є кілька каналів зв'язку, які є спільними елементами єдиного резервного маршруту для декількох основних.

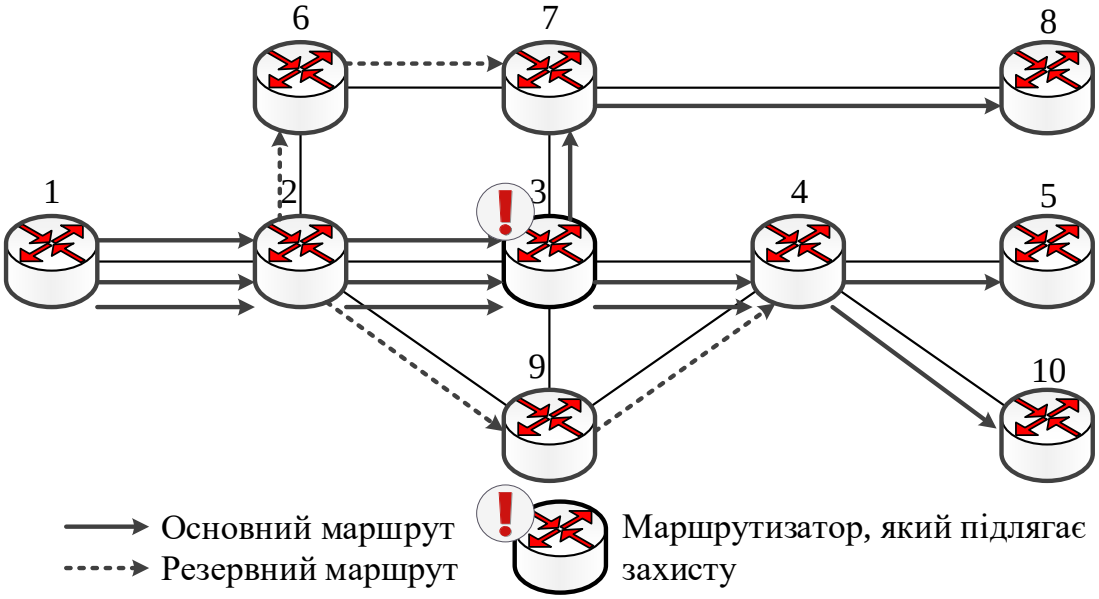


Рис. 2.13. Приклад захисту вузла в разі застосування схеми резервування 1:*n*

Отже, можна зробити висновок, що розглянуті протокольні рішення орієнтують на підвищення відмовостійкості мережі на підставі введення ресурсної надлишковості, пов'язаної з реалізацією тієї чи іншої схеми захисту елементів ІКМ. Тобто підвищення надійності ІКМ супроводжується необхідністю залучення додаткових обсягів канального та буферного ресурсу, що негативно впливає на продуктивність мережі загалом. Тому за умови відмовостійкої маршрутизації дуже важливо забезпечити збалансоване використання доступного мережного, насамперед канального, ресурсу, основане на ефективному балансуванні навантаження в ІКМ, щоб захист елементів мережі не призвів до її перевантаження та істотного зниження рівня QoS. Науково-практичному напряму реалізації швидкої перемаршрутизації з балансуванням навантаження в мережах MPLS (MPLS Traffic Engineering Fast ReRoute, MPLS TE FRR) також присвячено досить багато технологічних рішень [31, 32].

Як показав проведений аналіз [1, 3–6, 14–32], у процесі реалізації відмовостійкої маршрутизації в SDN виникають певні особливості. Зокрема залежно від місця розташування мережного елемента, який відмовив, ця проблема охоплює три основні площини: площину передачі даних; площину управління; площину комунікацій між елементами площин даних та

управління. Особливо гостро проблема забезпечення відмовостійкості постає на рівні інфраструктури через наявність на ньому великої кількості різнотипних мережних елементів (комутаторів, маршрутизаторів, шлюзів, каналів зв'язку тощо) і впливу широкого спектра чинників, що спричиняють відмови (рис. 2.1). Водночас важливо врахувати, що централізація функцій щодо управління трафіком у SDN негативно позначається на масштабованості протокольних рішень щодо відмовостійкої маршрутизації. Тому ці задачі в SDN зазнають певної модифікації як на рівні їх постановки, так і отримання кінцевого рішення, що й буде розглянуто в подальших підрозділах цієї роботи.

2.3. Аналіз моделей і методів відмовостійкої маршрутизації в ІКМ

Аналіз відомих рішень щодо відмовостійкої маршрутизації взагалі та швидкої перемаршрутизації зокрема [36–62] дозволив сформулювати перелік ключових вимог, яким повинні відповідати перспективні рішення в цій сфері і, насамперед, математичні моделі та методи, на яких вони ґрунтуються:

– урахування потокового характеру трафіку, що є відмінною рисою більшості мультимедійних послуг і обов'язковим моментом у реалізації схем захисту пропускної здатності та інших показників якості обслуговування в мережі;

– оптимізаційна постановка задачі: орієнтація на оптимізацію використання наявного мережного ресурсу;

– висока масштабованість рішень щодо відмовостійкої маршрутизації;

– підтримка базових схем захисту мережних елементів (вузла/каналу зв'язку/шляху/пропускної здатності);

– узгоджене вирішення окремих завдань відмовостійкої маршрутизації, наприклад, захист шлюзу за замовчуванням, швидка перемаршрутизація тощо;

– розширення можливостей наявних рішень щодо підтримки балансування навантаження, пов'язаних з реалізацією багатошляхової стратегії маршрутизації з відповідною підтримкою схем захисту не одного шляху, а мультишляху, тобто декількох шляхів, якими передаються пакети одного і того ж потоку;

– прийнятна обчислювальна складність рішень маршрутизації.

Серед евристичних алгоритмів відмовостійкої маршрутизації розглянемо найбільш вагомі, які були виокремлені під час проведеного аналізу робіт [36–46]. Так, у роботі [36] запропоновано адаптивний евристичний алгоритм відмовостійкої маршрутизації на основі використання графа (n, k)-зірки, який має широкі властивості щодо масштабованості. Автори реалізують ідею

зібрання інформації, яка використовується в процесі маршрутизації на графі n-зірки, для застосування на графі (n, k)-зірки $\left(S_{n,k}\right)$ (рис. 2.14).

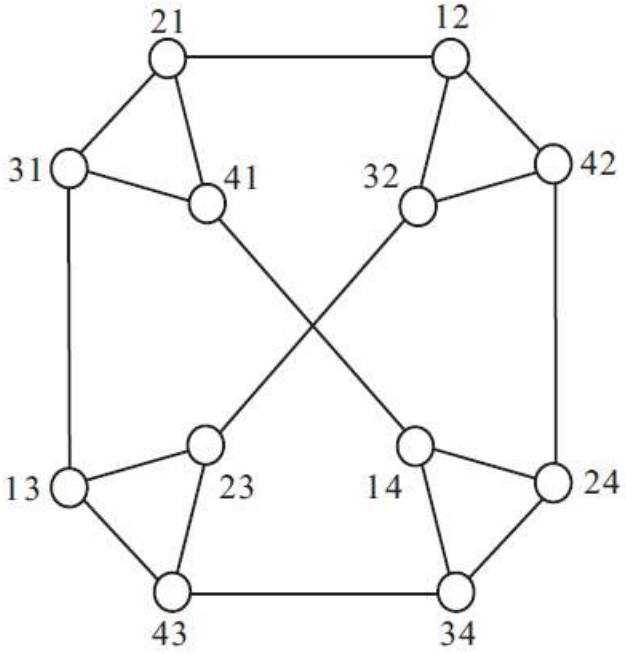


Рис. 2.14. Приклад графа (4, 2)-зірки $\left(S_{4,2}\right)$

У цьому випадку кожен вузол $S_{n,k}$ ідентифікується за допомогою перестановки k, вибраної з $\{1, 2, \ldots, n\}$, де n та k (якщо $1 \le k \le n-1$) є кількістю доступних для вибору та вибраних символів відповідно. Також авторами [36] запропоновано використання ймовірнісного вектора безпеки (Probabilistic Safety Vector, PSV) та розроблено алгоритм маршрутизації з метою визначення безвідмовного маршруту за допомогою PSV. Зазначимо, що ефективність маршрутизації PSV погіршується зі збільшенням відсотка вузлів, які відмовили, особливо за умови перевищення порогу відмов вузлів у 25 %. Для підвищення ефективності маршрутизації з більшим відсотком відмов вузлів також запропоновано адаптивний метод визначення порогу для PSV. Одночасно ефективність маршрутизації оцінювалася за середньою довжиною шляхів. Перевагами цього методу можна вважати його прийнятну обчислювальну складність.

У роботі [37] авторами запропоновано евристичний алгоритм відмовостійкої маршрутизації в mesh-мережах на основі мурашиного алгоритму пошуку оптимального шляху, коли враховуються вузли, що відмовили. У цьому випадку для розв'язання задачі відмовостійкої маршрутизації в запропонованому алгоритмі використовувався алгоритм оптимізації мурашиної колонії (Ant Colony Optimization, ACO) за умови застосування кольорових

феромонних мурах для подолання проблеми відновлення функціонування мережних елементів. Запропоноване рішення порівнювалося з алгоритмом відмовостійкої маршрутизації в mesh-мережах з використанням збалансованого кільця [37]. Результати моделювання показали, що запропонований алгоритм швидко реагував на відмови в мережі, щоб у кожний момент часу можна було вибрати оптимальний шлях від відправника до отримувача. Продуктивність алгоритму було підвищено за допомогою оновлень мурах з метою інформування інших вузлів про виявлений найкоротший шлях.

У праці [38] було запропоновано алгоритми відмовостійкої маршрутизації для ієрархічних дуальних мереж (Hierarchical Dual-Net, HDN) з обмеженою чи довільною кількістю вузлів, що відмовили. Зокрема HDN побудовано на основі симетричного графа, що називається базовою мережею, як тривимірного тора та *n*-вимірного гіперкуба. Наведені алгоритми дозволяють знайти маршрут без відмов між відправником та отримувачем за умови відомої множини вузлів, що відмовили.

У статті [39] авторами розроблено механізм швидкої перемаршрутизації в IP-мережах із використанням кістякових дерев із коренем, які не перетинаються за дугами, що гарантує відновлення від збоїв $(k-1)$ каналів зв'язку в мережі, яка описується *k*-реберно зв'язним графом. Оскільки кістякові дерева, які не перетинаються за дугами (рис. 2.15), можуть бути побудовані за час, пропорційний квадрату розміру мережі, запропонований підхід забезпечує високу масштабованість. Крім того, проведені експериментальні результати показали, що використання кістякових дерев, які не перетинаються за дугами, для відновлення після декількох відмов зменшує довжину шляху порівняно з раніше відомими методами.

Відомо, що інколи під час відмовостійкої маршрутизації виникає задача визначення шляху між двома вузлами в мережі, які повинні проходити через певні транзитні вузли. Наприклад, це може знадобитися у випадку, коли трафік, що передається, має бути проаналізований за допомогою глибокої перевірки пакетів з міркувань мережної безпеки на деякому специфічному вузлі мережі. Так, у статті [41] пропонується нова рекурсивна евристика для пошуку найкоротшого маршруту без циклів від вузла відправника до вузла отримувача, який відвідує певний набір транзитних вузлів у мережі. Для забезпечення стійкості до відмов уздовж шляху було запропоновано евристичний підхід, який модифікувався для того, щоб захистити розрахований шлях за допомогою відповідного резервного шляху, який не перетинається з основним за вузлами. Працездатність запропонованої евристики

в обчисленні шляху із захистом і без нього оцінювалася порівняно із розв'язанням цієї задачі методами цілочисельного лінійного програмування (Integer Linear Programming, ILP). У цьому випадку методи ILP можуть не отримати шукане рішення протягом заданого часу. Особливо це стосується мереж великої розмірності, що виправдовує необхідність розроблення саме евристичних алгоритмів.

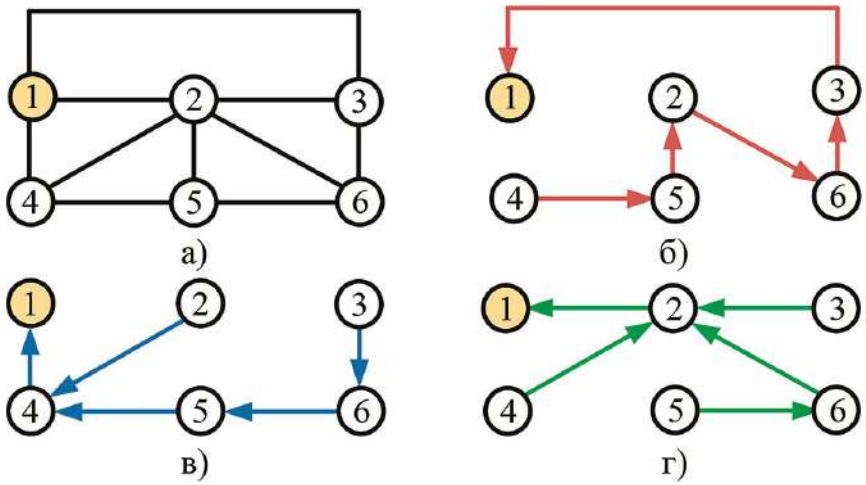


Рис. 2.15. Приклад дерев, які моделюють розв'язання задачі перемаршрутизації шляхами, що не перетинаються за каналами зв'язку:
а – мережа; б – червоне дерево; в – синє дерево; г – зелене дерево

Розглянемо ефективні графові та комбінаторні рішення щодо відмовостійкої маршрутизації, представлені в працях [47–52]. У роботі [47] запропоновано нові алгоритми відмовостійкої маршрутизації для гіперкубових мереж на основі приблизних маршрутних імовірностей (approximate routable probabilities), які характеризують доступність для маршрутизації будь-якого вузла на певній відстані. Кожен вузол вибирає один із сусідніх вузлів, щоб відправити повідомлення, беручи до уваги приблизні маршрутні ймовірності. Проведене авторами комп'ютерне моделювання підтвердило ефективність запропонованих алгоритмів [47].

Відомо, що вузли безпроводових сенсорних мереж (Wireless Sensor Networks, WSN) можуть швидко виходити з ладу, що призводить до відмов під час маршрутизації та блокування зв'язку. У свою чергу в роботі [48] запропоновано алгоритм відмовостійкої маршрутизації на основі використання структурованих орієнтованих графів де Брюйна (Fault-Tolerant Routing Based on the Structured Directional de Bruijn Graph, FTRSDDB) для підвищення ефективності маршрутизації для WSN. Алгоритм випадково розгортає деякі супервузли (super nodes) з великим запасом енергії та потужною

продуктивністю у WSN. Ці вузли відповідальні за збирання топологічної інформації з WSN для створення таблиці маршрутизації з резервуванням, а також для надання послуг передачі даних та маршрутизації для інших вузлів (popular nodes). Алгоритм FTRSDDB оптимізує топологічну структуру мережі, використовуючи граф де Брюйна, і може швидко знайти сусідні вузли, які відмовили, та недійсний маршрут, а потім обчислити новий маршрут з низькою умовною вартістю, що значно підвищує продуктивність відмовостійкої маршрутизації у WSN. Проведені експериментальні дослідження показали високу ефективність алгоритму FTRSDDB порівняно з іншими алгоритмами відмовостійкої маршрутизації (Gossiping, DD, Low Energy Adaptive Clustering Hierarchy (LEACH)), навіть в умовах атак шкідливих вузлів у WSN.

У дослідженні [49] було запропоновано модель відмовостійкої маршрутизації на основі графа зірки з векторами безпеки (безвідмовності). У цьому випадку використання вектора безпеки здатне забезпечувати ефективну відмовостійку маршрутизацію в ІКМ на основі шаблонів маршрутів. Виходячи з концепції шаблону маршрутів, спочатку визначається неорієнтований вектор безпеки. Крім того, авторами запропоновано кілька методів розв’язання задач щодо визначення довжини векторів безпеки та класифікації шаблонів маршрутів [49].

У працях [50, 51] було запропоновано моделі відмовостійкої маршрутизації на основі рівнів безпеки із застосуванням млинцевих графів та графів «гіперзірка». Крім того, було проведено порівняння таких типів графів, як «гіперзірка», «зірка», «гіперкуб» та «млинцевий граф» щодо ефективності їх використання за умови відмовостійкої маршрутизації.

У роботі [52] досліджено можливості застосування для підвищення відмовостійкості ІКМ циркулянтних графів, які забезпечують високу гнучкість щодо кількості вузлів та зв’язності мережі (рис. 2.16). Запропоновано архітектуру оптичної мережі на основі циркулянтного графа спільно з відмовостійкою маршрутизацією. Показано, що підвищення зв’язності мережі допомагає зменшити необхідну кількість використаних довжин хвиль для одночасної взаємодії між усіма вузлами. Також у [52] розроблено модель оцінки надійності з’єднання в разі відмови як вузлів, так і каналів зв’язку мережі. Зокрема із застосуванням запропонованого алгоритму надійність зростала майже лінійно із зростанням зв’язності мережі в логарифмічному масштабі.

Проте найбільш перспективними та ефективними є саме потокові моделі та методи відмовостійкої маршрутизації [4–6, 53–59], оскільки вони враховують потоковий характер трафіку, що передається в сучасних ІКМ.

У цьому випадку технологічна задача відмовостійкої маршрутизації формулюється в оптимізаційній формі, орієнтуючи на оптимізацію використання мережних ресурсів та допускаючи реалізацію схем захисту пропускної здатності мережі.

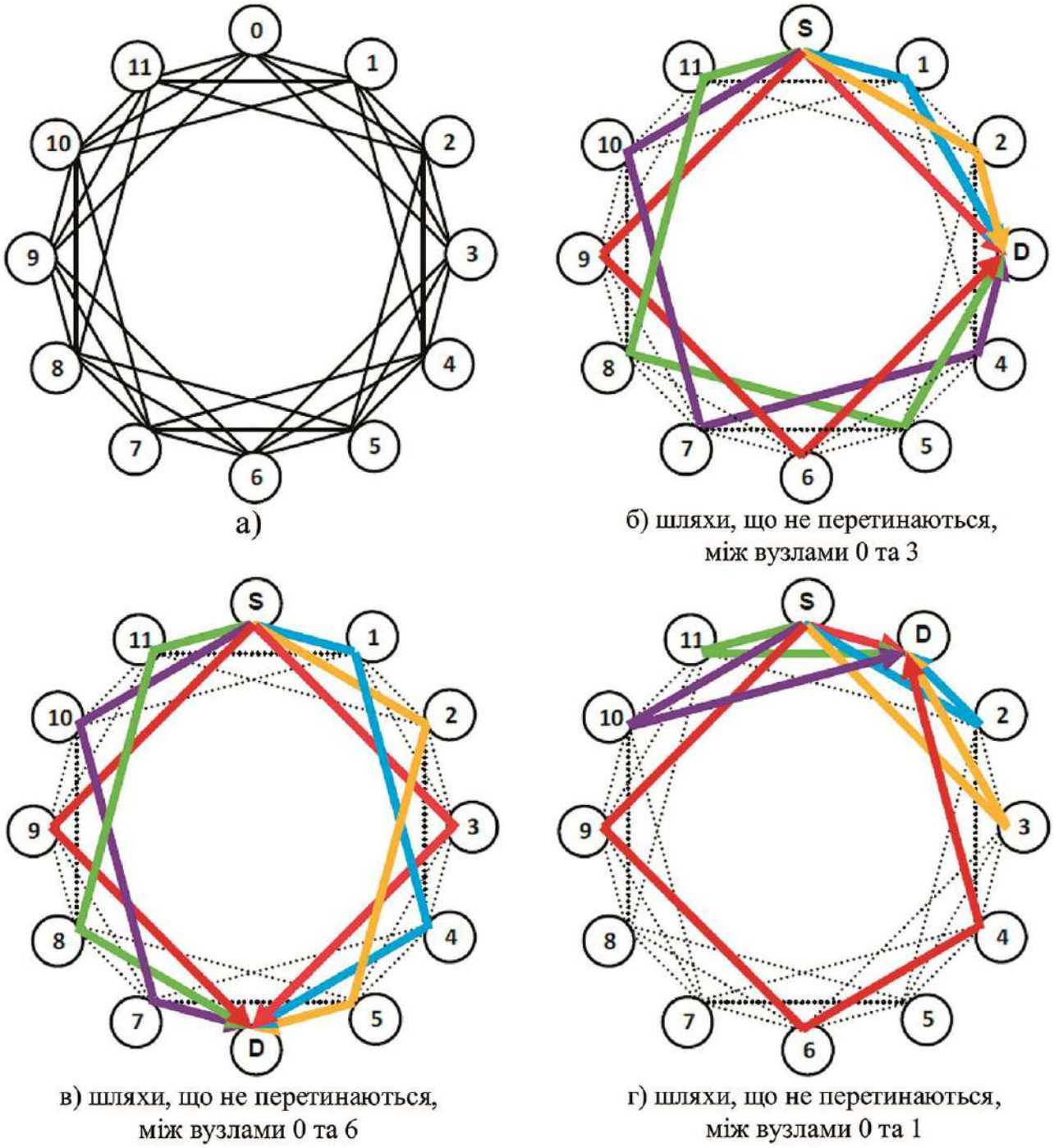


Рис. 2.16. Архітектура мережі на основі циркулянтного графа та приклади відмовостійкої маршрутизації шляхами, що не перетинаються за вузлами

Відомо, що основні та резервні шляхи у разі швидкої перемаршрутизації MPLS можуть бути визначені як найкоротші шляхи відповідно до умовної вартості каналів зв’язку або як явно розраховані довільні шляхи. В обох

випадках вибір маршруту можна оптимізувати таким чином, щоб максимальну завантаженість каналів зв'язку для множини розглянутих сценаріїв відмов було мінімізовано. У статті [53] авторами запропоновано лінійну оптимізаційну модель для розрахунку шляхів як у випадку реалізації одношляхової стратегії маршрутизації, так і за умови багатошляхової маршрутизації з метою забезпечення балансування навантаження. Отримані авторами результати щодо завантаженості каналів зв'язку у використанні запропонованої лінійної моделі під час одношляхової та багатошляхової маршрутизації було порівняно з відповідними значеннями для шляхів, розрахованих згідно зі стандартними процедурами для IP-мереж, що дозволило визначити виграш у використанні мережних ресурсів.

У свою чергу робота [54] присвячена вирішенню завдання мінімізації споживання енергії у відмовостійких ІКМ. У використанні підходу, запропонованого авторами, для кожного запиту має бути надана пара шляхів (основний та резервний), що не перетинаються за каналами зв'язку, і використовується спільна схема захисту (резервування). Споживання енергії здійснюється лише тими каналами зв'язку, що використовуються за відсутності відмов, але мережний ресурс задіюється як основним, так і резервним шляхами. Отже, автори [54] пропонують механізм спільного захисту (*shared protection*), який не залежить від відмов, у разі MPLS-маршрутизації, а сформульована задача носить назву *спільного захисту за умови вдосконаленого трафік-інжинірингу* (*Shared protection Smart Traffic Engineering, SSTE*). Зокрема задача SSTE є *NP*-складною, оскільки містить задачу визначення дерев Штейнера. Проте в роботі [54] наведено формулювання цієї задачі за Бендерсом, яке є набагато ефективнішим з обчислювальної точки зору.

У праці [55] запропоновано алгоритми розрахунку шляхів для відмовостійкої маршрутизації, які не перетинаються за вузлами та проходять через задані вузли. Задача розрахунку найкоротшого шляху, що проходить через задану множину вузлів, має принаймні таку ж складність, як і задача комівояжера, тому в літературі їй не було приділено значної уваги. Незважаючи на це, нещодавно було запропоновано ефективне формулювання цієї задачі як задачі ILP. Це формулювання, по-перше, адаптоване під включення обмеження, яке гарантує, що отриманий шлях може бути захищений за допомогою резервного шляху, який не перетинається з основним за вузлами, а по-друге, має бути отримана така пара основного та резервного шляхів, які не перетинаються за вузлами та мають мінімальну вартість за умови, що кожен з них повинен проходити через певний набір заданих вузлів.

Проте обчислювальні експерименти показали, що зазначені підходи у масштабних мережах можуть не дозволити розв'язати задачу відмовостійкої маршрутизації протягом заданого часу. Тому для її розв'язання автори запропонували евристику, яка здатна знайти рішення в більшості випадків. Крім того, отримані рішення мають прийнятну відносну похибку стосовно вартості отриманого шляху або пари шляхів, а процесорний час, який потребує евристика, значно менший за час, який вимагає вирішувач ILP.

У дослідженні [56] представлено рішення щодо розподілу резервної пропускної здатності (*Spare Capacity Allocation, SCA*) у використанні спільного резервного захисту шляху за умови подвійних відмов каналів зв'язку (*dual link failures*). Ця робота розширює застосування задачі SCA в IP mesh-мережах та WDM. Отже, у розв'язанні задачі SCA потоки пакетів попередньо розподіляються за одним робочим і двома резервними шляхами, що взаємно не перетинаються, використовуючи схему спільного резервного захисту шляху (*Shared Backup Path Protection, SBPP*). Метод матричного резервного забезпечення (*Spare Provision Matrix, SPM*) агрегує інформацію щодо кожного потоку та обчислює загальну вільну пропускну здатність для подвійних відмов каналів зв'язку. Цей метод має достатню масштабованість і гнучкість. Задача SCA сформульована як задача нелінійного цілочисельного програмування і розділена на дві послідовні лінійні підзадачі: одна дозволяє знайти всі первинні резервні шляхи, а інша знаходить всі вторинні резервні шляхи. Авторами розширено термінологію у захисті каналів 1+1 та 1:1 для захисту резервного шляху. Крім того, у роботі показано, що вдосконалений евристичний алгоритм успішної безвідмовної маршрутизації (*Successive Survivable Routing, SSR*) для випадку подвійних відмов добре масштабується в мережах великого розміру.

Використання резервних шляхів є загальною методикою забезпечення захисту в разі відмови елементів ІКМ (вузлів/каналів зв'язку/шляхів тощо). Однак обчислення відповідних множин основних і резервних шляхів, що не перетинаються, потребує значного часу, використовуючи доступні алгоритми (наприклад, підхід Бхандарі [57]). Це, у свою чергу, може значно вплинути на здатність мережі обслуговувати динамічні потоки (тобто ті, що характеризуються відносно короткою тривалістю надання послуги). Щоб забезпечити вирішення цієї проблеми, у роботі [57] запропоновано підхід щодо попереднього обчислення множини шляхів, які не перетинаються, з метою отримання можливості обслуговування потоків одразу після їх надходження в мережу. Цей підхід оснований на спостереженні, що задача обчислення множини шляхів, які не перетинаються за вузлами, еквівалентна

задачі визначення «найдешевшого» циклу топології мережі, що проходить через вузли відправника та отримувача відповідного потоку. Зокрема авторами [57] запропоновано узагальнення цієї схеми, якщо припустити, що будь-яка пара шляхів, які не перетинаються за вузлами, може бути отримана шляхом об'єднання базових циклів, визначених для топології мережі (рис. 2.17).

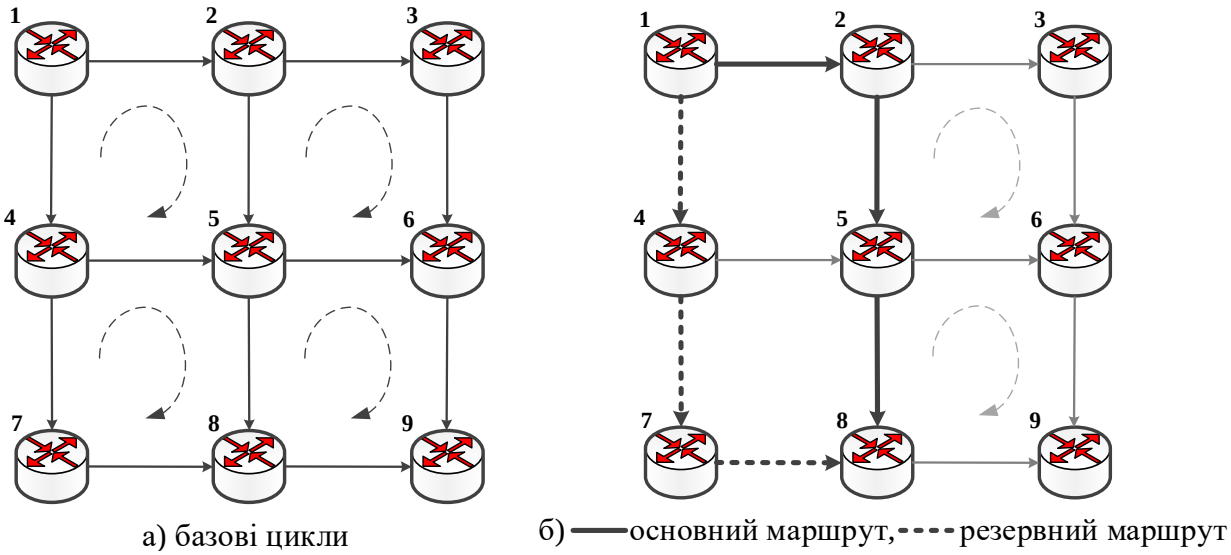


Рис. 2.17. Ілюстрація основної ідеї схеми попереднього розрахунку основного та резервного шляхів, що не перетинаються

У [57] вводиться новий метод для розрахунку «найдешевших» циклів на основі так званих базових циклів, що, як підтверджено для реальних мережних топологій, зменшує до 70 % часу, необхідного для встановлення шляхів, що не перетинаються за вузлами (порівняно з результатами, отриманими за схемою Бхандарі).

На сьогоднішній день ІКМ мають гарантувати, що всі вузлові пари, які беруть участь у комунікаціях критичних інфраструктур, мають високу доступність. Як правило, лише невелика частка трафіку та користувачів потребує високого рівня доступності, але саме такий тип трафіку вимагає перегляду мережних рішень у проектуванні відмовостійких ІКМ. У статтях [58, 59] запропоновано новий підхід до вирішення завдання ефективного забезпечення високого рівня міжкінцевої доступності, а саме використання концепції спайна. Основна ідея полягає в тому, щоб ввести високодоступну множину каналів зв'язку та вузлів, так званий *спайн* (*spine*), у топології мережі та відповідний захист і маршрутизацію з метою надання диференційованих класів відмовостійкості з різним рівнем доступності. У роботі [58] досліджено саму концепцію спайна на прикладі, що ілюструє потенційні переваги цього підходу. Також було показано, як структурні властивості топології мережі можуть бути

використані для визначення евристики у виборі відповідного спайна та порівняні з випадком, коли всі мережні компоненти мають однакову доступність.

Концепція застосування спайнів показана на наступному прикладі. Нехай повнозв'язна мережа, представлена графом (рис. 2.18), містить чотири вузли та шість каналів зв'язку. Зокрема для кожного l-го каналу зв'язку відома його метрика доступності a_l, яка змінюється в межах від 0 до 1 [58]. У цьому прикладі обрано спайн, що містить канали зв'язку 1→2, 1→3 та 1→4, які мають вищі значення метрики доступності a_1, a_5 та a_4 відповідно.

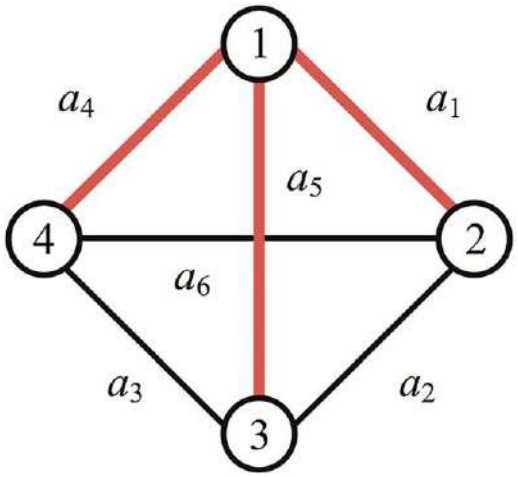


Рис. 2.18. Приклад мережі з повнозв'язною топологією
та обраного спайна на ній

Таким чином, доступність основного маршруту (*working path, WP*) для потоку, що передається, визначається за виразом [58]

$$A^{WP} = \prod_{l \in WP} a_l .$$

Аналогічно цій формулі визначається доступність резервного маршруту A^{BP} (*backup path, BP*). Тоді як доступність мережі для потоку, що передається, можна отримати таким чином [58]:

$$A = 1 - \left(1 - A^{WP}\right)\left(1 - A^{BP}\right).$$

Подібні результати є важливим кроком на шляху оптимального проектування фізичної мережі для підтримки методів захисту (резервування) для досягнення високого рівня доступності елементів ІКМ.

Далі задача ефективного забезпечення високого рівня міжкінцевої доступності під час передачі потоків між вузлами ІКМ формулювалася у вигляді оптимізаційної за умови використання різних критеріїв оптимальності:

– максимізація суми доступностей основних шляхів для всіх потоків;

– максимізація мінімального рівня доступності основних шляхів для всіх потоків.

У дослідженнях останніх років велика увага приділяється концепції надання диференційованих класів відмовостійких послуг через ІКМ. У деяких випадках учені намагалися вирішити ці завдання шляхом створення множини категорій послуг із різними схемами захисту. Проте більшість з них орієнтовані на застосування в однорангових мережах та не мають узгодженої міжрівневої координації в багаторівневих (ієрархічних) сценаріях. Крім того, зростає потреба в наданні послуг з високими вимогами до відмовостійкості в мережах майбутнього. Це, однак, має бути зроблено економічно ефективним способом і без надмірної складності. У статті [59] запропоновано вдосконалення попереднього підходу на основі спайнів, який дозволяє спростити синтез необхідного механізму та забезпечує як високу відмовостійкість, так і її диференціацію. Отже, цей підхід використовує ідею концепції спайна щодо введення підмереж на фізичному рівні з відносно високою доступністю каналів зв’язку та вузлів [58]. Це створює основу для диференціації відмовостійкості між різними класами потоків. Потім міжрівневе відображення та маршрутизація з урахуванням спайна виконуються таким чином, щоб інформація щодо здатності диференціювання передавалася на верхній рівень. Крім того, у [58] запропоновано два оптимізаційних формулювання задачі маршрутизації та відображення, а також оцінено їх ефективність у багаторівневому сценарії.

Серед досліджень щодо відмовостійкості в SDN можна виокремити роботи [5, 12, 60–62]. Так, наприклад, у [60] наведено алгоритм локальної швидкої перемаршрутизації (*Local Fast Reroute*, *LFR*) з агрегацією потоків у програмно-конфігурованих мережах. В алгоритмі LFR у разі виявлення відмови каналу зв’язку всі потоки трафіку, вражені відмовою, агрегуються у так званий «великий» потік. Далі локальний резервний шлях для перемаршрутизації динамічно розгортається контролером SDN для агрегованого потоку. Таким чином, алгоритм LFR зменшує кількість поточних операцій між контролером SDN та комутаційним обладнанням. Отримані результати довели, що LFR забезпечує швидке відновлення, мінімізуючи загальну кількість потоків у SDN.

Зростання складності сучасних мережних застосунків та величезний попит на інтернет-ресурси вимагають від інфраструктур ІКМ здатності адаптуватися до вимог високого ступеня робастності та надійності. Як було сказано вище, у SDN надзвичайно актуальним є саме завдання підвищення відмовостійкості та вчасного оновлення інформації про стан мережі, яким присвячено дослідження [61]. У ньому визначені нові алгоритми,

спрямовані на покращення пошуку резервних шляхів у мережах великої розмірності в разі одиночних відмов каналів зв'язку з мінімальними часовими витратами на оновлення інформації про стан мережі. Нове рішення спрямоване на підвищення ефективності та зменшення операцій з оброблення службової інформації під час відмов каналів зв'язку.

Також слід відзначити, що забезпечення узгодженого вирішення завдань балансування навантаження та відмовостійкої маршрутизації (наприклад, MPLS TE FRR) найчастіше призводить до підвищення обчислювальної складності та зниження масштабованості протокольних рішень. Відомо, що ефективність протокольного рішення багато в чому визначається адекватністю та якістю покладеної в його основу математичної моделі розрахунку. Як показав проведений аналіз [63], порядок FRR і TE визначається під час розв'язання оптимізаційних задач різного рівня складності. У цьому випадку реалізація схеми захисту пропускної здатності мережі, як правило, призводить до нелінійного формулювання оптимізаційної задачі та відповідного зростання обчислювальної складності отримуваних рішень.

2.4. Система потокових моделей відмовостійкої маршрутизації без резервування елементів ІКМ

Важливе місце з точки зору підвищення відмовостійкості ІКМ відводиться засобам багатошляхової маршрутизації, коли для доставки пакетів того чи іншого потоку одночасно використовується не один шлях, а множина маршрутів. Зокрема в роботах [64–67] запропоновані маршрутні рішення, орієнтовані на використання шляхів, що не перетинаються, тобто в яких спільними є тільки вузли відправника та отримувача пакетів. Використання маршрутів, які не перетинаються, гарантує, що відмова (вихід з ладу, перевантаженя або компрометація) одного елемента (вузла або каналу) мережі спричинить відмову лише одного, а не декількох маршрутів [64, 66], що має місце в разі маршрутизації шляхами, які перетинаються. Як показав проведений аналіз [64–67, 68, 69], перспективні теоретичні рішення в цьому напрямі мають забезпечувати:

– урахування особливостей як структури мережі, параметрів каналів зв'язку, так і характеристик трафіку, що передається;

– підтримку мультипотоковості, тобто модель має описувати порядок маршрутизації не одного, а одночасно декількох потоків з урахуванням їх взаємного впливу;

– контроль за можливим перевантаженням елементів мережі за рахунок виконання умов збереження потоку у вузлах мережі та запобігання перевантаження каналів зв'язку.

2.4.1. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що не перетинаються

Введемо наступні позначення, які є актуальними для всього другого розділу роботи. Припустимо, що структуру ІКМ описує граф $\Gamma = (R, E)$, в якому $R = \{R_i; i = \overline{1,m}\}$ – це множина вершин, що моделюють маршрутизатори, а $E = \{E_{i,j}; i, j = \overline{1,m}; i \neq j\}$ – множина дуг, які представляють канали зв'язку в ІКМ. Тоді $|E| = n$ визначає кількість каналів зв'язку в ІКМ. Кожну дугу $E_{i,j} \in E$ зважимо пропускною здатністю $\varphi_{i,j}$ відповідного каналу зв'язку. Також нехай s_k і d_k – вузол-відправник і вузол-отримувач пакетів k-го потоку відповідно, а λ^k – середня інтенсивність пакетів k-го потоку з множини K. Керуючою змінною є величина $x_{i,j}^k$, яка характеризує частку k-го потоку, що передається каналом зв'язку $E_{i,j} \in E$.

У синтезі потокової моделі багатошляхової маршрутизації шляхами, що не перетинаються, за основу були прийняті введені в підрозділі 1.7 умови збереження потоку (1.3), реалізації багатошляхової стратегії маршрутизації (1.2) та відсутності перевантаження каналів зв'язку ІКМ (1.4). Як приклад у розв'язанні маршрутної задачі буде мінімізуватися лінійна цільова функція такого вигляду:

$$J = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k , \qquad (2.1)$$

де $c_{i,j}^k$ – метрика каналу зв'язку між i-м та j-м вузлами ІКМ.

Розглянемо випадок, коли в мережі необхідно реалізувати багатошляхову маршрутизацію шляхами, що не перетинаються, з можливістю регулювання кількості використовуваних маршрутів, як це зроблено, наприклад, у роботах [64, 66]. Під час проведеного дослідження встановлено, що в разі багатошляхової маршрутизації шляхами, які не перетинаються, необхідно, щоб виконувалося таке припущення (гіпотеза): у кожен транзитний вузол потік повинен входити не більше ніж за одним каналом зв'язку і, відповідно, виходити також не більше ніж за одним вихідним КЗ. За наведеною гіпотезою

в позначеннях базової моделі (1.2)–(1.4) для всіх вхідних інтерфейсів i-го транзитного вузла повинні виконуватися такі умови [70]:

$$\sum_{j:E_{j,i}\in E}\ \sum_{\substack{l:E_{l,i}\in E,\\ l\neq j}} x_{j,i}^{k}x_{l,i}^{k}=0, \tag{2.2}$$

а для всіх вихідних інтерфейсів i-го транзитного вузла мережі мають бути справедливими такі рівності:

$$\sum_{n:E_{i,n}\in E}\ \sum_{\substack{m:E_{i,m}\in E,\\ m\neq n}} x_{i,n}^{k}x_{i,m}^{k}=0. \tag{2.3}$$

Виконання умов (2.2) та (2.3) гарантує, що потік, який проходить через i-й транзитний вузол, надходить не більше ніж від одного суміжного вузла і передається не більше ніж одному суміжному вузлу. Тобто відбувається формування множини шляхів, що не перетинаються, у яких спільними є тільки вузли відправника та отримувача. З огляду на нелінійність умов (2.2) та (2.3) оптимізаційна задача, пов'язана з мінімізацією виразу (2.1) в разі лінійних обмежень (1.2)–(1.4), належить до класу задач нелінійного програмування.

Для забезпечення регулювання числа використовуваних шляхів, які не перетинаються, у реалізації багатошляхової маршрутизації кожного k-го потоку позначимо через M_{UB}^{k} верхнє граничне значення (Upper Bound) кількості шляхів, що не перетинаються, яке визначається через степінь вершин, що моделюють вузли відправника й отримувача, тобто кількістю інцидентних цим вершинам дуг (каналів зв'язку) [70]:

$$M_{UB}^{k}=\min\left(\xi\left(s_k\right),\xi\left(d_k\right)\right), \tag{2.4}$$

де $\xi\left(s_k\right)$ – степінь вершини (вузла) відправника k-го потоку;

$\xi\left(d_k\right)$ – степінь вершини (вузла) отримувача k-го потоку.

Фактично використовуване число M^{k} шляхів, що не перетинаються, у процесі маршрутизації k-го потоку, застосовуючи модель (1.2)–(1.4), (2.1)–(2.4), за аналогією з виразом (2.4) можна розрахувати таким чином [70]:

$$M^{k}=\sum_{j:E_{i,j}\in E}\left\lceil x_{i,j}^{k}\right\rceil \ \text{ або }\ M^{k}=\sum_{n:E_{n,m}\in E}\left\lceil x_{n,m}^{k}\right\rceil \ \text{ при }\ R_i=s_k,\ R_m=d_k, \tag{2.5}$$

де $\sum_{j:E_{i,j}\in E}\left\lceil x_{i,j}^{k}\right\rceil$ – кількість вихідних інтерфейсів, за якими k-й потік виходить з вузла-відправника;

$\sum_{n:E_{n,m}\in E} \left\lceil x_{n,m}^{k} \right\rceil$ – кількість вхідних інтерфейсів, за якими k-й потік надходить до вузла-отримувача.

Величина M^k може бути як оцінюваним параметром, так і керованою величиною, тобто за її допомогою можна задавати мінімальне, максимальне або визначати задане (оптимальне) число використовуваних шляхів, що не перетинаються, у реалізації багатошляхової маршрутизації. Межі зміни цієї величини визначаються за допомогою нерівності

$$1 \le M^k \le M_{UB}^k. \qquad (2.6)$$

Проведено перевірку працездатності (адекватності) запропонованої потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що не перетинаються, з регулюванням числа використовуваних маршрутів на множині мережних структур. Як приклад розглянемо структуру мережі, що складалася з 12 вузлів і 25 каналів зв'язку (рис. 2.19). У цьому випадку вузлами «відправник–отримувач» були перший і дванадцятий вузли відповідно. Пропускна здатність кожного з каналів зв'язку, для прикладу, дорівнювала 100 пакетам за секунду (1/с).

Спочатку проаналізуємо результат рішення, отримуваний у разі використання базової потокової моделі (1.2)–(1.4), (2.1), коли метрика каналів зв'язку дорівнювала одиниці $\left(c_{i,j}^k = 1\right)$. Нехай між парою вузлів «відправник–отримувач» передавався потік пакетів інтенсивністю 300 1/с. Кінцевий порядок багатошляхової маршрутизації, отриманий на основі моделі (1.2)–(1.4), (2.1), наведено на рис. 2.19, де в розриві того чи іншого каналу зв'язку зображено інтенсивність потоку, що протікає по ньому. Аналіз рис. 2.19 показав, що базова модель (1.2)–(1.4), (2.1) забезпечує розрахунок множини маршрутів, які перетинаються як за вузлами, так і за каналами зв'язку. Для зручності незадіяні в маршрутизації канали зв'язку зображені на рис. 2.19 штриховою лінією.

Далі проведемо розв'язання задачі багатошляхової маршрутизації, але вже шляхами, що не перетинаються, тобто з урахуванням сформульованих умов (2.2) і (2.3). Результат розрахунку за умови тих самих вихідних даних показано на рис. 2.20, який представлено такими трьома $\left(M^k = 3\right)$ шляхами, що не перетинаються: $R_1 \to R_2 \to R_5 \to R_9 \to R_{12}$, $R_1 \to R_3 \to R_7 \to R_{10} \to R_{12}$ і $R_1 \to R_4 \to R_8 \to R_{11} \to R_{12}$. За кожним з цих шляхів передається потік інтенсивністю 100 1/с.

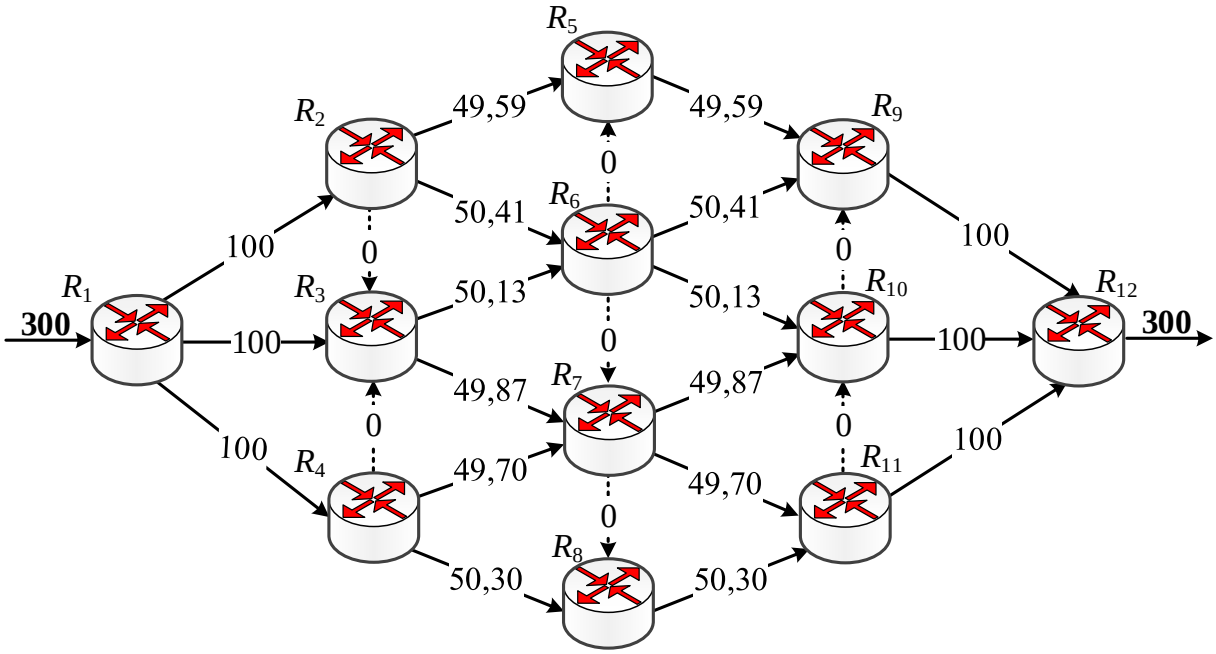


Рис. 2.19. Результат розрахунку множини шляхів
з використанням базової моделі (1.2)–(1.4), (2.1)
для обслуговування потоку інтенсивністю 300 1/с

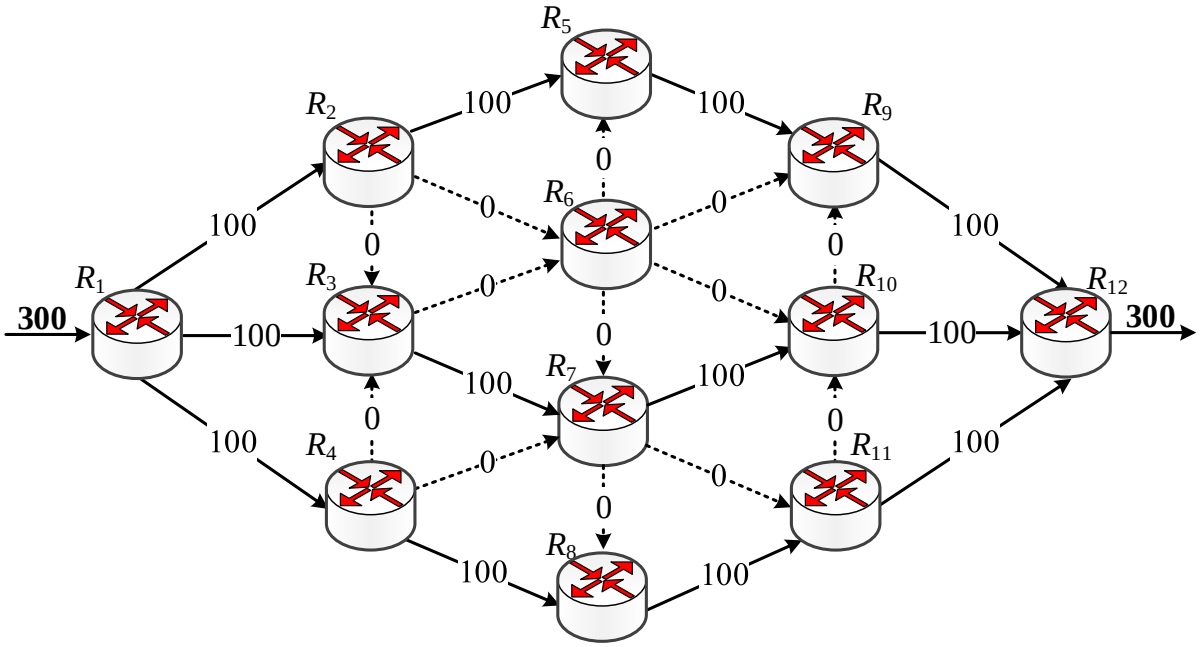


Рис. 2.20. Результат розрахунку множини шляхів з використанням
умов маршрутизації (2.2) і (2.3) шляхами, що не перетинаються,
для обслуговування потоку інтенсивністю 300 1/с

Змінимо дещо вихідні дані: нехай на вхід мережі надходить потік інтенсивністю 100 1/с, а $M^k = 2$, якщо $M^k_{UB} = 3$, тобто умова (2.6) виконується. Тоді використання моделі (1.2)–(1.4), (2.1)–(2.6) визначило порядок маршрутизації

потоків в ІКМ, представлений на рис. 2.21. Шляхи $R_1 \to R_2 \to R_5 \to R_9 \to R_{12}$ і $R_1 \to R_4 \to R_7 \to R_{10} \to R_{12}$ також не перетинаються.

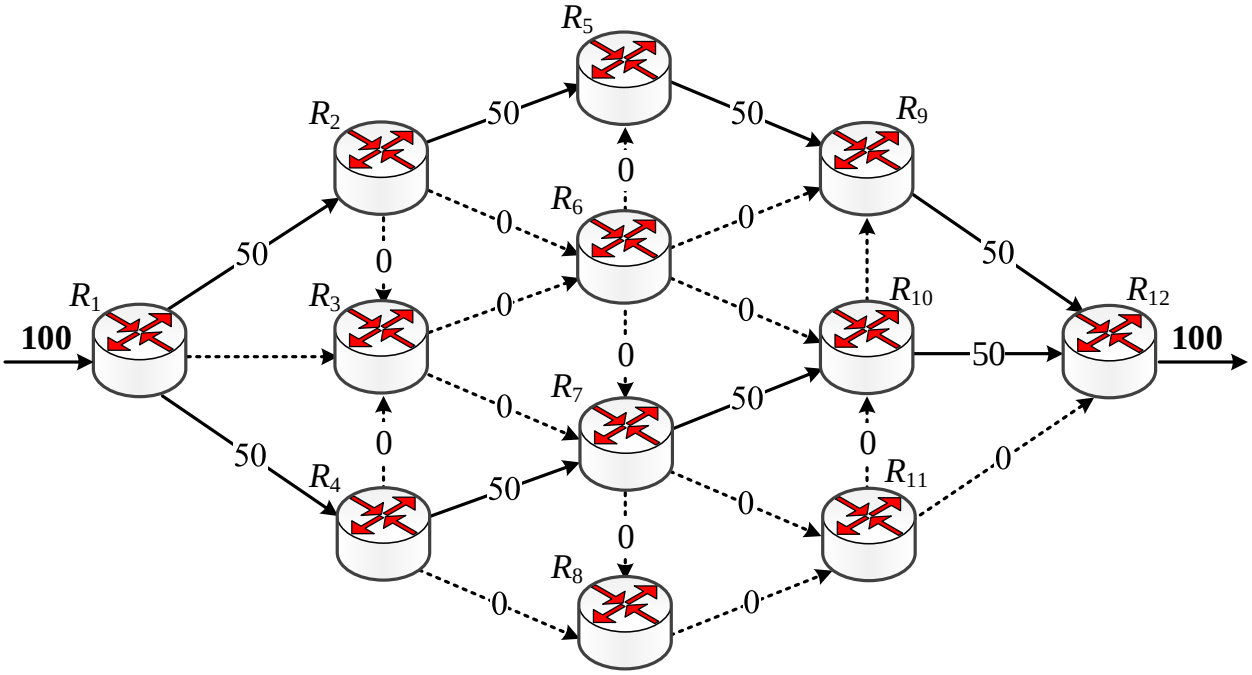


Рис. 2.21. Результат розрахунку множини шляхів з використанням умов (2.2), (2.3) і (2.6) для обслуговування потоку інтенсивністю 100 1/с $\left(M^k = 2\right)$

Отже, результати дослідження підтвердили працездатність та адекватність запропонованої потокової моделі багатошляхової маршрутизації шляхами, що не перетинаються, з регулюванням кількості використовуваних маршрутів у різних умовах зміни характеристик потоків.

Модель може забезпечувати отримання необхідних рішень також з іншими маршрутними метриками, які входять до критерію оптимальності (2.1), або з іншими критеріями оптимальності, наприклад (1.15), за умов (1.13), що позначиться як на характері визначених маршрутів, так і на порядку балансування навантаження цими шляхами.

2.4.2. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що перетинаються за вузлами

Варто окремо зазначити, що реалізація багатошляхової маршрутизації шляхами, що не перетинаються, як правило, не сприяє збалансованому використанню доступного мережного (канального) ресурсу, що негативно позначається на продуктивності ІКМ та рівні якості обслуговування загалом.

Пошук компромісу в питанні забезпечення відмовостійкості ІКМ, з одного боку, та якості обслуговування, з іншого, призвів до того, що в деяких важливих випадках вимоги щодо перетинання використовуваних шляхів можна дещо знизити і застосовувати шляхи, які допускають перетин, наприклад, лише за вузлами ІКМ. У таких маршрутах спільними є не тільки вузли «відправник» та «отримувач», але й деякі транзитні вузли, проте вони не містять спільних каналів зв'язку. Це є особливо актуальним для безпроводових мереж, в яких радіоканали більш схильні до перевантаження та/або компрометації переданих даних на фізичному рівні EMBBC [64, 65]. Тобто в таких випадках, коли до відмов схильні саме канали зв'язку, а не вузли ІКМ, доцільно використовувати маршрути, що перетинаються лише за вузлами, бо це може призвести до підвищення продуктивності мережі із забезпеченням того ж рівня відмовостійкості, що й за умови задіяння маршрутів, які не перетинаються взагалі.

Розглянемо випадок, коли в ІКМ необхідно реалізувати багатошляхову маршрутизацію за шляхами, що перетинаються за вузлами. У межах цієї моделі необхідно, щоб виконувалося таке припущення (гіпотеза) для всіх вхідних і вихідних інтерфейсів i-го транзитного вузла, які використовуються: кожен вхідний потік заданої інтенсивності також повинен відповідати вихідному потоку такої ж інтенсивності [71, 72]:

$$\sum_{m=1}^{N_{in}} \prod_{n=1}^{N_{out}} x_{m,i}^{k} \left(x_{m,i}^{k} - x_{i,n}^{k} \right) = 0, \qquad (2.7)$$

де N_{in} – кількість вхідних інтерфейсів i-го транзитного вузла;

N_{out} – кількість вихідних інтерфейсів i-го транзитного вузла.

Крім того, має бути виконана протилежна умова: кожен вихідний потік заданої інтенсивності повинен відповідати вхідному потоку з тією ж інтенсивністю [71, 72]:

$$\sum_{n=1}^{N_{out}} \prod_{m=1}^{N_{in}} x_{i,n}^{k} \left(x_{i,n}^{k} - x_{m,i}^{k} \right) = 0. \qquad (2.8)$$

Виконання нелінійних умов (2.7) та (2.8) гарантує, що потоки, які передаються через i-й транзитний вузол, надходять з однієї і тієї ж кількості сусідніх вузлів, які передаються іншим суміжним вузлам з однаковою інтенсивністю. Таким чином, формується множина шляхів, що мають не тільки спільну пару вузлів «відправник» та «отримувач», а також використовують спільні транзитні вузли. Можливість регулювання кількості використовуваних

маршрутів, як це зроблено в пункті 2.4.1, може бути застосована і для випадку шляхів, що перетинаються за вузлами.

Нехай необхідно розв'язати задачу багатошляхової маршрутизації шляхами, що перетинаються за вузлами. Для розв'язання задачі з використанням запропонованої потокової моделі як ІКМ застосовувалася мережа з восьми вузлів і 15 каналів зв'язку, що показано на рис. 2.22. Вузлами «відправник–отримувач» були перший і восьмий вузли відповідно. У розривах каналів зв'язку вказана їх пропускна здатність, яка вимірюється в пакетах за секунду (1/с) (рис. 2.22).

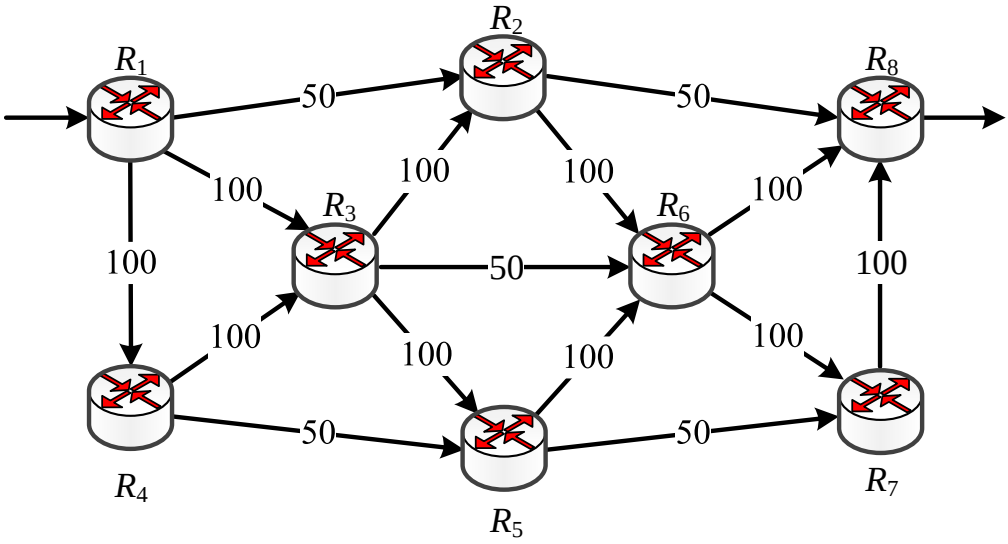


Рис. 2.22. Структура досліджуваної ІКМ

Для наочності розглянемо приклад, коли під час багатошляхової маршрутизації мінімізується кількість переприйомів пакетів на вузлах, тобто $c_{i,j}=1$. Тоді максимальна продуктивність напрямку зв'язку між першим та восьмим вузлами ІКМ у разі реалізації багатошляхової маршрутизації шляхами, що перетинаються за вузлами, буде становити 250 1/с (рис. 2.23). На рис. 2.23 в розриві того чи іншого каналу зв'язку зображена інтенсивність потоку, який протікає за ним. Незадіяні під час маршрутизації канали показані штриховою лінією.

Таким чином, за умови передачі потоку інтенсивністю 250 1/с отримана множина маршрутів містить такі три $\left(M^k=3\right)$ шляхи:

$R_1 \to R_2 \to R_8$,

$R_1 \to R_3 \to R_2 \to R_6 \to R_8$,

$R_1 \to R_4 \to R_3 \to R_5 \to R_6 \to R_7 \to R_8$, що перетинаються за вузлами.

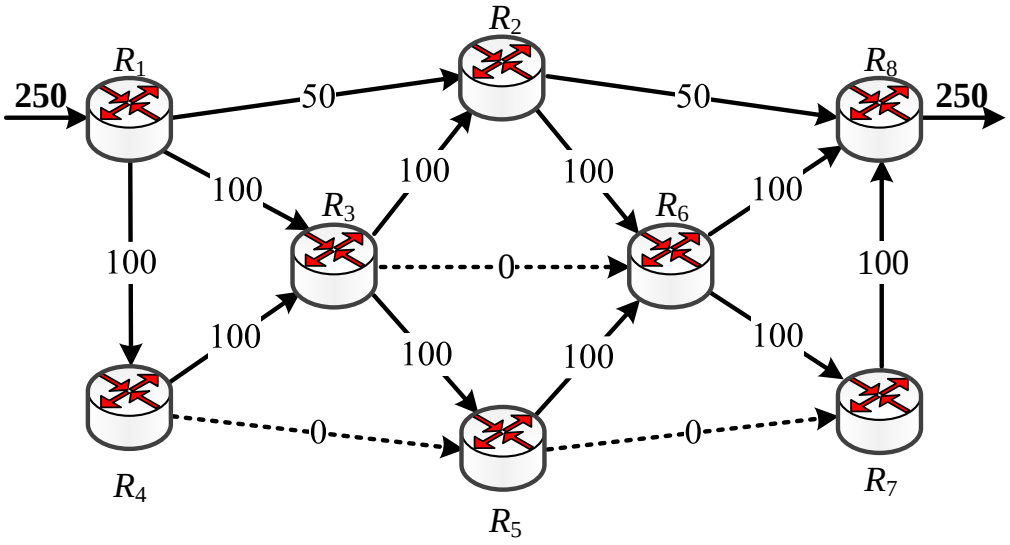


Рис. 2.23. Результат розрахунку множини шляхів
з використанням умов (2.7), (2.8) обслуговування потоку інтенсивністю 250 1/с

Зокрема у шляхів $R_1 \to R_2 \to R_8$ і $R_1 \to R_3 \to R_2 \to R_6 \to R_8$ вузол R_2 є спільним, а шляхи $R_1 \to R_3 \to R_2 \to R_6 \to R_8$ і $R_1 \to R_4 \to R_3 \to R_5 \to R_6 \to R_7 \to R_8$ у цьому випадку мають два спільних вузли, а саме транзитні вузли R_3 і R_6. Шляхом $R_1 \to R_2 \to R_8$ передається потік інтенсивністю 50 1/с, а шляхами $R_1 \to R_3 \to R_2 \to R_6 \to R_8$ і $R_1 \to R_4 \to R_3 \to R_5 \to R_6 \to R_7 \to R_8$ – потоки інтенсивністю по 100 1/с.

Для прикладу у використанні множини маршрутів, що не перетинаються $\left(R_1 \to R_2 \to R_8,\ R_1 \to R_3 \to R_6 \to R_8 \text{ та } R_1 \to R_4 \to R_5 \to R_7 \to R_8\right)$, продуктивність напрямку зв'язку між першим та восьмим вузлами за умови пропускних здатностей каналів зв'язку, зазначених на рис. 2.22, становитиме лише 150 1/с. Таким чином, перехід до задіяння шляхів, що перетинаються за вузлами, у розглянутому прикладі сприяє зростанню продуктивності обраного напрямку зв'язку приблизно в 1,7 раза. Одночасно із зростанням розміру мережі та зв'язності маршрутизаторів, коли кількість шляхів, що перетинаються, зростає, виграш за продуктивністю збільшувався до 2,5–4 разів.

2.5. Потокова модель швидкої перемаршрутизації в ІКМ

Як зазначалось у підрозділі 2.2, швидка перемаршрутизація належить до засобів відмовостійкої маршрутизації, що реалізується на рівні ядра ІКМ та основана на введенні ресурсної надлишковості [19, 20]. Тобто одночасно з основним шляхом (мультишляхом) для кожного потоку має розраховуватись і резервний шлях (мультишлях), що не проходить через проблемні елементи

мережі (вузли, канали, сегменти), які захищаються. Це накладає певні особливості на саму структуру моделі швидкої перемаршрутизації в ІКМ.

В описі потокової моделі швидкої перемаршрутизації в ІКМ варто зазначити, що надалі через $x_{i,j}^{k}$ будуть позначатися маршрутні змінні, кожна з яких характеризує частку інтенсивності k-го потоку в каналі зв'язку, що представляється дугою $E_{i,j} \in E$ і міститься в *основному* маршруті. Кількість маршрутних змінних $x_{i,j}^{k}$ відповідає добутку $|K| \cdot |E|$. Крім того, мають місце умови збереження потоку (1.3), реалізації багатошляхової стратегії маршрутизації (1.2) та відсутності перевантаження каналів зв'язку ІКМ (1.4).

У разі використання в ІКМ одношляхової маршрутизації потоків мають місце умови (1.1). Для визначення резервних маршрутів, як зазначено в роботах [5, 12, 41, 55, 57], вводяться додаткові маршрутні змінні $\overline{x}_{i,j}^{k}$, кожна з яких характеризує частку k-го потоку в каналі зв'язку, представленого дугою $E_{i,j}$, але вже *резервного* шляху/мультишляху. Наприклад, для забезпечення зв'язності резервного одноадресного шляху/мультишляху на змінні $\overline{x}_{i,j}^{k}$ накладаються обмеження, аналогічні (1.3) [73, 74]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = 0;\ k \in K^{o},\ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = 1;\ k \in K^{o},\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = -1;\ k \in K^{o},\ R_i = d_k. \end{cases} \quad (2.9)$$

Для реалізації багатоадресної маршрутизації на змінні $\overline{x}_{i,j}^{k}$ накладаються обмеження, аналогічні (1.7)–(1.10).

2.6. Формалізація умов забезпечення захисту вузла, каналу, маршруту та пропускної здатності під час швидкої перемаршрутизації в ІКМ

Як показав проведений у підрозділі 2.2 аналіз, у процесі швидкої перемаршрутизації можуть підтримуватися кілька основних схем захисту елементів мережі: вузла, каналу, шляху та його пропускної здатності. У працях [75, 76] формалізовано в аналітичному вигляді умови для підтримки зазначених схем захисту як елементи відповідних математичних моделей.

Так, у роботі [75] пропонується для реалізації схеми захисту каналу $E_{i,j} \in E$ на маршрутні змінні $\bar{x}_{i,j}^k$, що відповідають за визначення резервного шляху, накласти додаткові обмеження, аналогічні (1.1). Зокрема в разі реалізації одношляхової стратегії маршрутизації має місце таке обмеження:

$$\bar{x}_{i,j}^k \in \left\{0; \delta_{i,j}^k\right\} \ , \tag{2.10}$$

тоді як у випадку багатошляховій маршрутизації

$$0 \le \bar{x}_{i,j}^k \le \delta_{i,j}^k , \tag{2.11}$$

де

$$\delta_{i,j}^k = \begin{cases} 0, \text{ за умови захисту каналу зв'язку } E_{i,j}; \\ 1, \text{ в іншому випадку.} \end{cases} \tag{2.12}$$

Виконання умов (2.10)–(2.12) гарантує, що канал $E_{i,j} \in E$, який захищається, не буде застосовуватися резервним маршрутом. Умови (2.10) та (2.11) мають лінійний характер, на відміну від нелінійних виразів, запропонованих у роботі [74], що сприяє зниженню обчислювальної складності отримання кінцевих протокольних рішень.

Для забезпечення захисту вузла в праці [74] пропонується використовувати нелінійні вирази для реалізації цієї схеми. Тоді як в роботі [55] запропоновано підхід, оснований на введенні лінійних умов у вигляді

$$\sum_{R_j \in R_i^*} \left(x_{j,i}^k + \bar{x}_{j,i}^k\right) \le 1, \text{ якщо } R_j \in R_i^*, \ j = \overline{1,m}, \tag{2.13}$$

які, однак, справедливі лише у разі використання одношляхової стратегії маршрутизації, де через $R_i^* = \left\{R_j : E_{j,i} \ne 0; \ j = \overline{1,m}; i \ne j\right\}$ позначено підмножину маршрутизаторів, які є суміжними для вершини R_i.

У цій роботі пропонується узагальнення умов (2.10) та (2.11) на випадок захисту множини каналів зв'язку, інцидентних вузлу $R_i \in R$, що захищається [75, 76]. Тоді в разі одношляхової маршрутизації мають місце такі обмеження:

$$\bar{x}_{i,j}^k \in \left\{0; \delta_{i,j}^k\right\}, \text{ якщо } R_j \in R_i^*, \ j = \overline{1,m}, \tag{2.14}$$

а у випадку використання багатошляхової стратегії вводиться система умов

$$0 \le \bar{x}_{i,j}^k \le \delta_{i,j}^k, \text{ якщо } R_j \in R_i^*, \ j = \overline{1,m}, \tag{2.15}$$

де вибір значень $\delta_{i,j}^k$ підпорядковується умові (2.12).

Отже, виконання вимог умов (2.14), (2.15) гарантує захист вузла $R_i \in R$, забороняючи використання резервним маршрутом усіх каналів, які виходять з цього вузла. Оскільки захисту підлягають лише транзитні маршрутизатори, то заборона на застосування вихідних каналів запобігає включенню до резервного шляху і вхідних каналів для цього вузла R_i, що в результаті сприяє захисту вузла загалом. Варто зазначити, що умови захисту заздалегідь визначених вузлів і каналів мережі, як правило, є лінійними, а їх урахування критично не позначається на складності обчислення маршрутних змінних $x_{i,j}^k$ та $\overline{x}_{i,j}^k$, що відповідають за формування множини основних і резервних маршрутів відповідно.

У разі реалізації схеми захисту шляху необхідно забезпечити відсутність спільних вузлів і каналів як в основному, так і резервному маршрутах. Тоді за аналогією з результатами, отриманими в роботі [55], для реалізації одношляхової маршрутизації необхідно виконати такі лінійні умови:

$$\sum_{R_j \in R_i^*} \sum_{R_p \in R_i^*} \left(x_{j,i}^k + \overline{x}_{p,i}^k \right) \le 1, \ \forall R_i \in R \setminus \{ s_k, d_k \}. \tag{2.16}$$

Універсальні умови захисту шляху, які справедливі й для одношляхової, і для багатошляхової маршрутизації, мають нелінійний вигляд:

$$\sum_{R_j \in R_i^*} \sum_{R_p \in R_i^*} x_{j,i}^k \overline{x}_{p,i}^k = 0, \ \forall R_i \in R \setminus \{ s_k, d_k \}. \tag{2.17}$$

Вигляд виразів (2.17) дещо відрізняється від умов, запропонованих у [74]:

$$\sum_{R_i \in R} \sum_{\substack{R_j \in R, \\ i \ne j}} x_{i,j}^k \overline{x}_{i,j}^k = 0,$$

оскільки в раніше відомому рішенні резервний мультишлях допускав вузловий перетин з основним. Отже, введені умови (2.17) є більш чіткими.

Через необхідність здійснення резервування пропускної здатності мережі, а також з метою запобігання можливого перевантаження каналів зв'язку ІКМ у реалізації стратегій як одношляхової, так і багатошляхової маршрутизації основними і резервними маршрутами в модель за аналогією з результатами, отриманими в роботі [77], вводяться в загальному вигляді такі умови:

$$\sum_{k \in K} \lambda^k \cdot \max \left[x_{i,j}^k, \overline{x}_{i,j}^k \right] \le \varphi_{i,j}, \ E_{i,j} \in E. \tag{2.18}$$

Тобто довільний канал зв'язку $E_{i,j} \in E$ під час швидкої перемаршрутизації не повинен перевантажуватися потоками, які протікають основними або

резервними шляхами. У моделюванні процесів швидкої перемаршрутизації виникають певні складнощі в разі формалізації умов захисту пропускної здатності мережі, коли лише деякі з потоків, що передаються, перемикаються з основних на резервні маршрути. У роботах [73, 74] умови для реалізації одношляхової швидкої перемаршрутизації мають такий вигляд:

$$\sum_{k\in K} \lambda^k \left(\frac{x_{i,j}^k + \overline{x}_{i,j}^k}{x_{i,j}^k \overline{x}_{i,j}^k + 1} \right) \le \varphi_{i,j},\ E_{i,j} \in E. \qquad (2.19)$$

У найбільш загальному випадку, включаючи і варіант (2.19), тобто в разі реалізації одночасно одношляхової та багатошляхової швидкої маршрутизації, умови захисту пропускної здатності ІКМ записують таким чином [74]:

$$\frac{1}{2} \sum_{k\in K} \lambda^k \left[x_{i,j}^k + \overline{x}_{i,j}^k + \left| x_{i,j}^k - \overline{x}_{i,j}^k \right| \right] \le \varphi_{i,j},\ E_{i,j} \in E. \qquad (2.20)$$

Отже, умови захисту пропускної здатності (ПЗ) мережі (2.19) та (2.20) фактично зводяться до виконання умов запобігання перевантаження каналів зв'язку для реалізації швидкої перемаршрутизації, які справедливі навіть тоді, коли не всі, а лише деякі потоки будуть перенаправлені з основного на резервний маршрут. У цьому випадку для цих потоків завжди залишатиметься незадіяною деяка частина ПЗ каналів зв'язку резервних маршрутів, реалізуючи тим самим схему захисту пропускної здатності під час організації швидкої перемаршрутизації в ІКМ.

Окремо варто заначити, що умови (2.19) та (2.20) є адекватними і для випадку організації багатоадресної або широкомовної маршрутизації, коли маршрутні змінні $x_{i,j}^k$ та $\overline{x}_{i,j}^k$ визначають порядок балансування навантаження відповідно до обмежень (1.7)–(1.10).

2.7. Дослідження оптимальності рішень щодо швидкої перемаршрутизації в ІКМ

2.7.1. Формування критерію оптимальності рішень щодо швидкої перемаршрутизації на основі метрик

З огляду на те, що в загальному випадку вибір маршрутів (як основних, так і резервних) в ІКМ можна зробити множиною способів, доцільно задачу відмовостійкої маршрутизації сформулювати як оптимізаційну, щоб отримане рішення сприяло, наприклад, мінімізації використання доступного мережного ресурсу та/або покращенню рівня балансування навантаження, якості обслуговування загалом. Важливим моментом у формулюванні будь-якої

оптимізаційної задачі є вибір критерію оптимальності отримуваних рішень, вигляд якого, з одного боку, повинен адекватно відображати фізичний зміст процесу, що моделюється, а з іншого, – надавати можливість отримання шуканих результатів із заданими вимогами (прийнятною точністю, обчислювальною складністю в реальному часі тощо).

Класичний підхід у розв'язанні маршрутних задач в ІКМ полягає в мінімізації сумарної метрики розрахованого маршруту. Так, у роботах [73, 74] у процесі розрахунку маршрутних змінних для розв'язання задач відмовостійкої маршрутизації пропонується використовувати критерій оптимальності, пов'язаний з мінімізацією такої лінійної цільової функції:

$$F = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^{k} x_{i,j}^{k} + \sum_{k \in K} \sum_{E_{i,j} \in E} \overline{c}_{i,j}^{k} \overline{x}_{i,j}^{k}, \qquad (2.21)$$

де $c_{i,j}^{k}$ і $\overline{c}_{i,j}^{k}$ – маршрутні метрики каналів зв'язку, які застосовуються в обчисленні основного та резервного шляхів відповідно.

Функція (2.21) кількісно характеризує сумарні витрати на формування та використання основного та резервного маршрутів між парою вузлів «відправник» та «отримувач». Крім того, у дослідженнях [73, 74] установлено необхідність її доповнення умовою

$$\sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^{k} x_{i,j}^{k} \le \sum_{k \in K} \sum_{E_{i,j} \in E} \overline{c}_{i,j}^{k} \overline{x}_{i,j}^{k}, \qquad (2.22)$$

виконання якої гарантує те, що основний шлях (мультишлях) завжди буде не гіршим за резервний у межах обраних метрик $c_{i,j}^{k}$ і $\overline{c}_{i,j}^{k}$, тобто кожен k-й потік спочатку має використовувати, наприклад, найкоротший з точки зору кількості переприйомів (якщо $c_{i,j}^{k} = \overline{c}_{i,j}^{k} = 1$) або більш продуктивний (за умови $c_{i,j}^{k} = \overline{c}_{i,j}^{k} = 10^{7} / \varphi_{i,j}$) шлях/шляхи.

Як показав проведений аналіз, використання критерію (2.21) дійсно забезпечує адекватне рішення поставленого завдання щодо відмовостійкої маршрутизації, проте спостерігається і низка проблемних моментів, які в подальшому можуть негативно позначитися на результативності практичної реалізації моделі (1.1)–(1.4), (2.9)–(2.20) загалом. Насамперед це стосується зниження загальної продуктивності ІКМ з огляду на те, що застосування резервних шляхів так чи інакше пов'язано із залученням додаткового мережного ресурсу (канального та буферного), який з цієї причини не зможе бути використаний іншими потоками.

З іншого боку, необхідність розрахунку поряд з основними маршрутами ще й множини резервних шляхів пов'язана з підвищенням обчислювального навантаження на маршрутизатори ІКМ, а також необхідністю підтримки маршрутних таблиць підвищеної розмірності, в яких би зберігалися дані як про основні, так і резервні шляхи. Зокрема шляхи цих двох типів необхідно не тільки розрахувати, але ще й підтримувати в активному стані. Загалом перелічені чинники, разом зі зниженням продуктивності ІКМ, негативно позначаються на масштабованості рішень, пов'язаних з відмовостійкою маршрутизацією. Особливо це критично для ІКМ великої розмірності і з розгалуженою мережною структурою (високою зв'язністю вузлів).

Перелічені недоліки є спільними практично для всіх технологій, пов'язаних з підвищенням надійності мережі загалом, і є своєрідною «платою» за забезпечення заданого рівня відмовостійкості кінцевих рішень. Для мінімізації цих недоліків бажано, щоб унаслідок проведених розрахунків резервний шлях якомога менше відрізнявся за складом каналів і вузлів від основного – в ідеалі лише на проблемний елемент мережі, що підлягає подальшому захисту. Це має сприяти введенню мінімальної ресурсної надлишковості, коли резервуванню підлягатимуть мінімальні обсяги пропускної здатності каналів мережі, що позитивно позначиться на її продуктивності та показниках якості обслуговування загалом. Крім того, тоді на вузлах мережі для кожного потоку можуть зберігатися вже не дві маршрутні таблиці (для основного та резервного шляху), а одна, але з мінімально необхідними коригуваннями, що стосуються відмінностей основного та резервного шляхів.

Тоді за аналогією з підходом, описаним у роботі [75], критерій (2.21) пропонується замінити на мінімум такої цільової функції:

$$F = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^{k} x_{i,j}^{k} + \sum_{k \in K} \sum_{E_{i,j} \in E} \overline{c}_{i,j}^{k} \overline{x}_{i,j}^{k} - \sum_{k \in K} \sum_{E_{i,j} \in E} b_{i,j}^{k} x_{i,j}^{k} \overline{x}_{i,j}^{k}, \qquad (2.23)$$

в якій введення третього доданка якраз пов'язано із забезпеченням максимального збігу резервного шляху з основним за складом каналів і вузлів, що містяться в них; $b_{i,j}^{k}$ – досить великий за своєю величиною штрафний коефіцієнт $\left(b_{i,j}^{k} >> c_{i,j}^{k} \quad \text{і} \quad b_{i,j}^{k} >> \overline{c}_{i,j}^{k} \right)$. Знак мінус перед третім доданком вводиться з тієї причини, що ступінь збігу резервного й основного шляхів необхідно максимізувати, а метрики основного та резервного шляхів (перший і другий доданок у (2.23)) повинні бути мінімальними.

2.7.2. Характеристика оптимізаційних задач швидкої перемаршрутизації на основі метрик та методів їх розв'язання

Вирішення завдання щодо швидкої перемаршрутизації в межах запропонованого вдосконалення потокової моделі (1.1)–(1.4), (2.9)–(2.21), (2.23) зводиться до розв'язання оптимізаційної задачі, пов'язаної з мінімізацією цільової функції (2.23) за наявності системи обмежень:

– (1.1) або (1.2), що відповідають за реалізацію одношляхової або багатошляхової маршрутизації відповідно;

– (1.3) та (2.9), що описують умови збереження потоку у вузлах основного та резервного шляху (мультишляху);

– (2.10), (2.11), (2.14), (2.15) та (2.16), (2.17), що вводяться для реалізації можливих схем захисту елементів мережі (каналу, вузла та шляху відповідно);

– (2.19), (2.20), що формалізують умови запобігання перевантаження каналів зв'язку мережі та захисту пропускної здатності мережі, включаючи випадок, коли лише деякі з потоків перемикаються на резервні шляхи;

– (2.22), яка відповідає за те, що основний шлях (мультишлях) завжди буде не гірший, ніж резервний у межах обраних метрик.

Залежно від виду цільової функції та обмежень, які визначаються обраною стратегією маршрутизації (одношляховою або багатошляховою), сформульована оптимізаційна задача може належати до того чи іншого класу задач математичного програмування, що потребує використання відповідного методу розв'язання (табл. 2.3). З огляду на те, що обмеження (2.17), які вводяться для реалізації схеми захисту шляху, та умови (2.19) і (2.20), пов'язані із запобіганням перевантаження каналів зв'язку мережі, мають нелінійний характер, то і сформульована оптимізаційна задача в будь-якому випадку належатиме до класу задач нелінійного програмування.

Таблиця 2.3

Характеристика оптимізаційних задач відмовостійкої маршрутизації та методів їх розв'язання

Клас оптимізаційної задачі	Методи розв'язання
Стратегія маршрутизації: одношляхова	
змішаного цілочисельного нелінійного програмування	метод округлення, метод гілок і меж, методи послідовної лінеаризації, метод імітації відпалу, генетичний алгоритм, різні змішані (гібридні) методи
Стратегія маршрутизації: багатошляхова	
нелінійного програмування	метод невизначених множників Лагранжа, метод штрафних функцій, градієнтні методи

Крім того, у реалізації одношляхової маршрутизації маршрутні змінні матимуть булевий характер, у зв'язку з чим розв'язувана оптимізаційна задача вже належатиме до підкласу задач змішаного цілочисельного нелінійного програмування (Mixed Integer Nonlinear Programming, MINLP).

За відсутності необхідності в захисті шляху та/або його пропускної здатності сформульована задача належатиме до класу задач булевого програмування (у разі одношляхової маршрутизації) або лінійного програмування (за умови багатошляхової маршрутизації).

2.7.3. Обґрунтування вибору вагових коефіцієнтів у критерії оптимальності рішень щодо швидкої перемаршрутизації в ІКМ

Особливості розв'язання задачі швидкої перемаршрутизації з використанням моделі (1.1)–(1.4), (2.9)–(2.21), (2.23) продемонструємо на прикладі мережної структури, зображеної на рис. 2.24. Представлена мережа складається з 13 маршрутизаторів та 22 каналів зв'язку. У розривах каналів зв'язку вказані їх пропускні здатності. Нехай маршрутні метрики каналів приймали значення $10^7/\varphi_{i,j}$ за аналогією з протоколом IGRP.

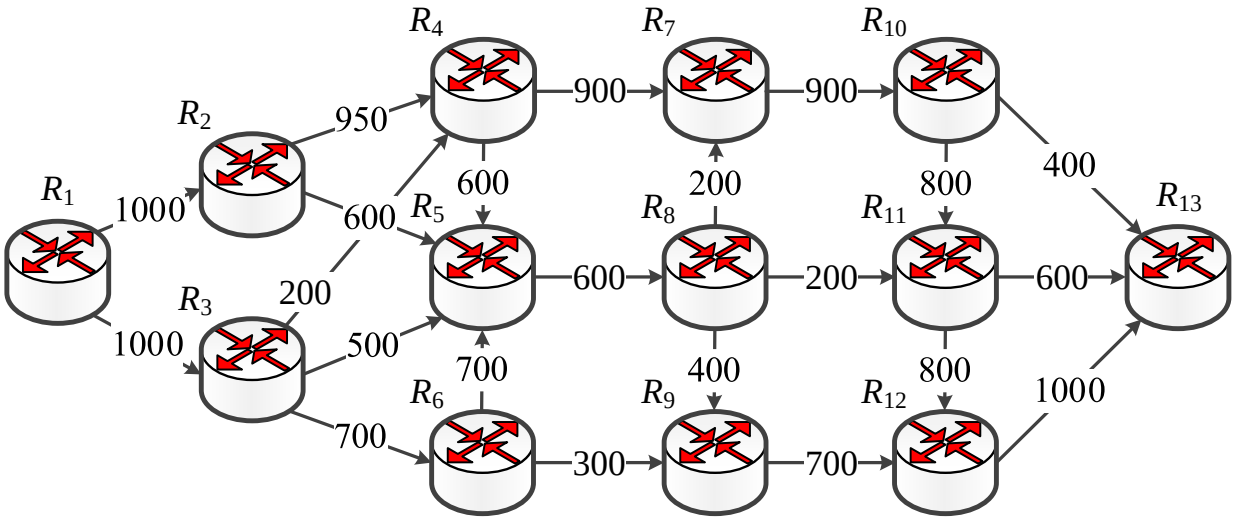


Рис. 2.24. Приклад структури ІКМ, що досліджуються

Під час дослідження встановлено низку закономірностей. По-перше, якщо для реалізації схем захисту вузла та каналу в ІКМ обирати співвідношення числових значень коефіцієнтів у (2.23) так, як пропонується в [74–76], тобто $b_{i,j}^k >> c_{i,j}^k$ і $b_{i,j}^k >> \bar{c}_{i,j}^k$, то визначальним у цільовій функції буде третій доданок. Це призводить до того, що в розрахунках як основний, так і резервний шлях завжди, поки це можливо, тобто за відсутності

перевантаження ІКМ, повністю збігатимуться, обходячи елемент мережі, який захищається. Наприклад, якщо необхідно передавати пакети з інтенсивністю 100 1/с від першого маршрутизатора до тринадцятого із забезпеченням захисту четвертого маршрутизатора, то основний і резервний шляхи пройдуть послідовно через маршрутизатори $R_1 \to R_3 \to R_6 \to R_9 \to R_{12} \to R_{13}$. Однак оптимальним маршрутом, з точки зору пропускної здатності та кількості переприйомів, є шлях $R_1 \to R_2 \to R_4 \to R_7 \to R_{10} \to R_{13}$. Таким чином, подібний вибір співвідношення коефіцієнтів у цільовій функції (2.23) може призвести до значної втрати продуктивності ІКМ, особливо якщо елемент (вузол або канал), який захищається і не включається в основний маршрут, є частиною високопродуктивної ділянки мережі.

Під час дослідження встановлено, що більш ефективною є така ієрархія співвідношень між ваговими коефіцієнтами в цільовій функції (2.23): $c_{i,j}^k >> b_{i,j}^k$ і $b_{i,j}^k >> \bar{c}_{i,j}^k$. Тоді основний маршрут завжди буде мати найкращу метрику незалежно від того, містить він елемент мережі, що захищається, чи ні. Ключовим критерієм для вибору резервного шляху тоді стане його мінімальне розходження з основним маршрутом за складом каналів, що його утворюють. Продемонструємо ці можливості на мультипотоковому прикладі.

Нехай в ІКМ, структура якої зображена на рис. 2.24, необхідно захистити високошвидкісний канал між маршрутизаторами R_4 і R_7 під час передачі пакетів двох потоків, що мають такі характеристики:

– $\lambda^1 = 100$ 1/с від вузла-відправника $s_1 = R_1$ до вузла-отримувача $d_1 = R_{13}$;

– $\lambda^2 = 100$ 1/с від вузла-відправника $s_2 = R_2$ до вузла-отримувача $d_2 = R_{10}$.

Ілюстрація отримуваного рішення за умови використання запропонованої моделі наведена на рис. 2.25, де основний шлях зображений суцільною лінією, резервний – пунктирною, тоді як канали зв’язку, що не використовуються, показані напівпрозорими лініями. У розривах каналів зв’язку вказані їх пропускні здатності (1/с).

У цьому випадку основні маршрути проходять через такі маршрутизатори:

– $R_1 \to R_2 \to R_4 \to R_7 \to R_{10} \to R_{13}$ – для першого потоку;

– $R_2 \to R_4 \to R_7 \to R_{10}$ – для другого потоку;

а резервні шляхи можна записати в такому вигляді:

– $R_1 \to R_2 \to R_4 \to R_5 \to R_8 \to R_7 \to R_{10} \to R_{13}$ – для першого потоку;

– $R_2 \to R_4 \to R_5 \to R_8 \to R_7 \to R_{10}$ – для другого потоку.

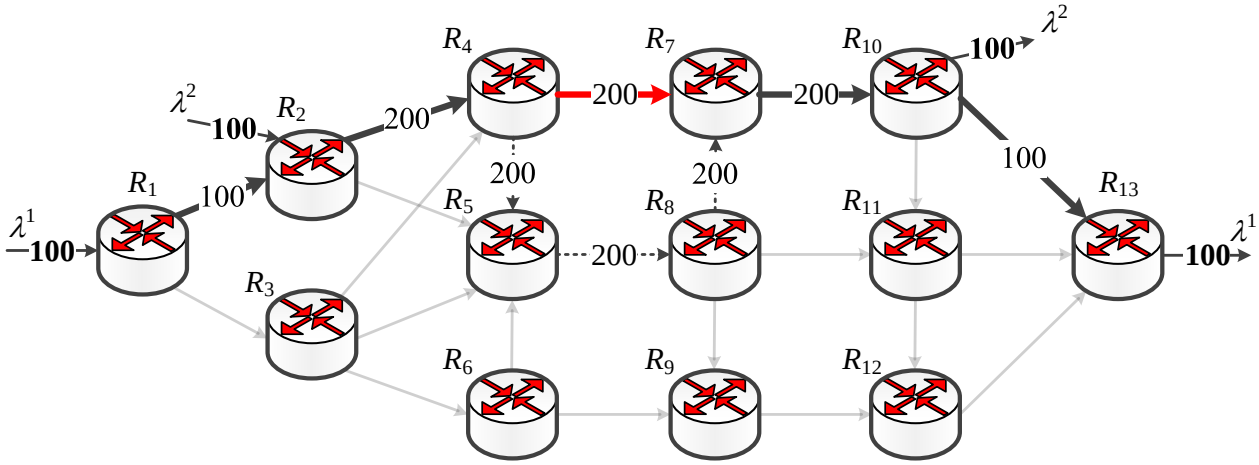


Рис. 2.25. Результати розв'язання задачі швидкої перемаршрутизації в ІКМ на основі використання критерію (2.23) та підтримки схеми «facility backup»

Як видно з отриманих результатів розрахунків (рис. 2.25), канал $E_{4,7}$, який захищається, має досить високу пропускну здатність (900 1/с) і використовується в основних маршрутах обох потоків, що позитивно позначається на продуктивності кінцевих рішень. З точки зору масштабованості ІКМ важливо зазначити, що отримане рішення щодо захисту зазначеного каналу максимально відповідає вимогам схеми «facility backup» [5, 34]. Це проявляється в тому, що спільний елемент $E_{4,7}$ основних маршрутів для розглянутих двох потоків захищено однією (спільною для цих потоків) резервною ділянкою $R_4 \to R_5 \to R_8 \to R_7$. Тоді резервний шлях відрізняється від основного за чотирма каналами зв'язку.

Варто задзначити, що вимогам схеми «facility backup» також відповідає і рішення $R_4 \to R_5 \to R_8 \to R_{11} \to R_{10}$ як частина резервних маршрутів. Однак воно не є оптимальним з точки зору критерію (2.23), тому що в цьому випадку резервний шлях відрізняється від основного за шістьма КЗ.

Окремо слід виокремити випадок, коли під час розрахунку резервних шляхів виникає неоднозначність у їх виборі. Приклад подібної ситуації наведений на рис. 2.26, на якому в розривах каналів зв'язку вказані їх пропускні здатності. Нехай основний шлях містить канал $E_{1,4}$, що захищається, тоді резервний шлях може пройти як через R_2, так і через R_3 – у кожному із зазначених випадків третій доданок у цільовій функції (2.23) прийме одне й те саме значення.

Тому у виборі резервного шляху важливо враховувати метрики каналів резервних маршрутів, представлених ваговими коефіцієнтами, для чого і було

введено в критерій оптимальності (2.23) другий доданок. У метриці числа переприйомів (як у протоколі RIP) ці два резервних шляхи є ідентичними.

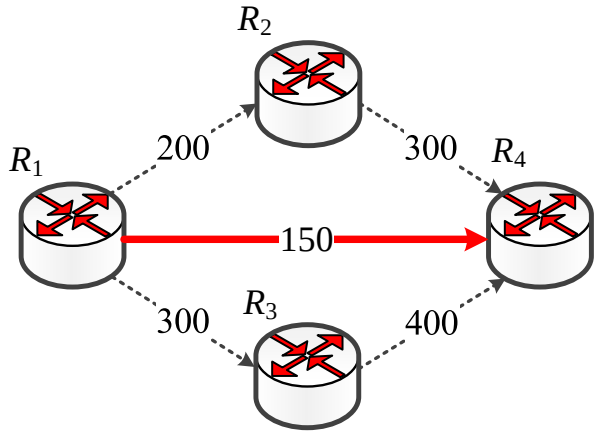


Рис. 2.26. Приклад виникнення неоднозначності
у виборі резервного шляху

Однак у разі використання метрики протоколу IGRP $\left(10^7/\varphi_{i,j}\right)$ буде оптимальним резервний шлях $R_1 \to R_3 \to R_4$, тому що він має пропускну здатність 300 1/с. Неоптимальний резервний маршрут $R_1 \to R_2 \to R_4$ має дещо меншу пропускну здатність (200 1/с).

Удосконалена модель швидкої перемаршрутизації може використовуватися і в тому випадку, коли як основний, так і резервний шляхи є мультишляхами, тобто містять кілька маршрутів від відправника до отримувача. Припустимо, що на структурі ІКМ, наведеної на рис. 2.24, пакети передаються від першого маршрутизатора до 13-го з інтенсивністю 700 1/с. Нехай необхідно реалізувати схему захисту шляху, зокрема основний і резервний мультишляхи не повинні мати спільних вузлів і каналів, тобто третій доданок у цільовій функції (2.23) дорівнюватиме нулю. Тоді на рис. 2.27 показано результат вирішення поставленого завдання за допомогою запропонованої потокової моделі швидкої перемаршрутизації в ІКМ, де, як і раніше, основний мультишлях представлено суцільною лінією, резервний – пунктирною, а невикористовувані канали зв'язку зображені напівпрозорими лініями. У розривах каналів зв'язку вказано інтенсивність потоку пакетів (1/с).

Таким чином, основний мультишлях містить два шляхи (рис. 2.27). Першим шляхом $R_1 \to R_2 \to R_4 \to R_7 \to R_{10} \to R_{13}$ передається потік пакетів з інтенсивністю 400 1/с, а другим $R_1 \to R_2 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{13}$ – потік з інтенсивністю 300 1/с.

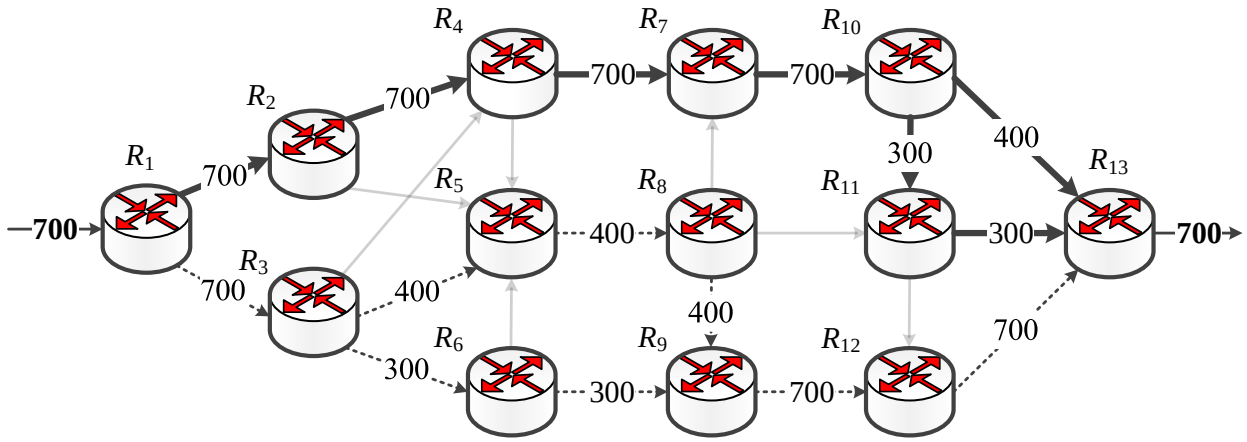


Рис. 2.27. Результат розв’язання задачі багатошляхової швидкої перемаршрутизації в ІКМ з використанням критерію оптимальності (2.23)

Резервний мультишлях також складається з двох маршрутів. Першим шляхом, який формується послідовністю маршрутизаторів $R_1 \to R_3 \to R_5 \to R_8 \to R_9 \to R_{12} \to R_{13}$, пакети передаються з інтенсивністю 400 1/с, а другим $R_1 \to R_3 \to R_6 \to R_9 \to R_{12} \to R_{13}$ – потік з інтенсивністю 300 1/с. Відповідно до отриманих результатів розрахунку основний і резервний мультишляхи не мають спільних мережних елементів (вузлів або каналів), що позитивно впливає на рівень відмовостійкості ІКМ, а реалізація багатошляхової стратегії маршрутизації сприяє підвищенню якості обслуговування.

2.7.4. Білінійний критерій оптимальності рішень щодо швидкої перемаршрутизації в процесі реалізації схеми захисту шляху

Нелінійність умов захисту мультишляху (2.17) негативно позначається на рівні обчислювальної складності рішень щодо швидкої перемаршрутизації. Тому в роботі пропонується використовувати критерій оптимальності, який основано на мінімізації такої білінійної цільової функції [77, 78]:

$$F = \sum_{k\in K}\sum_{E_{i,j}\in E} c_{i,j}^{k} x_{i,j}^{k} x_{i,j}^{k} + \sum_{k\in K}\sum_{E_{i,j}\in E} c_{i,j}^{k} x_{i,j}^{k} + \sum_{k\in K}\sum_{E_{i,j}\in E} \overline{c}_{i,j}^{k} \overline{x}_{i,j}^{k} \overline{x}_{i,j}^{k} +$$

$$+ \sum_{k\in K}\sum_{E_{i,j}\in E} \overline{c}_{i,j}^{k} \overline{x}_{i,j}^{k} + \sum_{R_i\in R\setminus\{s_k,d_k\}}\sum_{R_j\in R_i^*}\sum_{R_p\in R_i^*} h x_{j,i}^{k} \overline{x}_{p,i}^{k}, \quad (2.24)$$

де h – ваговий коефіцієнт, який характеризує важливість білінійного доданка в критерії оптимальності (2.24).

Перший і другий доданки у виразі (2.24) визначають умовні вартості формування та використання основного шляху/мультишляху, а третій і четвертий – резервного. П’ятий доданок є найбільш важливим і відповідає за

реалізацію схеми захисту шляху, тобто за відсутність спільних вузлів і каналів в основному і резервному маршрутах. Таким чином, установлюється така система ієрархії співвідношень вагових коефіцієнтів у цільовій функції (2.24):

$$h >> c_{i,j}^{k} \text{ і } h >> \bar{c}_{i,j}^{k}, \tag{2.25}$$

а також доданків:

$$\sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^{k} x_{i,j}^{k} x_{i,j}^{k} + \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^{k} x_{i,j}^{k} \leq$$

$$\leq \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^{k} \bar{x}_{i,j}^{k} \bar{x}_{i,j}^{k} + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^{k} \bar{x}_{i,j}^{k}. \tag{2.26}$$

Виконання умови (2.26) гарантує, що розрахований основний шлях/мультишлях не поступатиметься за ефективністю резервному.

Отже, у межах проведеного вдосконалення математичної моделі завдання швидкої перемаршрутизації було сформульовано в оптимізаційній формі. Зокрема критерієм оптимальності є мінімум цільової функції (2.24), а обмеженнями – умови (1.2), (1.3), (2.9), (2.11), (2.12), (2.15). Для реалізації швидкої перемаршрутизації в ІКМ розрахунок шуканих маршрутних змінних забезпечується внаслідок розв'язання задачі нелінійного програмування. Крім того, пропоноване вдосконалення моделі швидкої перемаршрутизації з білінійним критерієм оптимальності для захисту мультишляху є більш строгим, ніж у [74], тому що основний і резервний маршрути, які розраховуються, не перетинаються ні за вузлами, ні за каналами.

Проведемо аналіз впливу квадратичних доданків критерію (2.24) та завантаженості мережі на характер результативних маршрутних рішень для ІКМ на прикладі мережної структури, наведеної на рис. 2.28, за умови захисту мультишляху між вузлом-відправником $s_1 = R_1$ і вузлом-отримувачем $d_1 = R_9$. У розривах каналів зв'язку вказані їх пропускні здатності. Для забезпечення розрахунку шляхів з максимальною продуктивністю маршрутні метрики каналів зв'язку приймали значення $10^7 / \varphi_{i,j}$ за аналогією з протоколом IGRP.

Нехай інтенсивність потоку пакетів становить $\lambda^1 = 200$ 1/с. Тоді на рис. 2.29, а наведено результат розрахунків на випадок відсутності в критерії (2.24) квадратичних доданків, який визначив реалізацію одношляхової маршрутизації (без балансування навантаження). Основний шлях, що проходить через маршрутизатори $R_1 \to R_2 \to R_3 \to R_6 \to R_9$, представлено суцільною лінією, резервний $R_1 \to R_4 \to R_7 \to R_8 \to R_9$ – пунктирною, тоді як канали зв'язку, які не використовуються, зображені

напівпрозорими лініями. На рис. 2.29 у розривах каналів зв'язку вказано інтенсивність потоку пакетів (1/с).

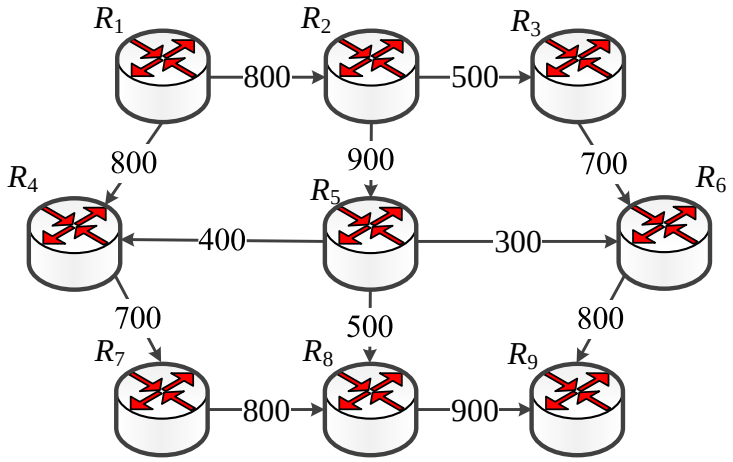
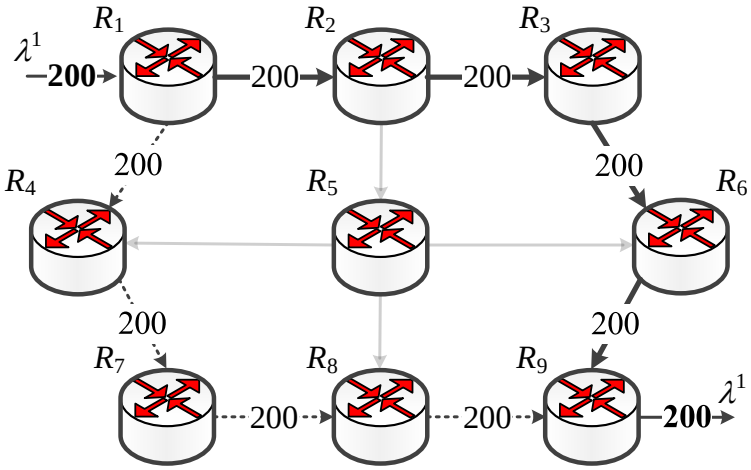
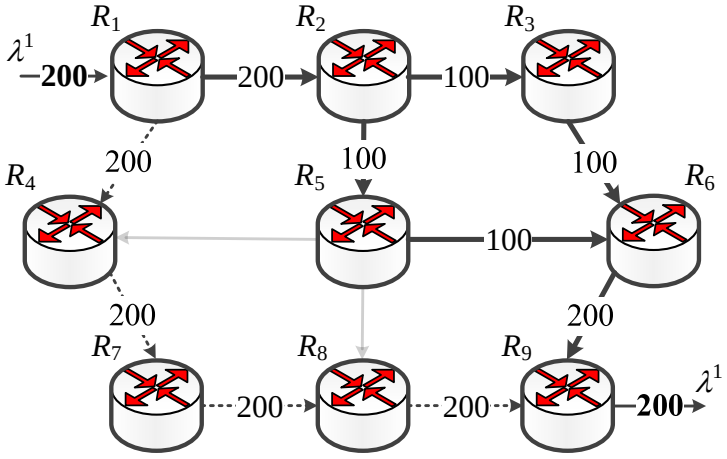


Рис. 2.28. Вихідна структура ІКМ, що досліджувалась



а) без квадратичних доданків у (2.24)



б) з квадратичними доданками в (2.24)

Рис. 2.29. Послідовність швидкої перемаршрутизації потоку з інтенсивністю 200 1/с на основі використання критерію оптимальності (2.24)

Введення квадратичних доданків у критерій (2.24) сприяло реалізації багатошляхової швидкої перемаршрутизації (рис. 2.29, б), коли основний мультишлях був представлений двома маршрутами:

– $R_1 \to R_2 \to R_3 \to R_6 \to R_9$ за умови передачі потоку з інтенсивністю 100 1/с;

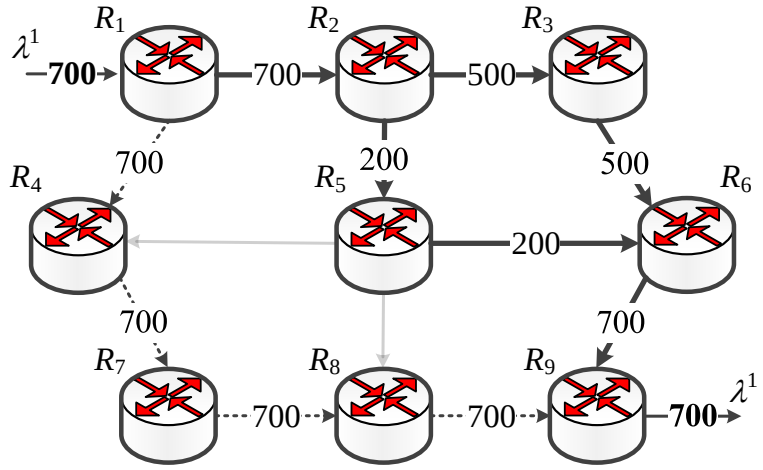
– $R_1 \to R_2 \to R_5 \to R_6 \to R_9$ у разі передачі потоку з інтенсивністю 100 1/с;

тоді як резервний шлях проходить через маршрутизатори:

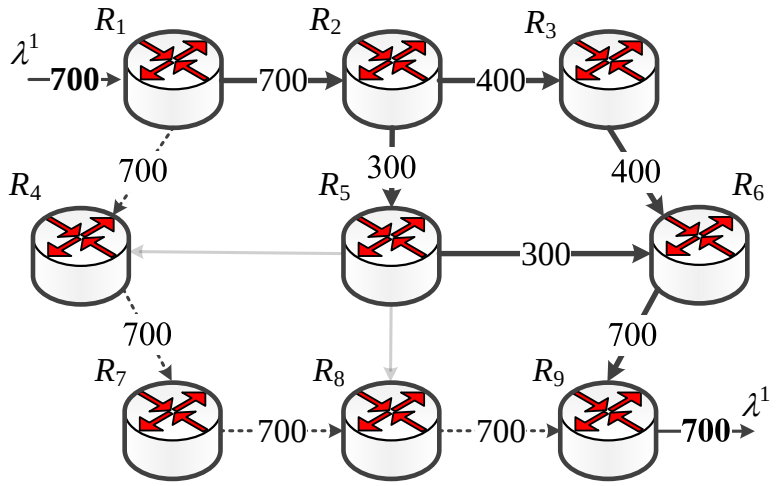
– $R_1 \to R_4 \to R_7 \to R_8 \to R_9$.

У випадку збільшення завантаженості мережі, коли інтенсивність потоку становила $\lambda^1 = 700$ 1/с, використання критерію (2.24) сприяло реалізації багатошляхової швидкої перемаршрутизації. У цьому випадку основний мультишлях складався з двох шляхів: $R_1 \to R_2 \to R_3 \to R_6 \to R_9$ та $R_1 \to R_2 \to R_5 \to R_6 \to R_9$. Зокрема, якщо квадратичні члени в функції (2.24) були відсутні, то потік балансувався між ними частинами за 500 та 200 1/с відповідно (рис. 2.30, а). У разі введення квадратичних доданків у цільову функцію (2.24) потік балансувався між основними маршрутами частинами за 400 та 300 1/с відповідно (рис. 2.30, б). Резервний шлях в обох випадках забезпечував передачу всього потоку через маршрутизатори $R_1 \to R_4 \to R_7 \to R_8 \to R_9$.

Отже, введення квадратичних членів у критерій (2.24) дозволяє, по-перше, забезпечити реалізацію багатошляхової швидкої перемаршрутизації навіть за умови невисокої завантаженості мережі, тоді як без їх введення здійснювалося послідовне вмикання шляхів відповідно до збільшення їх метрик; по-друге, у разі високої завантаженості ІКМ вдалося забезпечити краще балансування навантаження в мережі (рис. 2.30). Введення в критерій (2.24) відповідної білінійної форми дозволило забезпечити розрахунок основного та резервного шляху/мультишляху, які не перетинаються ні за вузлами, ні за каналами.



а) без квадратичних доданків у (2.24)



б) з квадратичними доданками в (2.24)

Рис. 2.30. Порядок швидкої перемаршрутизації потоку
з інтенсивністю 700 1/с на основі використання критерію оптимальності (2.24)

2.7.5. Приклади розв'язання задачі швидкої перемаршрутизації багатоадресних потоків в ІКМ

Розглянемо особливості організації швидкої перемаршрутизації багатоадресних потоків за умови реалізації різних схем захисту елементів мережі [73]. Нехай структура аналізованої мережі представлена на рис. 2.31, тобто вона складається з п'яти маршрутизаторів і семи каналів зв'язку, у розривах яких вказані їх пропускні здатності (1/с). Вузол-відправник – перший маршрутизатор $(s_1 = R_1)$, вузли-отримувачі – третій, четвертий і п'ятий маршрутизатори. Інтенсивність багатоадресного потоку становить $\lambda^1 = 70$ 1/с.

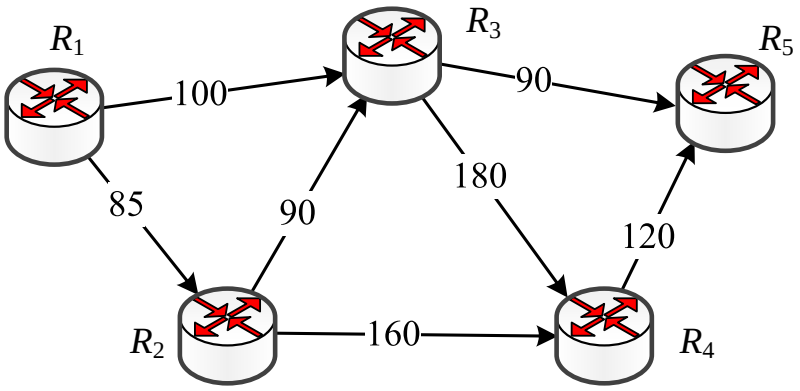


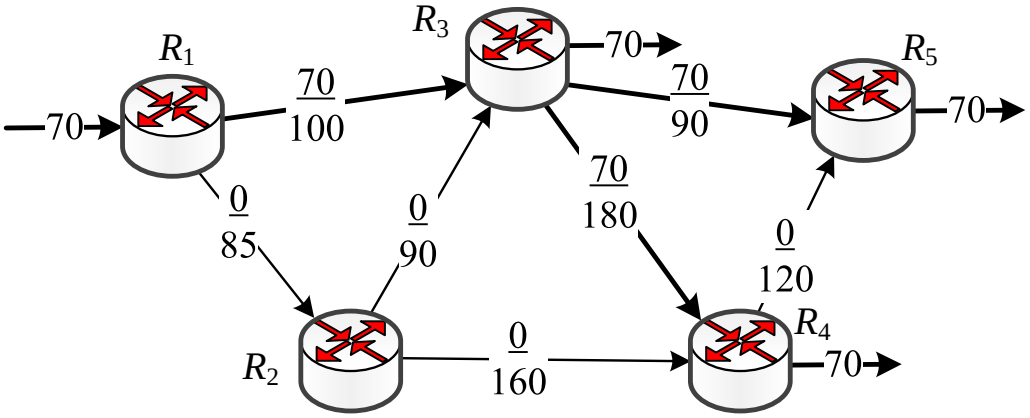
Рис. 2.31. Структура аналізованої мережі під час маршрутизації одного багатоадресного потоку

На рис. 2.32 наведено приклади розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі, наприклад, із захистом каналу зв'язку $E_{1,3}$ у разі мінімізації кількості переприйомів пакетів $\left(c_{i,j}^{k} = \bar{c}_{i,j}^{k} = 1\right)$. Тоді як основне дерево маршрутів є рішенням, представленим на рис. 2.32, а, зокрема «довжина» цього дерева мінімальна та становить три канали. Резервне дерево маршрутів (рис. 2.32, б), яке складається з чотирьох КЗ, відповідно до реалізованої схеми захисту не містить каналу $E_{1,3}$. На рис. 2.32 в розривах каналів зв'язку вказано дріб, в якому в чисельнику наведено інтенсивність потоку пакетів, а в знаменнику – пропускну здатність цього ж каналу. Як зображено на рис. 2.32, і основне, і резервне дерево маршрутів можуть обслужити багатоадресний потік інтенсивністю 70 1/с.

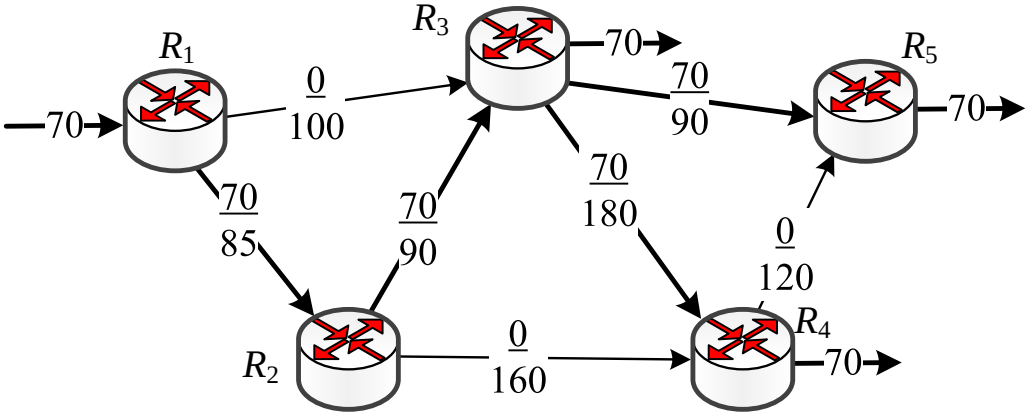
У процесі реалізації схеми захисту шляху дерево основного маршруту представлено на рис. 2.32, а, а резервне дерево маршрутів тоді буде також містити чотири канали й мати структуру, наведену на рис. 2.33.

Порядок швидкої перемаршрутизації багатоадресного потоку також сильно залежить від типу використовуваної маршрутної метрики. Якщо вибрати метрику, орієнтовану на врахування пропускної здатності КЗ, тобто якщо $c_{i,j}^{k} = \bar{c}_{i,j}^{k} = 10^{7} / \varphi_{i,j}$, то й основне дерево маршрутів, і резервне дещо зміняться (рис. 2.34). Так, наприклад, для захисту каналу $E_{1,3}$ застосування цієї метрики дозволяє підвищити пропускну здатність основного маршруту до 120 1/с (рис. 2.34, а). Резервний маршрут (рис. 2.34, б) також міститиме більш продуктивні канали, ніж у рішенні, наведеному на рис. 2.32, б, що призведе до зниження середньої затримки та ймовірності втрат пакетів.

Рішення, запропоноване на рис. 2.34, також повністю відповідає вимогам схеми «facility backup».



а) основне дерево маршрутів для багатоадресного потоку



б) резервне дерево маршрутів для багатоадресного потоку

Рис. 2.32. Приклад розв’язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом каналу зв’язку $E_{1,3}$ за умови мінімізації кількості переприйомів пакетів

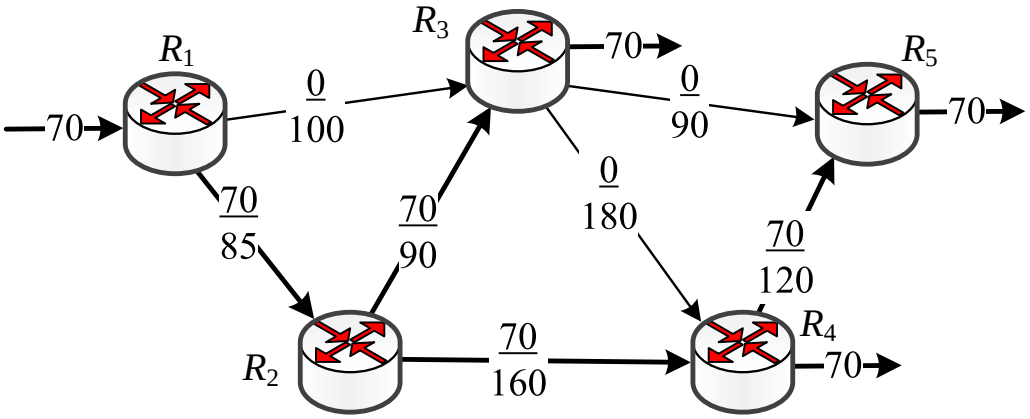
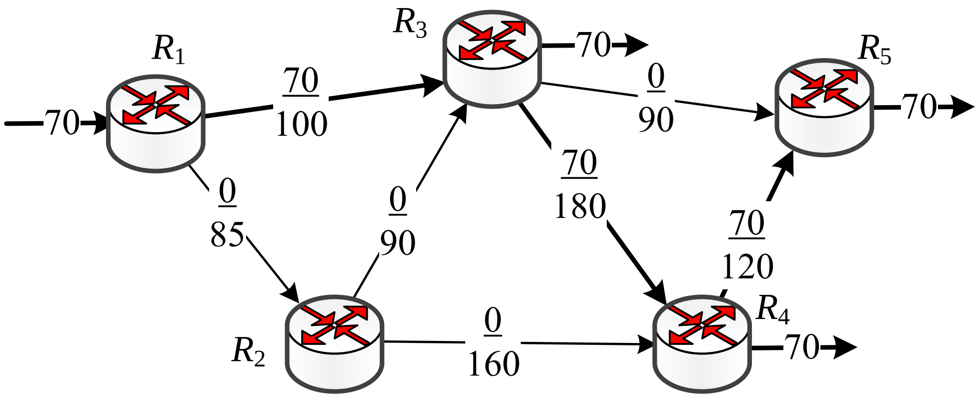
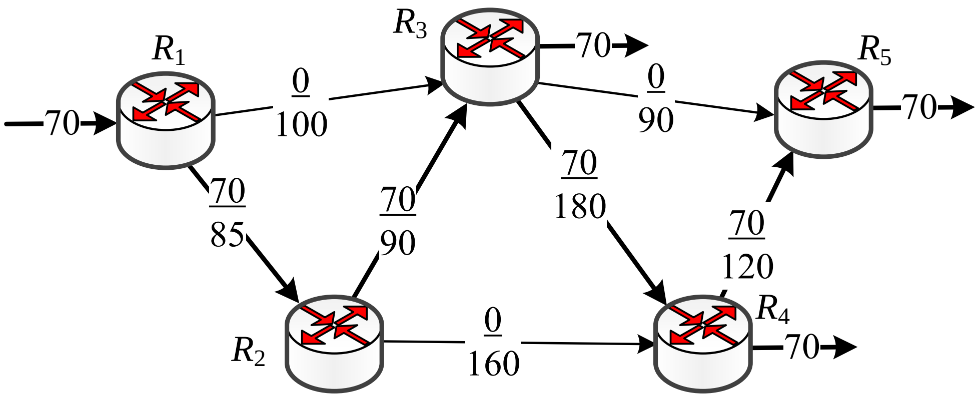


Рис. 2.33. Приклад розв’язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом шляху за умови мінімізації кількості переприйомів пакетів



а) основне дерево маршрутів для багатоадресного потоку



б) резервне дерево маршрутів для багатоадресного потоку

Рис. 2.34. Приклад розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом каналу зв'язку $E_{1,3}$ за умови використання метрики $c_{i,j}^k = \bar{c}_{i,j}^k = 10^7 / \varphi_{i,j}$

2.8. Рішення щодо швидкої перемаршрутизації з балансуванням навантаження в ІКМ

Реалізація відмовостійкої маршрутизації з резервуванням мережних елементів основане на введенні ресурсної надлишковості, коли одночасно з визначенням основного маршруту (ОМ) розраховується і резервний маршрут (РМ) відповідно до реалізованої схеми захисту. У зв'язку з цим у вирішенні завдань швидкої перемаршрутизації важливо забезпечити збалансоване використання доступного мережного, насамперед канального ресурсу, щоб захист елемента мережі не спричинив перевантаження ІКМ та істотне зниження рівня QoS. Тому для науки та практики є актуальним дослідження, спрямоване на розвиток концепції швидкої перемаршрутизації з балансуванням навантаження (Traffic Engineering Fast ReRoute, TE FRR) [31, 32, 63]. Тому в цьому підрозділі будуть запропоновані теоретичні рішення

щодо узгодженого вирішення завдань швидкої перемаршрутизації та балансування навантаження, орієнтованих на зниження обчислювальної складності та підвищення масштабованості протокольних рішень у процесі реалізації як одношляхової, так і багатошляхової стратегії маршрутизації.

2.8.1. Синтез та дослідження дворівневого методу одношляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ

Для забезпечення балансування навантаження в ІКМ на принципах концепції Traffic Engineering під час реалізації одношляхової швидкої перемаршрутизації (1.1) в ІКМ пропонується модифікувати модель (1.3), (2.9), (2.10), (2.14), (2.17), по-перше, змінивши форму умов захисту ПЗ (2.19) зі збереженням їх фізичного змісту, по-друге, сформулювавши задачу розрахунку маршрутних змінних $x_{i,j}^k$ і $\overline{x}_{i,j}^k$ як оптимізаційну, пов'язану з балансуванням навантаження в ІКМ, а по-третє, увівши дворівневу функціональну ієрархію розрахунків маршрутних змінних різних типів.

Тоді умови (2.19) пропонується представити в формі [81, 82]

$$\sum_{k\in K} \lambda^k \left(x_{i,j}^k + \overline{x}_{i,j}^k - x_{i,j}^k \overline{x}_{i,j}^k \right) \le \alpha \varphi_{i,j}, \; E_{i,j} \in E, \tag{2.27}$$

де α – додатково введена змінна, яка визначає верхній поріг завантаженості каналів зв'язку ІКМ і підпорядковується умовам [79, 80]:

$$0 \le \alpha \le 1. \tag{2.28}$$

Відзначимо, що ліві частини нерівностей (2.19) і (2.27) завжди дають однаковий числовий результат. Критерієм оптимальності розв'язань задачі швидкої перемаршрутизації в ІКМ за аналогією з результатами, отриманими в [79, 80], буде мінімум уведеного в (2.27) порога α, тобто

$$\min_{x,\overline{x},\alpha} \alpha. \tag{2.29}$$

Виконання умов (2.27)–(2.29) дозволяє забезпечити оптимальне балансування навантаження у процесі реалізації схеми захисту пропускної здатності розрахованих шляхів. У межах пропонованого методу вводиться дворівнева ієрархія розрахунків, яка підпорядковується принципу прогнозування взаємодій теорії ієрархічних багаторівневих систем [83, 84]. Тоді на нижньому рівні (рис. 2.35) пропонується здійснювати розрахунок маршрутних змінних $x_{i,j}^k$, які відповідають за визначення основних шляхів у мережі, під час мінімізації порогу α (2.29), але за умови фіксованих значень $\overline{x}_{i,j}^k$, що задаються на верхньому ієрархічному рівні. У цьому випадку

важливо забезпечити задоволення умов-обмежень (1.1), (1.3), (2.17), (2.28), а для захисту шляху – додатково й умови (2.27). У разі такого формулювання задачі умови (2.17) і (2.27) уже будуть лінійними, тому що значення $\bar{x}_{i,j}^{k}$ для нижнього рівня є відомими.

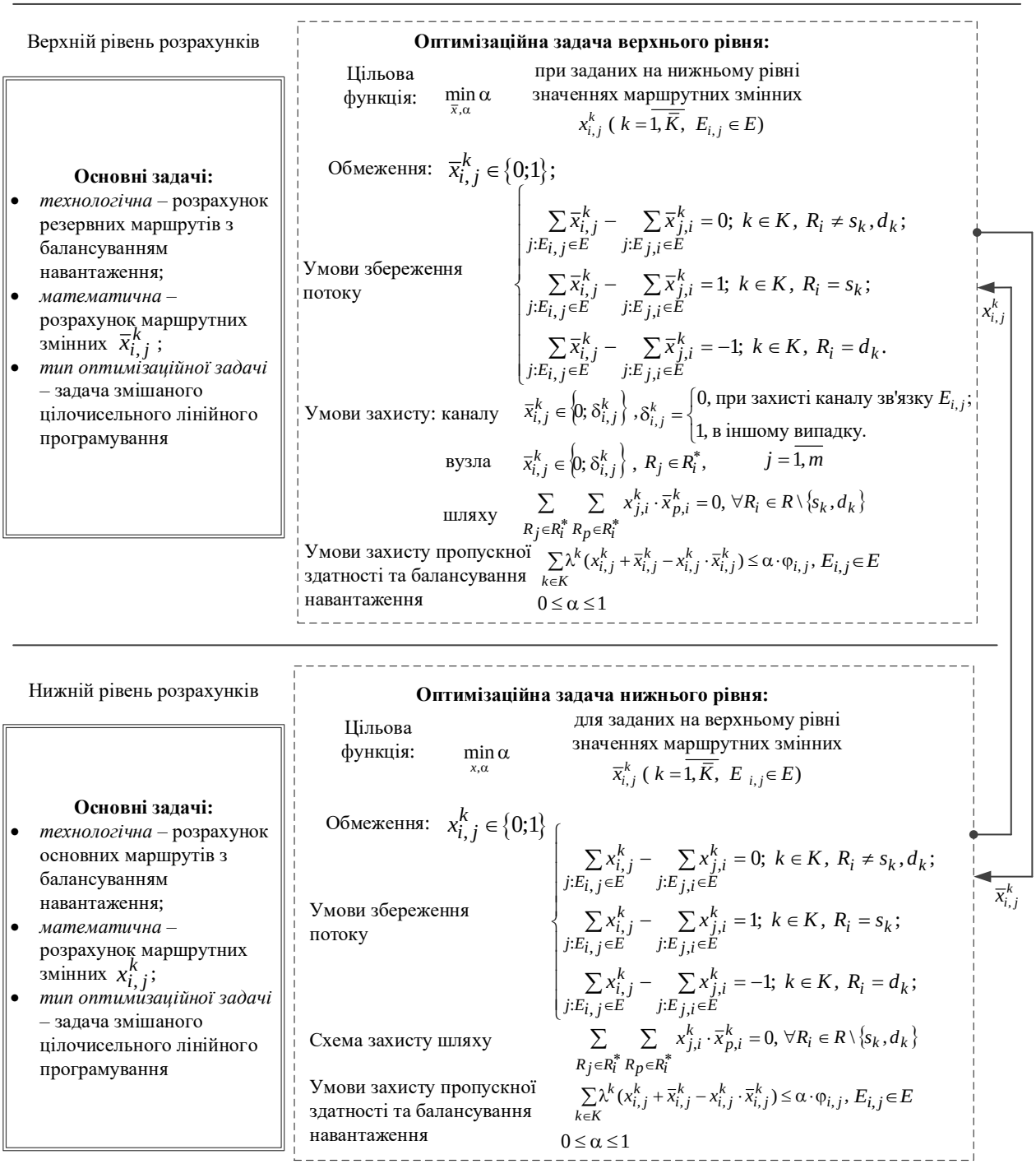


Рис. 2.35. Структура дворівневого методу швидкої перемаршрутизації з балансуванням навантаження в ІКМ [81]

На верхньому рівні ієрархії (рис. 2.35) розраховуються маршрутні змінні $\bar{x}_{i,j}^{k}$, які відповідають за формування (а фактично прогнозування) резервних маршрутів, також шляхом мінімізації змінної α (2.29) за умови фіксованих і розрахованих на нижньому рівні значень маршрутних змінних $x_{i,j}^{k}$. У процесі оптимізації на цьому рівні необхідно виконати умови:

– у разі реалізації схеми захисту шляху – (2.9), (2.17), (2.27) і (2.28);

– у випадку реалізації схем захисту каналу або вузла – (2.9), (2.27), (2.28) і (2.10) або (2.14).

З огляду на те що для верхнього рівня розрахунку значення $x_{i,j}^{k}$ відомі, то умови (2.17) і (2.27) також стають лінійними. Таким чином, процес розв'язання сформульованої задачі швидкої перемаршрутизації в ІКМ набуває ітераційного характеру. Зокрема критерієм завершення розрахунків є досягнення оптимуму (2.29), що проявляється в близькості значень цільової функції (2.29), розрахованої на сусідніх ітераціях, але на різних ієрархічних рівнях.

Важливо зазначити, що для забезпечення захисту каналу, вузла, шляху та пропускної здатності в мережі застосування описаного методу дозволяє відмовитися від розв'язання вихідної нелінійної та досить розмірної оптимізаційної задачі шляхом переходу до ітераційного розв'язання лінійних оптимізаційних задач удвічі меншої розмірності (рис. 2.35).

Це неодмінно позначається на кінцевій масштабованості протокольних рішень щодо швидкої перемаршрутизації з балансуванням навантаження в мережі загалом. Таким чином, ефективність запропонованого методу безпосередньо залежить від кількості ітерацій, за які він забезпечує пошук оптимальних з точки зору критерію (2.29) значень маршрутних змінних, що відповідають за формування основних і резервних маршрутів. Ця функціональна особливість запропонованого методу підлягає додатковому дослідженню.

Особливості роботи методу продемонструємо на числовому прикладі. За основу буде взята структура мережі, показана на рис. 2.36. У табл. 2.4 вказані пропускні здатності каналів зв'язку мережі.

Нехай у мережі (рис. 2.36) необхідно забезпечити вирішення завдань швидкої перемаршрутизації з реалізацією схеми захисту шляху для двох потоків, характеристики яких наведені в табл. 2.5.

Як показали результати проведеного аналізу, запропонований метод швидкої перемаршрутизації в ІКМ для вихідних даних, представлених у табл. 2.4 та 2.5, забезпечував знаходження оптимальних значень маршрутних

змінних (1.1), (2.10) і порога завантаженості (2.28) (рис. 2.37) у середньому за 2–3 ітерації (рис. 2.38). Зокрема, як видно з рис. 2.37 та 2.38, кількість ітерацій збільшується до трьох у разі рівності або близькості значень інтенсивностей потоків пакетів, що передаються. У табл. 2.6–2.8 для прикладу показані результати розрахунків для трьох ітерацій роботи методу за умови $\lambda^1 = 240$ 1/с та $\lambda^2 = 220$ 1/с.

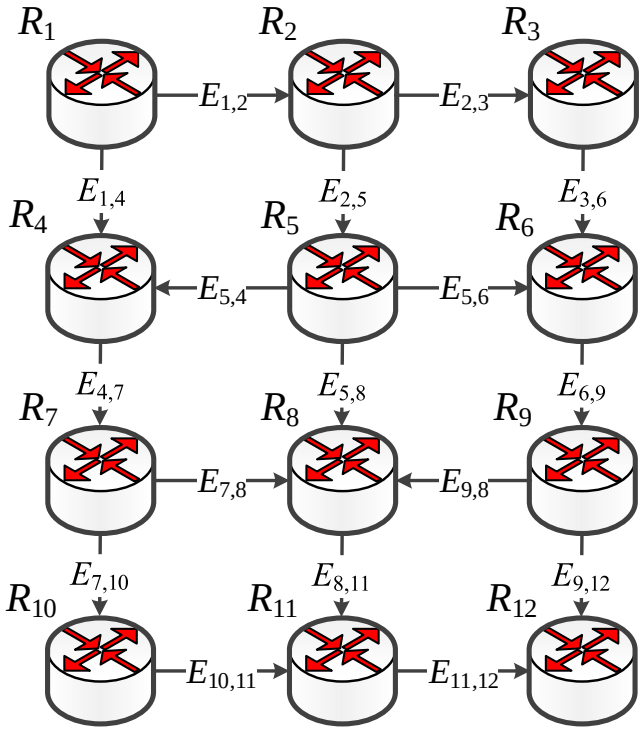


Рис. 2.36. Структура аналізованої ІКМ

Таблиця 2.4

Пропускні здатності каналів зв'язку мережі

Канал зв'язку	Пропускна здатність, 1/с	Канал зв'язку	Пропускна здатність, 1/с	Канал зв'язку	Пропускна здатність, 1/с
$E_{1,2}$	800	$E_{5,6}$	300	$E_{7,10}$	500
$E_{2,3}$	500	$E_{4,7}$	700	$E_{8,11}$	900
$E_{1,4}$	800	$E_{5,8}$	500	$E_{9,12}$	800
$E_{2,5}$	900	$E_{6,9}$	800	$E_{10,11}$	700
$E_{3,6}$	700	$E_{7,8}$	400	$E_{11,12}$	600
$E_{5,4}$	400	$E_{9,8}$	500		

Таблиця 2.5

Характеристики потоків

Номер потоку	Інтенсивність потоку	Відправник	Отримувач
1	$\lambda^1 = 10 \div 250$ 1/с	R_1	R_{12}
2	$\lambda^2 = 10 \div 250$ 1/с	R_5	R_{11}

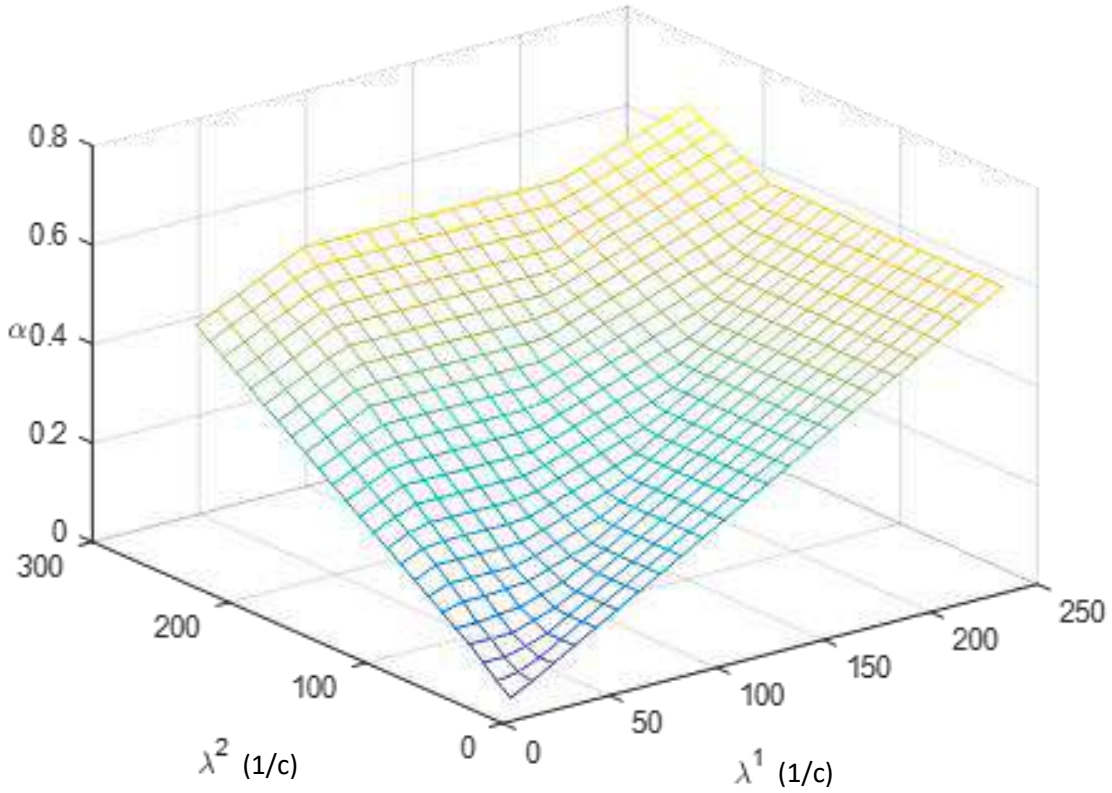


Рис. 2.37. Залежність порога завантаженості каналів зв'язку мережі (2.28) від інтенсивностей потоків пакетів, що передаються (у разі захисту шляхів для двох потоків)

У цих таблицях для кожного каналу вказано коефіцієнт його використання

$$\alpha_{i,j} = \frac{\sum_{k \in K} \max\left[x_{i,j}^k, \bar{x}_{i,j}^k \right] \cdot \lambda^k}{\varphi_{i,j}}. \qquad (2.30)$$

Фактично α (2.28) є граничним, тобто максимальним значенням серед множини коефіцієнтів $\alpha_{i,j}$ (2.30).

Після першої ітерації роботи методу саме завантаженість каналу $E_{7,10}$ визначає значення порога завантаженості каналів зв'язку мережі в 0,92 (табл. 2.6). У цьому випадку для першого потоку основний шлях проходить через маршрутизатори $R_1 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{12}$, а резервний – $R_1 \to R_2 \to R_5$

$\rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$. Тоді як для другого потоку основний шлях визначається маршрутизаторами $R_5 \rightarrow R_8 \rightarrow R_{11}$, а резервний – $R_5 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11}$.

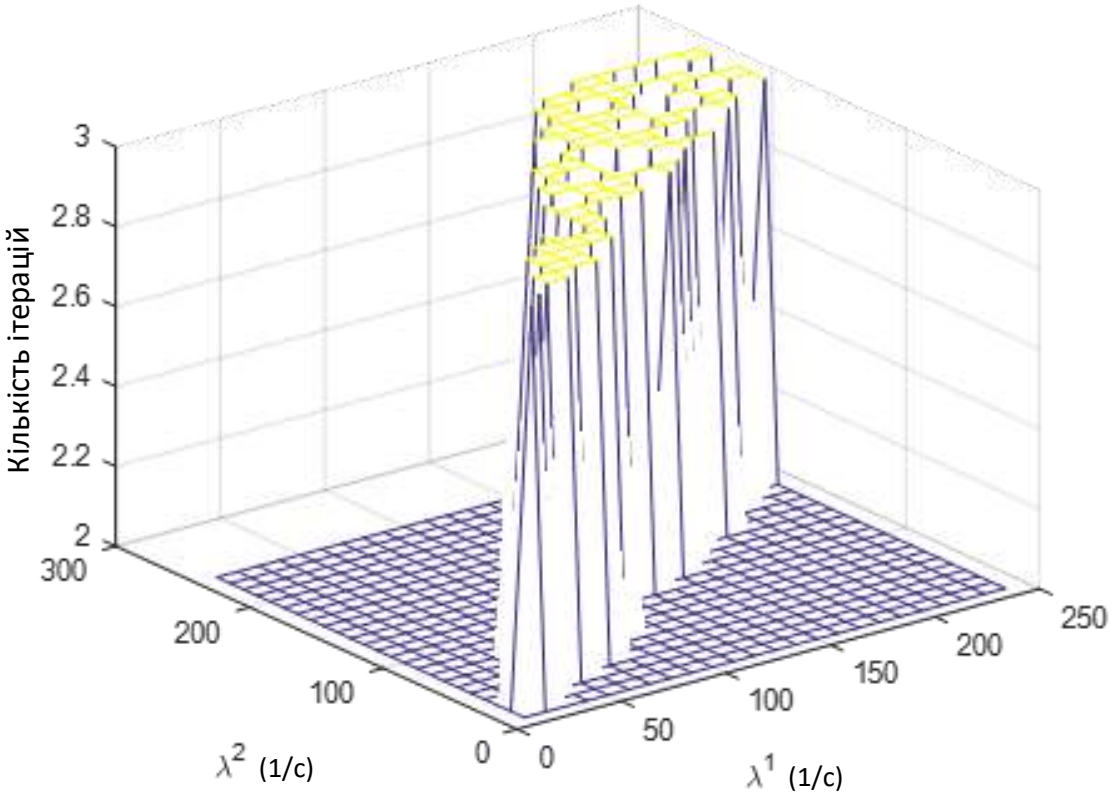


Рис. 2.38. Залежність кількості ітерацій роботи запропонованого методу від інтенсивностей потоків пакетів, що передаються (у разі захисту шляхів для двох потоків)

Після другої ітерації метод забезпечує подальше зниження порога завантаженості каналів зв'язку до 0,8, який (табл. 2.7) визначається за коефіцієнтом використання каналу $E_{5,6}$. У цьому випадку основний шлях для першого потоку є $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{12}$, а резервний – $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$. Зокрема для другого потоку основний і резервний шляхи залишаються незмінними.

І тільки після третьої ітерації метод визначив кінцеве розв'язання задачі швидкої перемаршрутизації з $\alpha = 0,657$ (табл. 2.8). Тут для першого потоку основний шлях представлений маршрутизаторами $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{12}$, а резервний – $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$. Як і раніше, для другого потоку основний і резервний шляхи не змінилися.

Таблиця 2.6

Результати розрахунку після першої ітерації роботи методу $(\alpha = 0{,}92)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	240	0	0	220	0,92
$E_{8,11}$	0	0	220	0	0,244
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	240	0	0	220	0,657
$E_{11,12}$	240	0	0	0	0,4

Продемонструємо особливості роботи запропонованого методу під час реалізації схеми захисту каналу $E_{8,11}$ для тих самих двох потоків (табл. 2.5). У цьому випадку відповідно до умов (2.14) захист каналу $E_{8,11}$ фактично забезпечує захист маршрутизатора R_8. Як показали результати проведеного аналізу, запропонований дворівневий метод одношляхової швидкої перемаршрутизації в ІКМ (табл. 2.4) забезпечував знаходження оптимальних значень маршрутних змінних (1.1), (2.10) і порога завантаженості (2.28) (рис. 2.39) у середньому також за 2–3 ітерації (рис. 2.40).

Таблиця 2.7

Результати розрахунку після другої ітерації роботи методу $(\alpha = 0{,}8)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	240	0	0	0	0,6
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	0	220	0,44
$E_{8,11}$	240	0	220	0	0,511
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	0	0	0	220	0,314
$E_{11,12}$	240	0	0	0	0,4

Запропонований дворівневий метод одношляхової швидкої перемаршрутизації, як і для реалізації схеми захисту шляху (рис. 2.37), забезпечував досить поступову зміну порогового значення завантаженості каналів зв'язку мережі (2.29). Це є перевагою отриманого рішення, тому що воно сприяє відповідній сталій зміні й ключових показників якості обслуговування (середньої затримки та ймовірності втрат пакетів), які багато в чому залежать від завантаженості каналів зв'язку мережі.

Таблиця 2.8

Результати розрахунку після третьої ітерації роботи методу $(\alpha = 0,657)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	240	0	0	0,48
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	0	0	0	0
$E_{3,6}$	0	240	0	0	0,343
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	0	0	0	0
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	240	0	0	0	0,6
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	0	220	0,44
$E_{8,11}$	240	0	220	0	0,511
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	0	0	0	220	0,314
$E_{11,12}$	240	0	0	0	0,4

У табл. 2.9–2.11 для прикладу показані результати розрахунків для трьох ітерацій роботи методу за умови $\lambda^1 = 240$ 1/с і $\lambda^2 = 240$ 1/с. Після першої ітерації роботи методу завантаженість каналу $E_{7,10}$ визначає значення порога завантаженості каналів зв'язку мережі в 0,96 (табл. 2.9). Зокрема для першого потоку основний шлях проходить через маршрутизатори $R_1 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{12}$, а резервний – $R_1 \to R_2 \to R_5 \to R_6 \to R_9 \to R_{12}$. Тоді для другого потоку основний шлях проходить через маршрутизатори $R_5 \to R_8 \to R_{11}$, а резервний – $R_5 \to R_4 \to R_7 \to R_{10} \to R_{11}$.

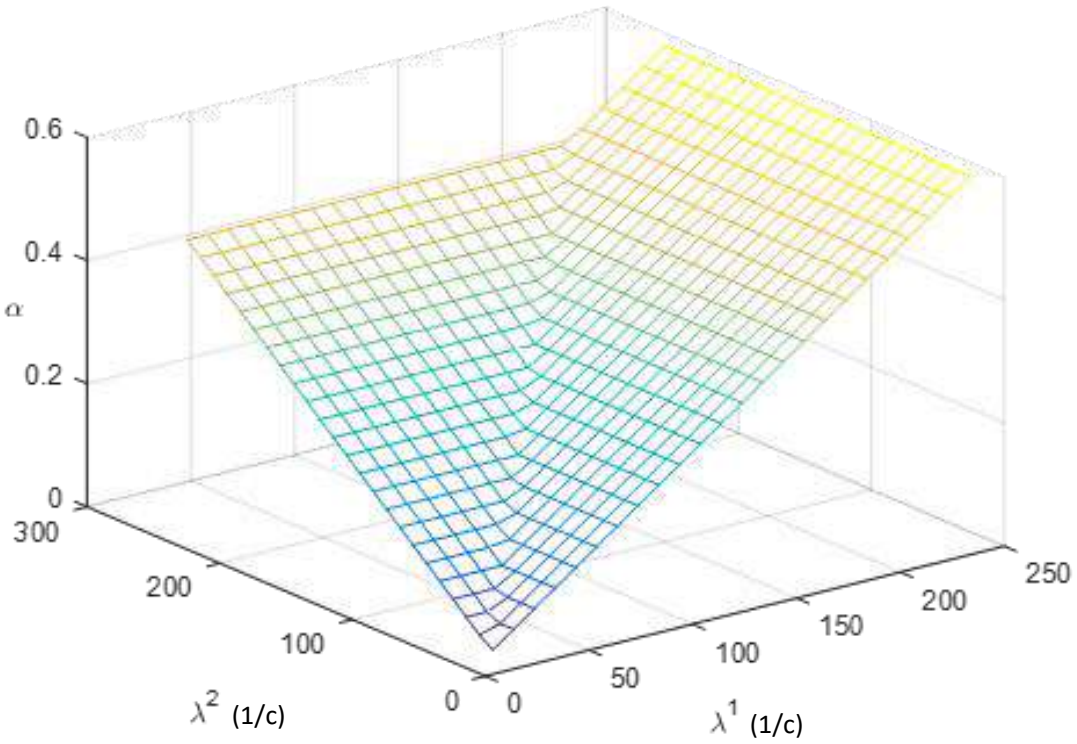


Рис. 2.39. Залежність порога завантаженості каналів зв'язку мережі (2.28) від інтенсивностей потоків пакетів, що передаються (у разі захисту каналу $E_{8,11}$)

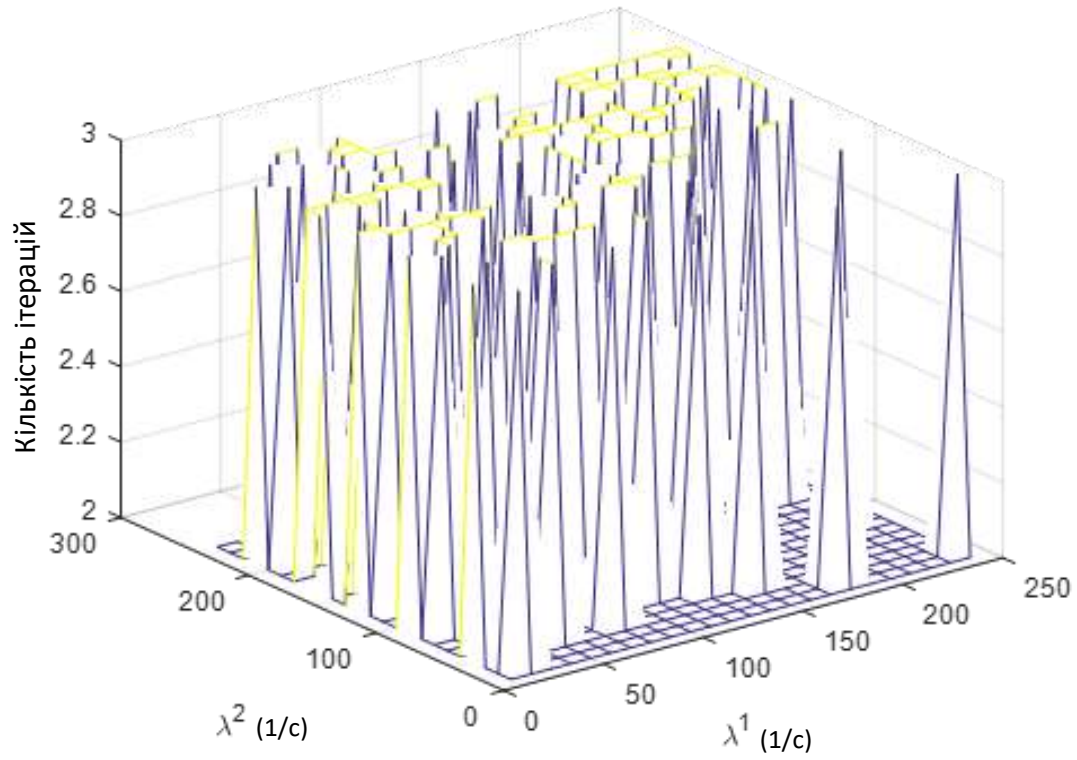


Рис. 2.40. Залежність кількості ітерацій роботи запропонованого методу від інтенсивностей потоків пакетів, що передаються (у разі захисту каналу $E_{8,11}$)

Таблиця 2.9

Результати розрахунку після першої ітерації роботи методу $(\alpha = 0{,}96)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	240	0,6
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	240	0,6857
$E_{5,8}$	0	0	240	0	0,48
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	240	0	0	240	0,96
$E_{8,11}$	0	0	240	0	0,2667
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	240	0	0	240	0,6857
$E_{11,12}$	240	0	0	0	0,4

Після другої ітерації метод забезпечує подальше зниження порога завантаженості каналів зв'язку до 0,8, який у цьому випадку (табл. 2.10) визначається за коефіцієнтом використання каналу $E_{5,6}$. Тут для першого потоку основний шлях містить маршрутизатори $R_1 \to R_2 \to R_3 \to R_6 \to R_9 \to R_{12}$, а резервний – $R_1 \to R_2 \to R_5 \to R_6 \to R_9 \to R_{12}$. У той час як для другого потоку основний і резервний шляхи збігаються та приймають вигляд $R_5 \to R_4 \to R_7 \to R_{10} \to R_{11}$, але вже не містять у собі канал $E_{8,11}$, що захищається.

Таблиця 2.10

Результати розрахунку після другої ітерації роботи методу $(\alpha = 0{,}8)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	240	240	0	0	0,3
$E_{2,3}$	240	0	0	0	0,48
$E_{1,4}$	0	0	0	0	0
$E_{2,5}$	0	240	0	0	0,2667
$E_{3,6}$	240	0	0	0	0,3429
$E_{5,4}$	0	0	240	240	0,6
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	0	0	240	240	0,3429
$E_{5,8}$	0	0	0	0	0
$E_{6,9}$	240	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	240	240	0,48
$E_{8,11}$	0	0	0	0	0
$E_{9,12}$	240	240	0	0	0,3
$E_{10,11}$	0	0	240	240	0,3429
$E_{11,12}$	0	0	0	0	0

Запропонований метод розрахував оптимальний порядок швидкої перемаршрутизації двох потоків пакетів після третьої ітерації з $\alpha = 0{,}6$ (табл. 2.11). Таку завантаженість можна спостерігати для каналу $E_{5,4}$. У цьому випадку для першого потоку основний і резервний шляхи збігаються та проходять через маршрутизатори $R_1 \to R_2 \to R_3 \to R_6 \to R_9 \to R_{12}$ так само, як і для другого потоку маршрутизатори $R_5 \to R_4 \to R_7 \to R_{10} \to R_{11}$ визначають і основний, і резервний шляхи. Однак жоден з розрахованих маршрутів не містить елемент мережі, який захищається, а саме канал $E_{8,11}$.

Таблиця 2.11

Результати розрахунку після третьої ітерації роботи методу $(\alpha = 0,6)$

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	240	240	0	0	0,3
$E_{2,3}$	240	240	0	0	0,48
$E_{1,4}$	0	0	0	0	0
$E_{2,5}$	0	0	0	0	0
$E_{3,6}$	240	240	0	0	0,3429
$E_{5,4}$	0	0	240	240	0,6
$E_{5,6}$	0	0	0	0	0
$E_{4,7}$	0	0	240	240	0,3429
$E_{5,8}$	0	0	0	0	0
$E_{6,9}$	240	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	240	240	0,48
$E_{8,11}$	0	0	0	0	0
$E_{9,12}$	240	240	0	0	0,3
$E_{10,11}$	0	0	240	240	0,3429
$E_{11,12}$	0	0	0	0	0

Як показано в табл. 2.9–2.11, основні шляхи, розраховані для кожного з переданих потоків, можуть проходити через елементи мережі, що захищаються, а саме канал $E_{8,11}$ і маршрутизатор R_8. Резервні шляхи не містили канали та маршрутизатори мережі, що захищалися.

Наведений приклад продемонстрував працездатність запропонованого дворівневого методу швидкої перемаршрутизації. У цьому випадку кінцеве значення порога завантаженості каналів зв'язку мережі (2.29), отримане за допомогою цього методу, повністю відповідало результатам централізованого

розрахунку маршрутних змінних $x_{i,j}^{k}$ і $\bar{x}_{i,j}^{k}$ за умови використання критерію (2.29) і наявності обмежень (1.1), (1.3), (2.9), (2.10), (2.14), (2.17), (2.27), (2.28). Розрахунок змінних (1.1), (2.10) у розв'язанні оптимізаційної задачі змішаного цілочисельного лінійного програмування (Mixed Integer Linear Programming, MILP), представленої цільовою функцією (2.29), виконувалося за допомогою інструментарію Optimization Toolbox середовища MatLab, зокрема функції intlinprog. У цьому випадку згідно з (2.29) було отримано рішення двох завдань: швидкої перемаршрутизації та балансування навантаження.

Результати дослідження для інших мережних структур і вихідних даних також дозволили сформулювати умови, за яких запропонований дворівневий метод демонстрував максимальну ефективність з точки зору отримання оптимальних рішень щодо забезпечення одношляхової швидкої перемаршрутизації з балансуванням навантаження каналів зв'язку ІКМ за критерієм (2.29) і реалізацією необхідних схем захисту елементів мережі. Насамперед, варто зазначити, що з ростом розмірності мережних структур і зв'язності маршрутизаторів ІКМ через наявність більшої кількості маршрутів між парами «відправник–отримувач» і додаткового доступного мережного (канального) ресурсу запропонований метод дозволяє забезпечити краще балансування навантаження за критерієм (2.29) для вирішення завдань швидкої перемаршрутизації. Особливо це помітно в реалізації схем захисту шляху та його пропускної здатності, які вимагають наявності надлишкового мережного ресурсу. Крім того, запропонований метод демонстрував максимальну ефективність у разі одношляхової швидкої перемаршрутизації більшої кількості потоків з різними відправниками та отримувачами, а також високими пакетними інтенсивностями.

2.8.2. Синтез та дослідження лінійної оптимізаційної моделі багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ

Масштабована реалізація багатошляхової стратегії швидкої перемаршрутизації стикається з проблемою подолання нелінійності умов захисту пропускної здатності ІКМ (2.20). Тому в цьому пункті роботи пропонується доповнити модель (1.2), (1.3), (2.9), (2.11), (2.15), (2.17) для забезпечення лінійного вигляду умов захисту пропускної здатності мережі в процесі реалізації як одношляхової, так і багатошляхової швидкої

перемаршрутизації такими модифікованими умовами запобігання перевантаження з метою забезпечення балансування навантаження в мережі [85, 86]:

$$\sum_{k \in K} \lambda^k u_{i,j}^k \le \alpha \varphi_{i,j},\ E_{i,j} \in E \tag{2.31}$$

за умови

$$x_{i,j}^k \le u_{i,j}^k \ \text{і}\ \overline{x}_{i,j}^k \le u_{i,j}^k, \tag{2.32}$$

де $u_{i,j}^k$ також є змінними, які підлягають розрахунку

$$0 \le u_{i,j}^k \le 1 \tag{2.33}$$

і є верхнім порогом (ВП) значень маршрутних змінних основних і резервних шляхів. Критерієм оптимальності розв'язань задач TE FRR залишається вираз (2.29), модифікований під розширену множину керуючих змінних:

$$\min_{x,\overline{x},u,\alpha} \alpha. \tag{2.34}$$

Таким чином, рішення вихідного технологічного завдання багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ із захистом каналу, вузла та пропускної здатності мережі було зведено до розв'язання оптимізаційної задачі лінійного програмування з критерієм (2.34) за наявності множини обмежень (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.33), які обираються залежно від реалізованої схеми захисту.

Особливості роботи моделі TE FRR продемонструємо на розрахунковому прикладі. Зокрема структура досліджуваної мережі зображена на рис. 2.41, а в розривах каналів зв'язку мережі вказані їх пропускні здатності.

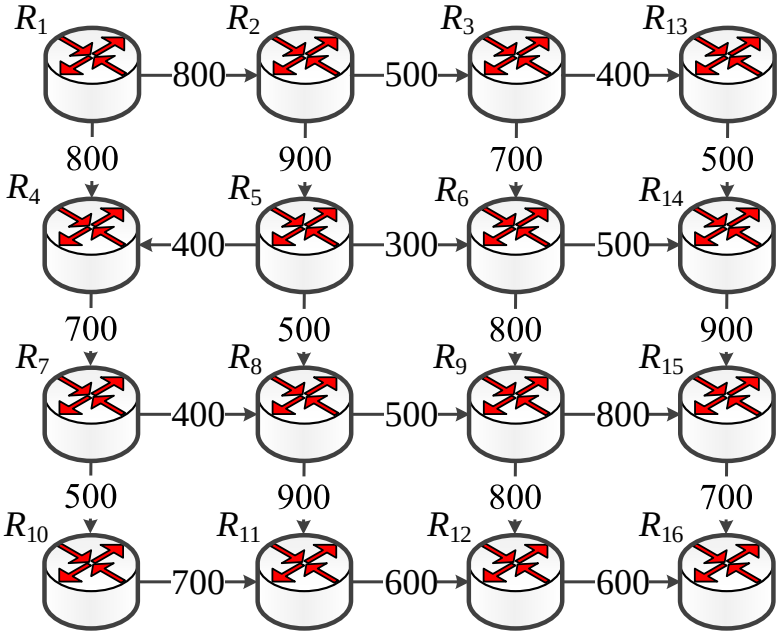


Рис. 2.41. Структура досліджуваної мережі

Нехай у мережі необхідно забезпечити розв'язання задачі багатошляхової швидкої перемаршрутизації двох потоків. У цьому випадку пакети першого потоку передавалися від R_1 до R_{16}. Пакети другого потоку – від R_5 до R_{12}. Припустимо, що інтенсивності цих потоків змінювались у таких межах: $\lambda^1 = 10 \div 400$ 1/с і $\lambda^2 = 10 \div 400$ 1/с. У табл. 2.12 показані мінімальні та максимальні значення виграшу щодо значень критерію (2.34) у реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з каналів зв'язку окремо. Таким чином, у захисті каналів зв'язку використання моделі (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.33) дозволяє покращити критерій (2.34) у середньому від 37,12 % до 59,41 %.

Для наочності на рис. 2.42 показано залежність верхнього порога завантаженості каналів зв'язку від значень інтенсивностей потоків, якщо реалізується, наприклад, схема захисту каналу $E_{8,11}$ у випадку багатошляхової (рис. 2.42, а) або одношляхової маршрутизації (рис. 2.42, б).

Отже, реалізація багатошляхової маршрутизації у разі TE FRR і захисту каналу $E_{8,11}$ дозволяє покращити значення критерію (2.34) від 44,44 % до 61,54 % порівняно з використанням одношляхової ТЕ-маршрутизації (рис. 2.43).

Більш докладно розглянемо випадок використання запропонованої моделі TE FRR у процесі передачі пакетів двох потоків з інтенсивностями $\lambda^1 = 400$ 1/с та $\lambda^2 = 300$ 1/с (табл. 2.13). У цьому випадку завантаженість для кожного каналу зв'язку $E_{i,j} \in E$ визначалася як

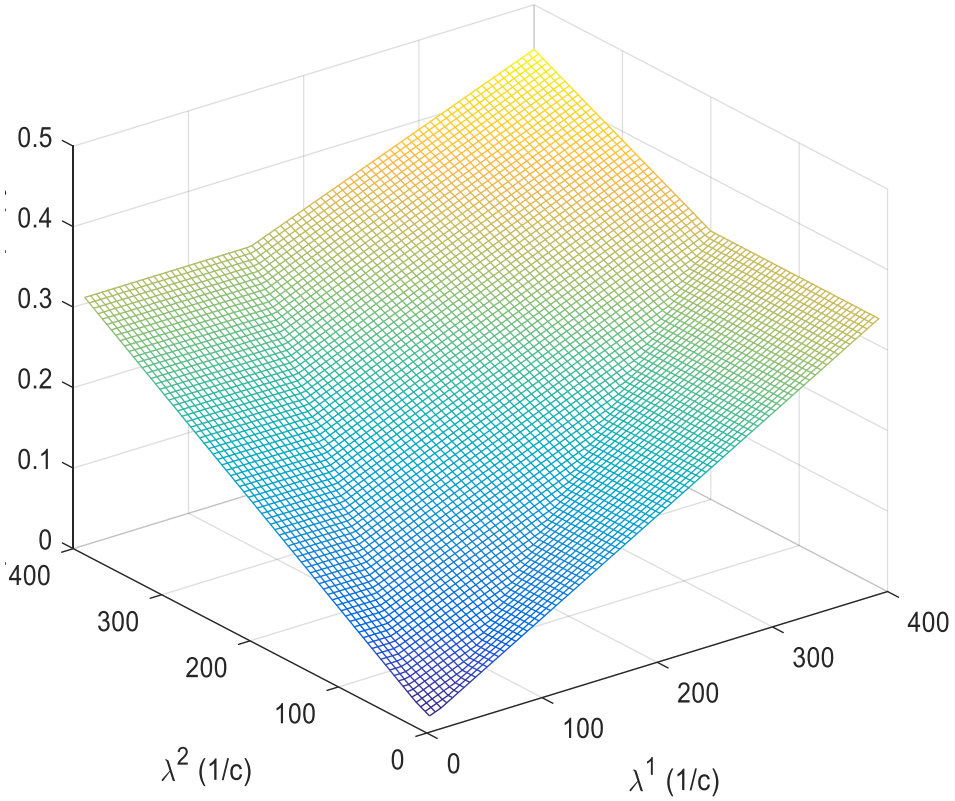
$$\alpha_{i,j} = \frac{\sum\limits_{k \in K} u_{i,j}^k \lambda^k}{\varphi_{i,j}}. \qquad (2.35)$$

У табл. 2.13 також показано порядок одно- та багатошляхової маршрутизації та балансування двох потоків за каналами зв'язку мережі з використанням запропонованої моделі TE FRR (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.34). Зокрема α (2.34) є максимальним значенням серед множини коефіцієнтів $\alpha_{i,j}$ (2.35). Відповідно до отриманих результатів розрахунку (табл. 2.13) реалізація одношляхової маршрутизації в захисті каналу $E_{8,11}$ забезпечила значення α=0,8, тоді як застосування багатошляхової маршрутизації – α=0,39, що на 51,25 % краще, ніж у разі одношляхової стратегії.

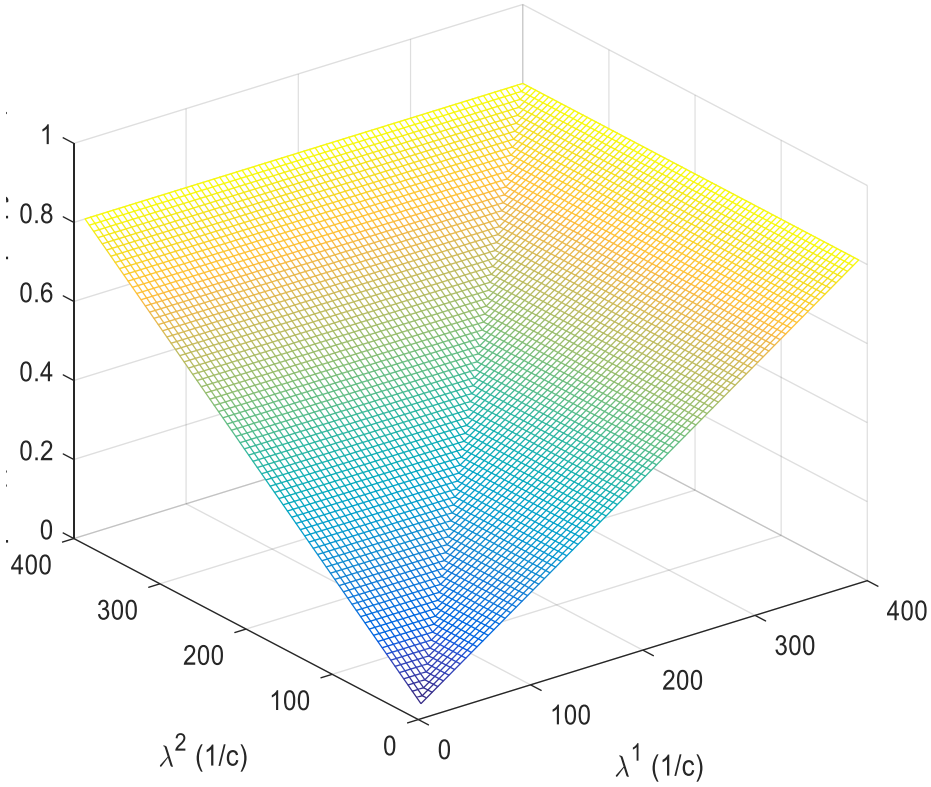
Таблиця 2.12

Виграш за критерієм (2.34) у разі реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з каналів зв'язку мережі окремо

Канал зв'язку, що захищається	Виграш, %	
	min	max
$E_{1,2}$	28,57	58,33
$E_{2,3}$	28,57	61,54
$E_{1,4}$	37,5	58,33
$E_{2,5}$	47,37	58,33
$E_{3,6}$	44,44	61,54
$E_{5,4}$	37,5	61,54
$E_{5,6}$	37,5	61,54
$E_{4,7}$	23,08	37,05
$E_{5,8}$	40,17	61,54
$E_{6,9}$	44,44	61,54
$E_{7,8}$	44,44	61,54
$E_{8,9}$	28,57	61,54
$E_{7,10}$	41,18	58,33
$E_{8,11}$	44,44	61,54
$E_{9,12}$	16,67	60,55
$E_{10,11}$	41,18	58,33
$E_{11,12}$	23,08	58,33
$E_{3,13}$	47,37	61,54
$E_{13,14}$	47,37	61,54
$E_{6,14}$	47,37	61,54
$E_{14,15}$	47,37	61,54
$E_{9,15}$	47,37	61,54
$E_{15,16}$	16,67	58,33
$E_{12,16}$	28,57	58,33



а) за умови багатошляхової маршрутизації



б) за умови одношляхової маршрутизації

Рис. 2.42. Залежність верхнього порога завантаженості каналів зв'язку мережі від значень інтенсивностей потоків, якщо реалізується схема захисту каналу $E_{8,11}$

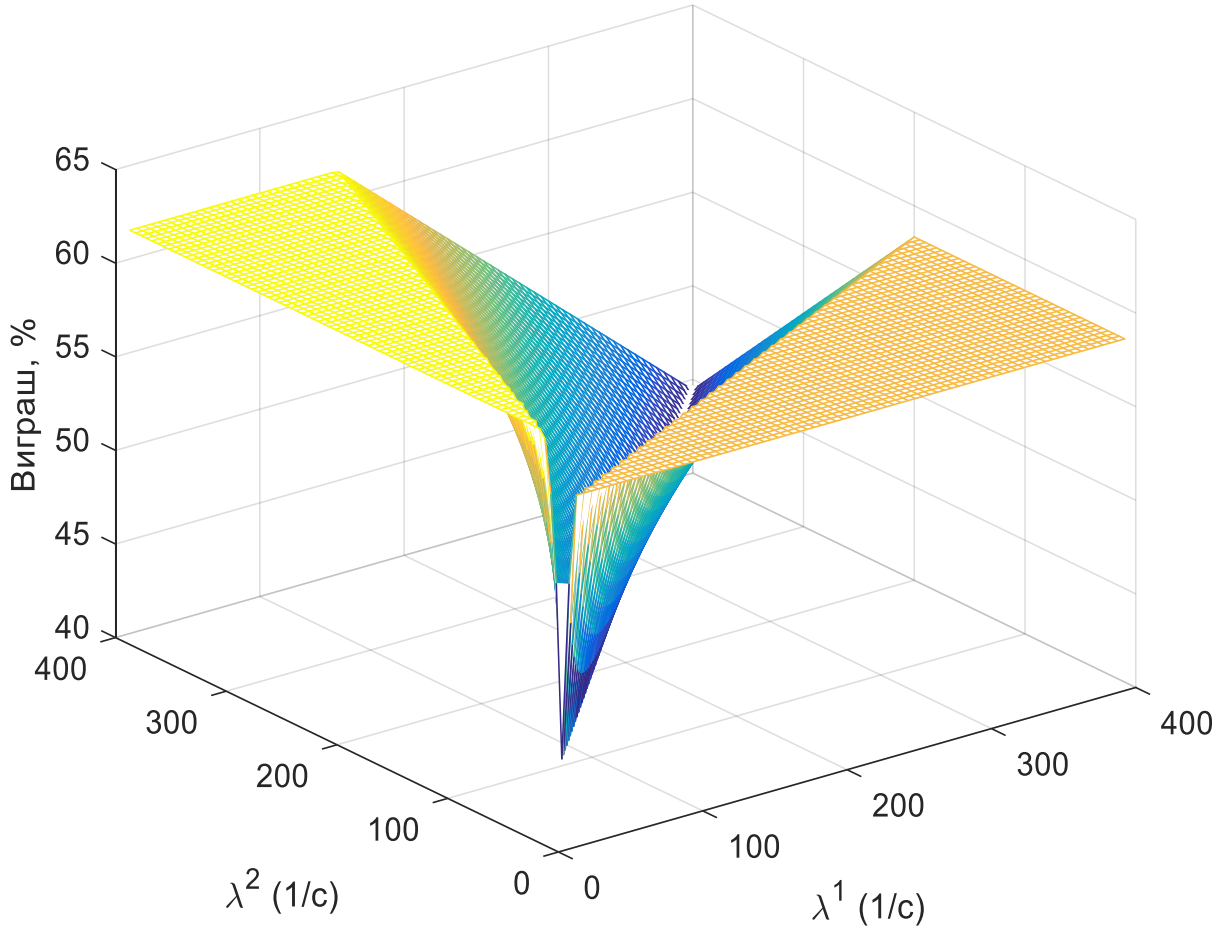


Рис. 2.43. Виграш за критерієм (2.34) від реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації (захист каналу $E_{8,11}$)

У табл. 2.14 показані мінімальні та максимальні значення виграшу щодо значень критерію (2.34) під час реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з вузлів мережі окремо. Таким чином, у разі захисту вузлів мережі застосування запропонованої моделі дозволяє покращити критерій (2.34) в середньому від 31,5 % до 56,3 %.

На рис. 2.44, наприклад, показано, що реалізація багатошляхової маршрутизації за умови захисту вузла R_9 дозволяє від 16,67 % до 60,55 % покращити значення критерію (2.34) порівняно з одношляховою маршрутизацією.

Таблиця 2.13

Результати порівняння за критерієм (2.34) одно- та багатошляхової швидкої перемаршрутизації в разі захисту каналу $E_{8,11}$

КЗ	Багатошляхова маршрутизація						$\alpha_{i,j}$	Одношляхова маршрутизація						$\alpha_{i,j}$
	Перший потік			Другий потік				Перший потік			Другий потік			
	ОМ	РМ	ВП	ОМ	РМ	ВП		ОМ	РМ	ВП	ОМ	РМ	ВП	
$E_{1,2}$	257,50	256,93	267,91	0	0	0	0,37	400	400	400	0	0	0	0,50
$E_{2,3}$	188,42	194,44	194,44	0	0	0	0,39	0	0	0	0	0	0	0
$E_{1,4}$	142,50	143,07	192,67	0	0	0	0,35	0	0	0	0	0	0	0
$E_{2,5}$	69,08	62,49	142,64	0	0	0	0,32	400	400	400	0	0	0	0,44
$E_{3,6}$	133,28	138,09	171,75	0	0	0	0,36	0	0	0	0	0	0	0
$E_{5,4}$	8,62	9,08	32,03	83,38	92,69	106,81	0,35	0	0	0	300	300	300	0,75
$E_{5,6}$	19,99	23,58	23,57	89,15	93,09	93,09	0,39	0	0	0	0	0	0	0
$E_{4,7}$	151,12	152,15	163,14	83,38	92,69	99,06	0,37	0	0	0	300	300	300	0,43
$E_{5,8}$	40,47	29,83	50,14	127,47	114,22	134,53	0,37	400	400	400	0	0	0	0,80
$E_{6,9}$	95,78	102,81	153,04	89,15	93,09	146,44	0,37	0	0	0	0	0	0	0
$E_{7,8}$	68,42	43,88	82,50	32,66	6,52	52,99	0,34	0	0	0	0	0	0	0
$E_{8,9}$	69,45	73,71	73,71	114,23	120,74	120,74	0,39	400	400	400	0	0	0	0,80
$E_{7,10}$	82,70	108,27	108,27	50,72	86,17	86,17	0,39	0	0	0	300	300	300	0,60
$E_{8,11}$	39,44	0	137,71	45,90	0	137,98	0,31	0	0	0	0	0	0	0
$E_{9,12}$	49,00	60,85	76,63	203,38	213,83	222,45	0,37	400	400	400	0	0	0	0,50
$E_{10,11}$	82,70	108,27	140,51	50,72	86,17	111,48	0,36	0	0	0	300	300	300	0,43
$E_{11,12}$	122,14	108,27	126,88	96,62	86,17	100,64	0,382	0	0	0	300	300	300	0,50
$E_{3,13}$	55,14	56,35	78,87	0	0	0	0,34	0	0	0	0	0	0	0
$E_{13,14}$	55,14	56,35	89,92	0	0	0	0,33	0	0	0	0	0	0	0
$E_{6,14}$	57,49	58,86	90,32	0	0	0	0,33	0	0	0	0	0	0	0
$E_{14,15}$	112,63	115,21	168,42	0	0	0	0,33	0	0	0	0	0	0	0
$E_{9,15}$	116,23	115,67	175,17	0	0	0	0,34	0	0	0	0	0	0	0
$E_{15,16}$	228,86	230,88	240,10	0	0	0	0,37	0	0	0	0	0	0	0
$E_{12,16}$	171,14	169,12	183,21	0	0	0	0,37	400	400	400	0	0	0	0,67

Таблиця 2.14

Виграш за критерієм (2.34) під час реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з вузлів мережі окремо

Вузол, що захищається	Виграш, %	
	min	max
R_2	28,57	58,33
R_3	28,57	61,54
R_4	23,08	37,5
R_6	33,33	61,54
R_7	23,08	37,5
R_8	30,97	60,55
R_9	16,67	60,55
R_{10}	41,18	58,33
R_{11}	41,18	58,33
R_{13}	47,37	61,54
R_{14}	47,37	61,54
R_{15}	16,67	58,33

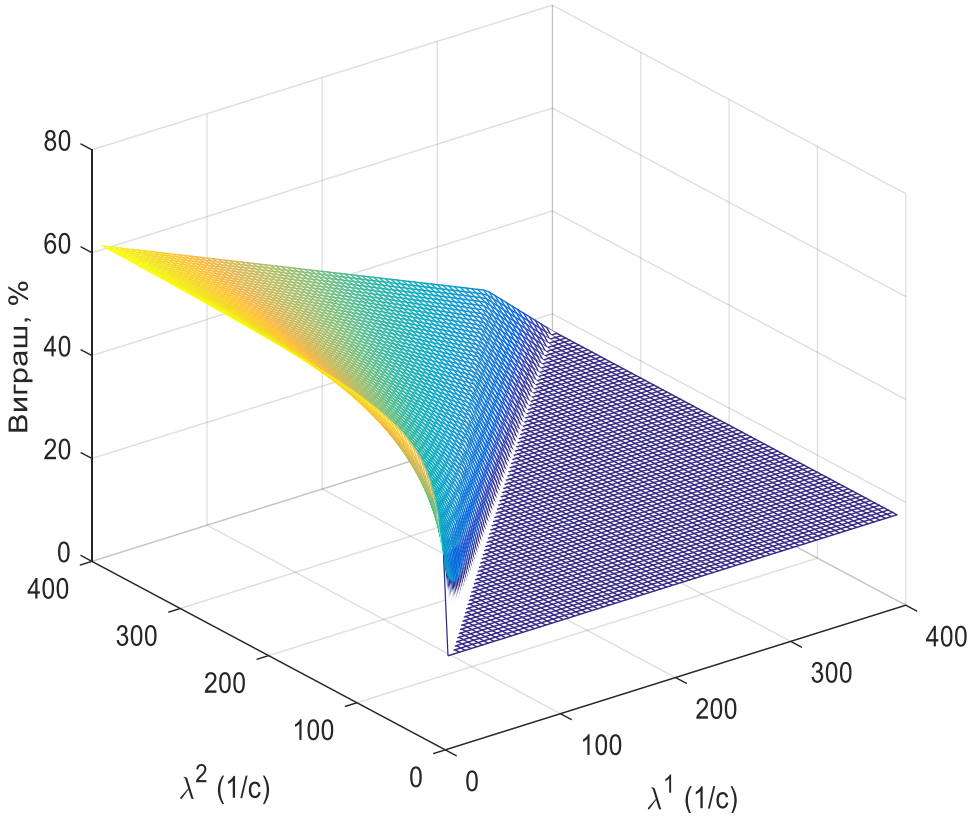


Рис. 2.44. Виграш за критерієм (2.34) від реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації (захист вузла R_9)

2.9. Потокова модель відмовостійкої маршрутизації із захистом шлюзу за замовчуванням

Як було показано в підрозділі 2.2, сфера застосування відмовостійкої маршрутизації не обмежується лише захистом елементів транспортної мережі. Дуже важливим моментом у підвищенні відмовостійкості ІКМ є реалізація захисту шлюзу за замовчуванням, за допомогою якого мережі доступу комутуються до транспортної мережі. Результати аналізу наявних теоретичних та протокольних рішень у цьому напрямі дозволили сформулювати такі вимоги до перспективних моделей і методів відмовостійкої маршрутизації із захистом шлюзу за замовчуванням: орієнтація на потокові рішення; підтримка балансування навантаження між інтерфейсами віртуального шлюзу за замовчуванням; забезпечення погодженого розв'язання задач захисту шлюзу за замовчуванням на границі мереж і швидкої перемаршрутизації на рівні транспортної мережі.

2.9.1. Графова модель відмовостійкої маршрутизації в ІКМ

Нехай структура ІКМ описується за допомогою графа $\Gamma = (M, L)$ (рис. 2.45). Зокрема $M = R \bigcup V$ – множина вершин графа, що містить дві підмножини: $R = \left\{ R_i, i = \overline{1,m} \right\}$ – множина вершин, що моделюють маршрутизатори транспортної мережі (ТМ), $V = \left\{ V_j, j = \overline{1,v} \right\}$ – множина вершин, що моделюють мережі доступу (МД) ІКМ [87–90].

У свою чергу множина R також містить дві підмножин: R^+ – множина вершин, що моделюють приграничні маршрутизатори транспортної мережі, тобто маршрутизатори, до яких можуть бути підключені мережі доступу, де $m^+ = \left| R^+ \right|$ – загальне число приграничних маршрутизаторів у ТМ; R^- – множина вершин, що моделюють транзитні маршрутизатори транспортної мережі, де $m^- = \left| R^- \right|$ – загальна кількість транзитних маршрутизаторів у ТМ.

Підмножиною множини R^+ є множина R_j^+, що моделює ті приграничні маршрутизатори, а точніше їх інтерфейси, які утворюють віртуальний маршрутизатор для j-ї мережі доступу, що описується вершиною V_j. Тоді $m_j^+ = \left| R_j^+ \right|$ – загальне число приграничних маршрутизаторів, що утворюють

віртуальний маршрутизатор для j-ї мережі доступу. Наприклад, як показано на рис. 2.46, для першої мережі доступу віртуальним маршрутизатором є множина маршрутизаторів, представлених вершинами R_1, R_2 та R_3, тобто $m_1^+ = 3$; для другої мережі віртуальний маршрутизатор утворюють інтерфейси маршрутизаторів, що моделюються вершинами R_2 та R_3, тобто $m_2^+ = 2$.

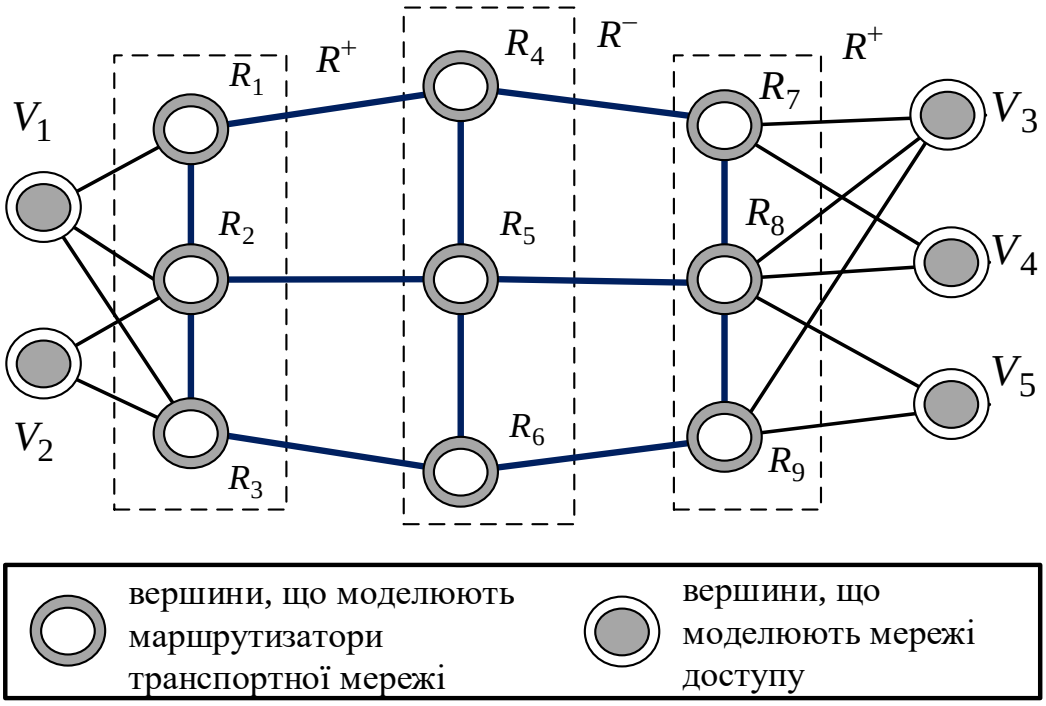


Рис. 2.45. Приклад опису структури ІКМ у вигляді графа

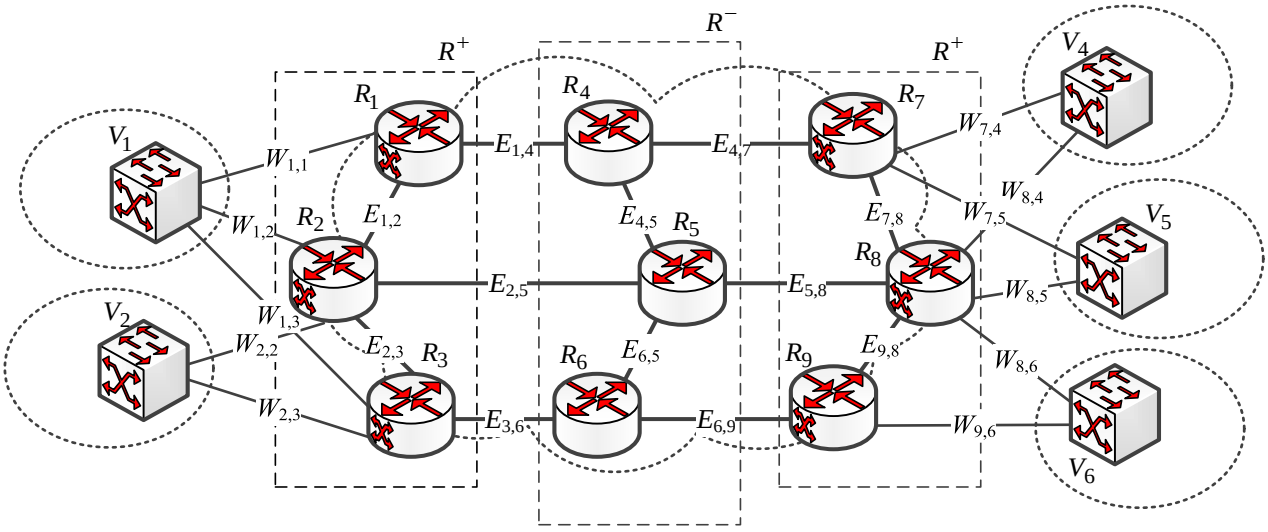


Рис. 2.46. Приклад структури ІКМ,
яка містить транспортну мережу та п’ять мереж доступу

Отже, множини $R_j^+ \ \left(j=\overline{1,v}\right)$ можуть перетинатися, тому що інтерфейси одного й того ж приграничного маршрутизатора можуть бути у складі різних віртуальних маршрутизаторів. У свою чергу множина дуг $L=E\bigcup W$ вихідного графа Г містить також дві підмножини: $E=\left\{E_{i,j}, i, j=\overline{1,m}, i\neq j\right\}$ – множина каналів зв'язку транспортної мережі, $W=\left\{W_{i,j}, i=\overline{1,v}, j=\overline{1,m^+}\right\}$ – множина ліній доступу, що з'єднують мережі доступу та приграничні маршрутизатори транспортної мережі. Кожній дузі $E_{i,j}\in E$ графа, що моделює відповідний КЗ транспортної мережі, як і раніше, ставиться у відповідність пропускна здатність цього каналу.

2.9.2. Потокова модель відмовостійкої маршрутизації в ІКМ

Нехай кожному k-му потоку з множини K, що надходять на приграничні маршрутизатори від мереж доступу, зіставляється низка параметрів: V_s^k – мережа доступу, яка є джерелом k-го потоку; V_d^k – мережа доступу, що є отримувачем k-го потоку пакетів; λ^k – це, як і раніше, середня інтенсивність пакетів k-го потоку (1/с). Тоді внаслідок розв'язання задачі відмовостійкої маршрутизації в ІКМ за допомогою пропонованої моделі необхідно розрахувати три типи керуючих змінних, які належать до основного маршруту:

– $x_{i,j}^k$ – маршрутна змінна, що характеризує частку k-го потоку в каналі зв'язку транспортної мережі, представленого дугою $E_{i,j}$;

– $y_{i,j}^k$ – змінна доступу, що характеризує частку k-го потоку, який протікає в лінії доступу, представленій дугою $W_{i,j}$, тобто від мережі доступу V_i до приграничного маршрутизатора R_j транспортної мережі;

– $z_{j,i}^k$ – змінна доступу, що характеризує частку k-го потоку, який протікає в лінії доступу, представленій дугою $W_{j,i}$, тобто від приграничного маршрутизатора R_j ТМ до мережі доступу V_i.

Кількість маршрутних змінних $x_{i,j}^k$ відповідає добутку $|K|\cdot|E|$, тоді як загальна кількість змінних доступу $y_{i,j}^k$ і $z_{j,i}^k$ визначається як $v\cdot m^+\cdot|K|$.

На керуючі змінні згідно з їх фізичним змістом накладається низка обмежень. На маршрутні змінні $x_{i,j}^k$ у разі використання одношляхової маршрутизації потоків у ТМ мають місце умови (1.1), а у випадку багатошляхової – (1.2). Під час підключення в певний момент часу мережі доступу лише до одного інтерфейсу віртуального маршрутизатора, як це реалізовано, наприклад, у протоколі HSRP [26], на змінні доступу накладаються обмеження у вигляді

$$\begin{cases} y_{i,j}^k \in \{0;1\}; \\ \sum\limits_{j:R_j \in R_i^+} \prod\limits_{k \in K} y_{i,j}^k = 1; \end{cases} \text{ і } \begin{cases} z_{j,i}^k \in \{0;1\}; \\ \sum\limits_{j:R_j \in R_i^+} \prod\limits_{k \in K} z_{j,i}^k = 1. \end{cases} \quad (2.36)$$

За можливості балансування трафіку за всіма доступними інтерфейсами віртуального маршрутизатора так, як це реалізовано в протоколах VRRP, GLBP і CARP [24, 25, 27], умови (2.36) замінюються на нерівності:

$$0 \le y_{i,j}^k \le 1 \text{ та } 0 \le z_{j,i}^k \le 1. \quad (2.37)$$

Крім того, на доповнення до (2.37) мають місце такі умови:

$$\sum_{R_j \in R_p^+} y_{p,j}^k = 1,\ V_p = V_s^k; \quad (2.38)$$

$$\sum_{R_j \in R_h^+} z_{j,h}^k = 1,\ \ V_h = V_d^k. \quad (2.39)$$

Ці умови вводяться для того, щоб не допустити втрат пакетів на ділянках «мережа доступу – віртуальний маршрутизатор ТМ» (2.38) і «віртуальний маршрутизатор ТМ – мережа доступу» (2.39).

Для забезпечення узгодженості в процесі розрахунку керуючих змінних, що відповідають за реалізацію відмовостійкої маршрутизації, важливо виконати дещо видозмінені порівняно з (1.3) умови збереження потоку:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = 0; k \in K,\ R_i \in R^-; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = y_{p,i}^k; k \in K,\ R_i \in R^+,\ V_p = V_s^k; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = -z_{i,h}^k; k \in K,\ R_i \in R^+,\ V_h = V_d^k. \end{cases} \quad (2.40)$$

У (2.40) індекс j вказує на номер вхідного або вихідного інтерфейсу i-го маршрутизатора, через який k-й потік відповідно надходить або відправляється

через маршрутизатор. Умови (2.40) гарантують відсутність втрат пакетів на маршрутизаторах ТМ і в ІКМ загалом, а також те, що потік будь-якого користувача з МД приймається та обслуговується транспортною мережею.

Для забезпечення відмовостійкості ІКМ загалом, у якій МД з ТМ з'єднані через певний віртуальний інтерфейс/інтерфейси маршрутизатора, вводяться додаткові керуючі змінні, які визначають резервний шлях для тих самих відправника та отримувача [5, 55–59]. З математичної точки зору необхідно розрахувати такі додаткові керуючі змінні:

– $\overline{x}_{i,j}^{k}$ – маршрутна змінна, що характеризує частку k-го потоку в каналі зв'язку $E_{i,j}$ резервного шляху відповідно до умов (2.10) або (2.11) для ТМ;

– $\overline{y}_{i,j}^{k}$ – змінна доступу, що характеризує частку k-го потоку, який протікає в резервній лінії доступу $W_{i,j}$;

– $\overline{z}_{j,i}^{k}$ – змінна доступу, що характеризує частку k-го потоку, який протікає в резервній лінії доступу $W_{j,i}$.

Як і у випадку формування основного маршруту, змінні доступу для резервного шляху обмежені умовами, аналогічними до (2.36) та (2.39). Крім того, ті самі умови (2.38)–(2.40) відповідно повинні запобігати втратам пакетів і забезпечити збереження потоку в транспортній мережі для резервного шляху. Для уникнення можливого перевантаження каналів зв'язку ТМ і забезпечення захисту пропускної здатності ІКМ загалом вводяться умови (2.20).

Для реалізації схеми захисту шлюзу за замовчуванням з можливістю балансування навантаження за всіма доступними інтерфейсами віртуального маршрутизатора в модель вводяться такі нелінійні умови [89, 90]:

$$\sum_{i:V_i \in V} y_{i,j}^{k} \overline{y}_{i,j}^{k} + \sum_{n:E_{j,n} \in E} x_{j,n}^{k} \overline{x}_{j,n}^{k} = 0\,,\ R_j \in R^{+}\,. \qquad (2.41)$$

Якщо ці умови виконуються, це гарантує, що пригранічний маршрутизатор R_j (тобто всі інцидентні до цього вузла канали зв'язку та лінії доступу) використовується або основним, або резервним шляхом.

У запропонованій моделі отримані також такі лінійні умови у здійсненні підключення мережі доступу лише до одного інтерфейсу віртуального маршрутизатора (тобто без балансування навантаження) [89, 90]:

$$\begin{cases} x_{j,n}^{k} + \overline{x}_{j,n}^{k} \le 1; \\ y_{i,j}^{k} + \overline{y}_{i,j}^{k} \le 1. \end{cases} \qquad (2.42)$$

Виконання умов (2.42) гарантує, що пригранічний маршрутизатор R_j буде використано k-м потоком лише в одному шляху – основному або резервному.

За аналогією з (2.23), (2.24) за критерій оптимальності отримуваних рішень щодо відмовостійкої маршрутизації пропонується вибрати мінімум такої цільової функції [89]:

$$J = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k + \sum_{k \in K} \sum_{W_{i,j} \in W} b_{i,j}^k y_{i,j}^k + \\ + \sum_{k \in K} \sum_{W_{i,j} \in W} \bar{b}_{i,j}^k \bar{y}_{i,j}^k + \sum_{k \in K} \sum_{W_{j,i} \in W} a_{j,i}^k z_{j,i}^k + \\ + \sum_{k \in K} \sum_{W_{j,i} \in W} \bar{a}_{j,i}^k \bar{z}_{j,i}^k - \sum_{k \in K} \sum_{E_{i,j} \in E} d_{i,j}^k x_{i,j}^k \bar{x}_{i,j}^k \ , \qquad (2.43)$$

де $c_{i,j}^k$ і $\bar{c}_{i,j}^k$ – метрики каналів зв'язку, які використовуються в обчисленні основного та резервного шляхів відповідно в ТМ, а сьомий доданок вноситься в цільову функцію для покращення масштабованості [74] шляхом максимізації збігу між основним і резервним шляхами за незахищеними каналами зв'язку, тоді як $d_{i,j}^k >> c_{i,j}^k$ і $d_{i,j}^k >> \bar{c}_{i,j}^k$.

Вагові коефіцієнти $b_{i,j}^k$ і $a_{j,i}^k$ у свою чергу є набором метрик доступу для k-го потоку, який визначає умовну вартість підключення МД до пригранічного маршрутизатора під час вибору шлюзу за замовчуванням; $\bar{b}_{i,j}^k$ і $\bar{a}_{j,i}^k$ мають той самий фізичний зміст, але для резервних ліній доступу. Вибір цих показників у запропонованому рішенні визначається за допомогою зворотних функцій коефіцієнтів готовності ліній доступу. Отже, перший та другий доданки у виразі (2.43) описують умовну вартість використання каналів зв'язку ТМ основним і резервним шляхами, а доданки з третього до шостого відображають умовну вартість на використання основних і резервних ліній доступу для вхідного трафіку до ТМ або вихідного трафіку з ТМ відповідно.

Таким чином, у вирішенні технологічного завдання щодо відмовостійкої маршрутизації за умови реалізації одношляхової стратегії в ТМ без балансування навантаження на рівні пригранічних маршрутизаторів необхідно розв'язати задачу змішаного цілочисельного нелінійного програмування (MINLP) у ході мінімізації (2.43) з урахуванням умов (1.1), (2.20), (2.36), (2.40), (2.42). У разі реалізації багатошляхової стратегії в ТМ та балансування навантаження на рівні пригранічних маршрутизаторів оптимізаційна задача

прийме вигляд задачі нелінійного програмування (NLP) з обмеженнями (1.2), (2.20), (2.37)–(2.41).

2.9.3. Дослідження схеми захисту шлюзу за замовчуванням у разі використання різних стратегій маршрутизації в ІКМ

Нехай мережа доступу V_1 є джерелом потоку інтенсивністю 300 1/с, а отримувачем пакетів цього потоку є мережа доступу V_6 (рис. 2.46). Необхідно забезпечити захист шлюзу за замовчуванням – маршрутизатор R_2. Продемонструємо функціонування схеми захисту шлюзу за замовчуванням для випадків одношляхової та багатошляхової маршрутизації. Пропускні здатності каналів зв'язку ТМ наведені в табл. 2.15. Під час дослідження встановлено, що саме ці значення визначали маршрутні метрики $c_{i,j}^k$ та $\bar{c}_{i,j}^k$ (2.43) для всіх відповідних каналів зв'язку транспортної мережі, які розраховувалися за аналогією з метрикою протоколу IGRP, а саме $10^7/\varphi_{i,j}$. Це дозволило забезпечити розрахунок маршрутів з максимальною пропускною здатністю.

Таблиця 2.15

Пропускні здатності каналів зв'язку транспортної мережі

Канал зв'язку ТМ	$E_{1,2}$	$E_{2,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$
Пропускна здатність, 1/с	150	110	350	400	400	300
Канал зв'язку ТМ	$E_{6,5}$	$E_{4,7}$	$E_{5,8}$	$E_{6,9}$	$E_{7,8}$	$E_{9,8}$
Пропускна здатність, 1/с	200	200	800	350	100	120

Для забезпечення вибору найбільш надійного приграничного маршрутизатора (інтерфейсу віртуального маршрутизатора) у процесі реалізації відмовостійкої маршрутизації пропонується вагові коефіцієнти (метрики доступу) $b_{i,j}^k$, $\bar{b}_{i,j}^k$ і $a_{j,i}^k$, $\bar{a}_{j,i}^k$ у (2.43) обирати як функцію, що є оберненою до коефіцієнтів готовності $\left(A_{i,j}\right)$ тієї чи іншої лінії доступу $\left(W_{i,j}\right)$ та/або інтерфейсу приграничного маршрутизатора. Нехай коефіцієнти готовності ліній доступу представлені в табл. 2.16.

Таблиця 2.16

Коефіцієнти готовності ліній доступу

Лінія доступу	$W_{1,1}$	$W_{1,2}$	$W_{1,3}$	$W_{8,6}$	$W_{9,6}$
$A_{i,j}$	0,999	0,9999	0,998	0,9995	0,999

Тоді варіант розв'язання задачі одношляхової відмовостійкої маршрутизації з реалізацією схеми захисту шлюзу за замовчуванням, отриманий з використанням запропонованої моделі, наведено на рис. 2.47. Інтенсивності потоків пакетів для основного і резервного шляхів показано в розривах каналів зв'язку мережі. Основний шлях формується маршрутизаторами транспортної мережі таким чином: $R_2 \to R_5 \to R_8$. Вибір цього рішення визначається, з одного боку, більш надійним шлюзом за замовчуванням для мереж доступу V_1 та V_6 (відповідно до коефіцієнтів готовності, наведених у табл. 2.16), а з іншого – вибором шляху в ТМ з максимальною пропускною здатністю. У разі відмови шлюзу за замовчуванням, тобто маршрутизатора R_2, потік пакетів автоматично переключиться на резервний маршрут: $R_1 \to R_4 \to R_5 \to R_8$.

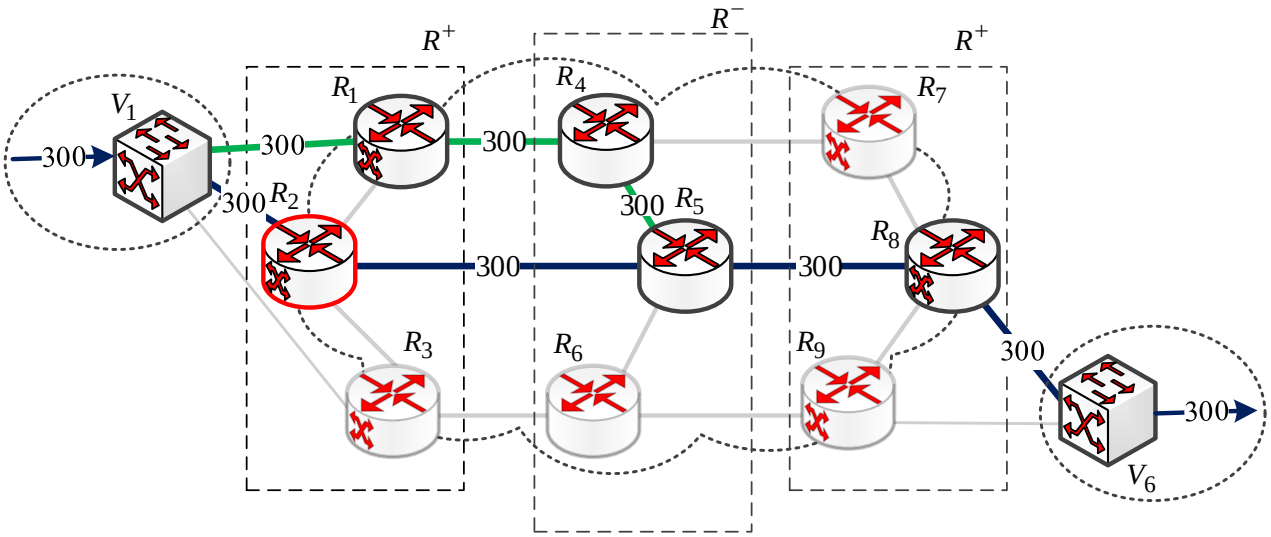


Рис. 2.47. Приклад розв'язання задачі
одношляхової відмовостійкої маршрутизації

У дослідженні багатошляхової відмовостійкої маршрутизації вихідні дані не змінювались, але інтенсивність потоку становила 1100 1/с. Результат розв'язання поставленої задачі показано на рис. 2.48. Тоді основний мультишлях (рис. 2.48, а) складається з таких маршрутів:

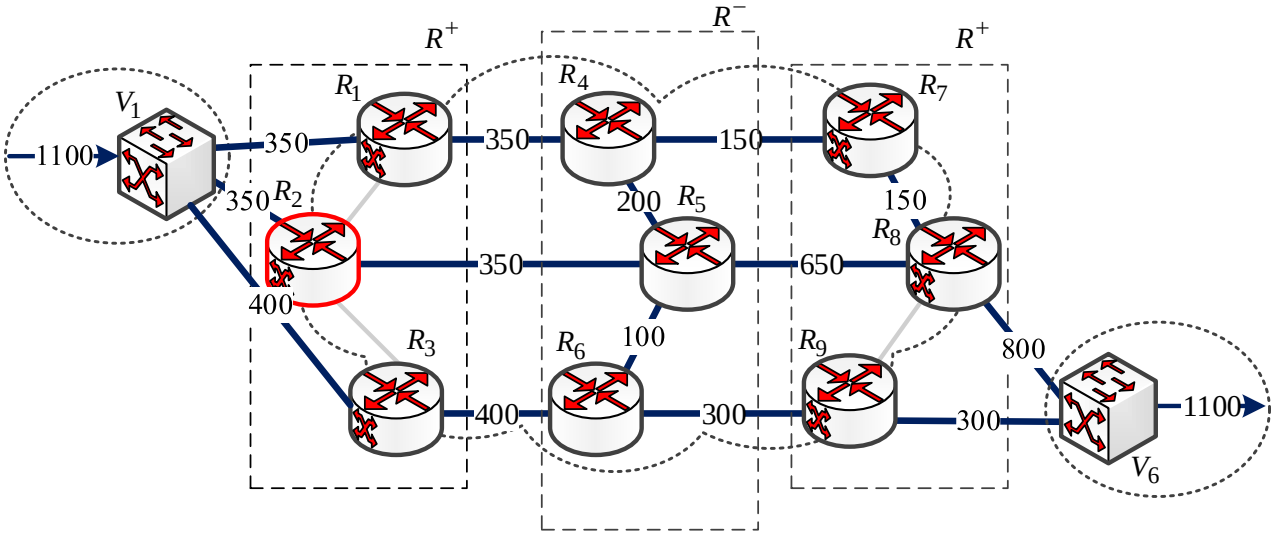
– $R_1 \to R_4 \to R_7 \to R_8$ за умови передачі потоку з інтенсивністю 150 1/с;

– $R_1 \to R_4 \to R_5 \to R_8$ у випадку передачі потоку з інтенсивністю 200 1/с;

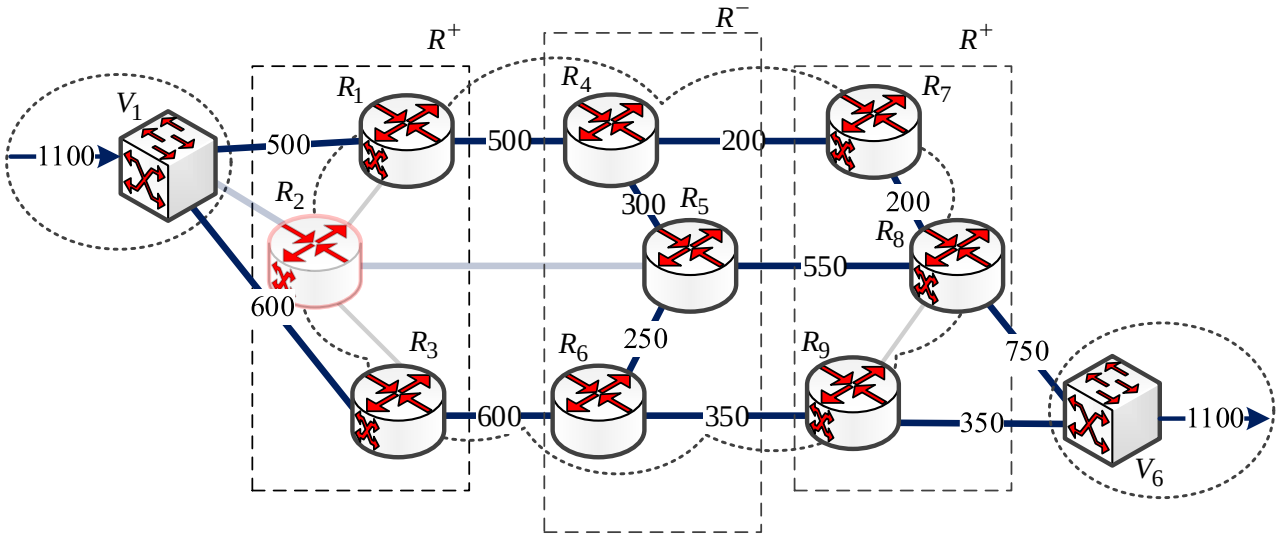
– $R_2 \to R_5 \to R_8$ у разі передачі потоку з інтенсивністю 350 1/с;

– $R_3 \to R_6 \to R_5 \to R_8$ за умови передачі потоку з інтенсивністю 100 1/с;

– $R_3 \to R_6 \to R_9$ у разі передачі потоку з інтенсивністю 300 1/с.



а) основний мультишлях



б) резервний мультишлях

Рис. 2.48. Приклад розв’язання задачі
багатошляхової відмовостійкої маршрутизації

Це рішення ґрунтується на можливості забезпечення балансування навантаження за всіма доступними інтерфейсами віртуальних маршрутизаторів: R_1, R_2 та R_3 для мережі доступу V_1, і R_8, R_9 – для V_6 відповідно. Це також супроводжується використанням багатошляхової маршрутизації безпосередньо в транспортній мережі. У цьому випадку в разі відмови шлюзу за

замовчуванням R_2 відповідно до розрахунків, отриманих у межах запропонованої моделі, потік буде автоматично перенаправлено на резервний мультишлях (рис. 2.48, б), за винятком маршруту з R_2:

- $R_1 \to R_4 \to R_7 \to R_8$ у випадку передачі потоку з інтенсивністю 200 1/с;
- $R_1 \to R_4 \to R_5 \to R_8$ у разі передачі потоку з інтенсивністю 300 1/с;
- $R_3 \to R_6 \to R_5 \to R_8$ за умови передачі потоку з інтенсивністю 250 1/с;
- $R_3 \to R_6 \to R_9$ у випадку передачі потоку з інтенсивністю 350 1/с.

Загалом результати дослідження підтвердили адекватність запропонованої моделі та ефективність отриманих на її основі маршрутних рішень з точки зору рівня відмовостійкості та продуктивності ІКМ.

Висновки до другого розділу

1. Подальший розвиток отримала система потокових моделей відмовостійкої маршрутизації без резервування елементів ІКМ шляхами, що не перетинаються або перетинаються лише за вузлами (2.1)–(2.8), з регулюванням числа використовуваних маршрутів (2.5), (2.6). Новизною рішень є введення в структуру моделей нелінійних умов застосування шляхів заданого типу (2.2), (2.3) та (2.7), (2.8) за умови балансування навантаження, які використовувалися як обмеження в розв'язанні оптимізаційної задачі (2.1) відмовостійкої маршрутизації. Представлене рішення, основане на використанні шляхів, які перетинаються за вузлами, є компромісом у разі забезпечення відмовостійкості та безпеки, з одного боку, та якості обслуговування, з іншого. Це є актуальним в умовах, коли місцем відмов та/або компрометації є саме канали зв'язку, а не вузли ІКМ. Як показали проведені дослідження, загалом запропоновані рішення дозволили забезпечити підвищення продуктивності мережі приблизно в 1,7 раза. У цьому випадку зі зростанням розміру мережі та зв'язності маршрутизаторів виграш за продуктивністю збільшувався до 2,5–4 разів.

2. Удосконалення отримала потокова модель швидкої перемаршрутизації (1.1), (1.2), (2.9)–(2.20), у межах якої технологічне завдання вдалося представити в формі оптимізаційної задачі. Під час проведеного вдосконалення вдалося сформулювати в лінійній формі умови захисту вузла та каналу (2.10)–(2.16) у разі реалізації як одношляхової, так і багатошляхової стратегій маршрутизації. Обґрунтовано до використання лінійно-квадратичний критерій оптимальності, оснований на мінімізації цільової функції (2.23). Установлено систему ієрархії співвідношень вагових коефіцієнтів у цільовій функції (2.23),

за якої забезпечувалися б максимальні значення продуктивності ІКМ і масштабованості рішень щодо швидкої перемаршрутизації, зокрема на основі оптимізації роботи схеми захисту схильних до відмов елементів мережі одною (спільною для множини потоків) резервною ділянкою – «facility backup».

Крім того, запропоновано білінійний критерій оптимальності (2.24), що містить умови захисту шляху за можливості реалізації як одношляхової, так і багатошляхової стратегій маршрутизації. Установлено систему ієрархії співвідношень вагових коефіцієнтів (метрик) цільовій функції (2.24), коли забезпечувалися коректні рішення щодо швидкої перемаршрутизації. Працездатність та адекватність запропонованої потокової моделі швидкої перемаршрутизації підтверджена на певних розрахункових прикладах у процесі вирішення завдань одношляхової та багатошляхової маршрутизації у разі реалізації різних схем захисту елементів мережі.

3. У розділі представлено дворівневий метод одношляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ, який забезпечує реалізацію схем захисту каналу, вузла, шляху та їх пропускної здатності. Показано, що ефективна реалізація принципів швидкої перемаршрутизації з балансуванням навантаження в ІКМ, наприклад із застосуванням програмно-конфігурованих архітектур, може бути основана на використанні математичної моделі (1.1), (2.9)–(2.23), яка передбачає централізацію рішення досить складних маршрутних завдань на відповідних SDN-контролерах. У цьому випадку чинниками складності є їх висока розмірність $\left(2\cdot|K|\cdot|E|\right)$ та нелінійність (2.17)–(2.19) у процесі реалізації схем захисту шляху та пропускної здатності ІКМ, що передбачає підвищені вимоги до продуктивності даних контролерів.

У межах запропонованого обчислювального методу відповідно до принципу прогнозування взаємодій пропонується поділ за двома ієрархічними рівнями функцій розрахунку основних (нижній рівень) і резервних (верхній рівень) маршрутів у разі особливого запису раніше відомих умов захисту пропускної здатності мережі (2.27). Це дозволило відмовитися від вихідної досить розмірної та нелінійної оптимізаційної задачі шляхом переходу до ітераційного розв’язання лінійних оптимізаційних задач удвічі меншого розміру. Реалізація на практиці подібного підходу дозволить істотно знизити вимоги до обчислювальної потужності сервера (контролера) маршрутів, на який покладено централізовані вирішення завдань маршрутизації в мережі. Проведений аналіз запропонованого дворівневого методу (рис. 2.32–2.36) підтвердив його працездатність та ефективність з точки зору отримання

оптимальних рішень щодо забезпечення збалансованої завантаженості каналів зв'язку (2.28), (2.29) та реалізації необхідних схем захисту елементів мережі у разі швидкої перемаршрутизації в ІКМ. Зокрема ефективність отриманих за допомогою запропонованого дворівневого методу рішень повністю відповідала результатам централізованих розрахунків.

4. Запропоновано математичну модель багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ, представлену виразами (1.2)–(1.4), (2.9), (2.11), (2.15), (2.17) і (2.31)–(2.34). Новизною запропонованої моделі є те, що узгоджене вирішення завдань з TE та FRR із захистом каналу, вузла та пропускної здатності забезпечується під час розв'язання задачі лінійної оптимізації. Критерієм оптимальності був мінімум верхнього порога завантаженості каналів зв'язку мережі (2.34) потоками, що протікають як за основними, так і за резервними маршрутами. Перехід від нелінійних умов захисту пропускної здатності (2.18) (2.20) до лінійного аналога (2.31) було досягнуто шляхом певного розширення числа змінних, що розраховуються, (2.32) і (2.33), які визначають верхній поріг для маршрутних змінних основного та резервного шляхів. Подібний підхід орієнтує на зниження обчислювальної складності в розрахунку маршрутних змінних, відповідальних за формування основного та резервного шляхів, і забезпечує збалансовану завантаженість каналів зв'язку мережі відповідно до вимог концепції Traffic Engineering.

Результати проведеного аналізу запропонованої моделі на низці числових прикладів підтвердили її адекватність і можливість отримання оптимальних розв'язань задачі швидкої перемаршрутизації з балансуванням навантаження в ІКМ у процесі реалізації різних схем захисту елементів мережі (каналу, вузла) та пропускної здатності. Показано, що виграш від реалізації багатошляхової стратегії маршрутизації у випадку TE FRR дозволив знизити верхній поріг завантаженості каналів зв'язку в середньому від 37,12 % до 59,41 % за умови захисту каналу та від 31,5 % до 56,3 % у разі захисту вузла, що позитивно позначається і на рівні якості обслуговування в мережі загалом.

5. У розділі представлено узгоджене рішення щодо захисту шлюзу за замовчуванням та швидкої перемаршрутизації в ІКМ на основі синтезу відповідної потокової математичної моделі (1.1), (1.2), (2.36)–(2.43). У межах запропонованої моделі задача відмовостійкої маршрутизації була зведена до розв'язання оптимізаційної задачі нелінійного програмування з цільовою функцією (2.43) та обмеженнями (2.36)–(2.42). Частина керуючих змінних (2.36), (2.37) відповідає за вибір шлюзу за замовчуванням у мережі доступу,

а частина (1.2), (2.10) – за вибір шляху або мультишляху в транспортній мережі. Сформульовано умови захисту шлюзу за замовчуванням як у разі балансування навантаження (2.41), так і без балансування (2.42). Задача відмовостійкої маршрутизації із захистом шлюзу за замовчуванням сформульована як оптимізаційна (2.43), де вибір маршрутних метрик забезпечувався таким чином, щоб вибір шлюзу за замовчуванням виконувався за критерієм максимального коефіцієнта готовності (табл. 2.16), а вибір маршруту в транспортній мережі – відповідно до критерію максимальної пропускної здатності (за аналогією з протоколом IGRP). Наведені розрахункові приклади продемонстрували особливості застосування запропонованої моделі для вирішення завдання захисту шлюзу за замовчуванням за умови відмовостійкості маршрутизації в ІКМ для випадку реалізації одношляхової (рис. 2.47) та багатошляхової маршрутизації (рис. 2.48). Результати підтвердили ефективність запропонованої моделі та адекватність отриманих розрахункових результатів.

Як правило, збільшення кількості маршрутизаторів і каналів зв'язку в мережі призводить до підвищення обчислювальної складності отримуваних рішень. Водночас ефективність використання запропонованої моделі також багато в чому визначається розміром транспортної мережі та кількістю мереж доступу. Чим більше існує варіантів вибору шлюзу за замовчуванням і можливих шляхів у транспортній мережі, тим ефективнішою є саме оптимізаційне формулювання задачі для узгодженого вирішення цих завдань. У цих визначених умовах скоординовані рішення забезпечують більш високу ефективність відмовостійкої маршрутизації в мережі порівняно з наявними, в яких завдання вибору шлюзу та маршрутизації вирішуються окремо.

Перелік джерел посилання до другого розділу

1. Макаренко С.И. Время сходимости протоколов маршрутизации при отказах в сети. Системы управления, связи и безопасности. 2015. № 2. С. 45–98. URL: http://journals.intelgr.com/sccs/archive/2015-02/03-Makarenko.pdf.

2. Matsubara D., Egawa T., Nishinaga N., Kafle V.P., Shin M.K., Galis A. Toward future networks: A viewpoint from ITU-T. IEEE Communications Magazine. 2013. Vol. 51, No. 3. P. 112–118.

3. 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.

4. 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.

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

6. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop. Halmstad, Sweden, 13–15 September, 2016. IEEE, 2016. P. 1–10. DOI: 10.1109/RNDM.2016.7608262.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. Chaparadza R., Wodczak M., Meriem T.B., De Lutiis P., Tcholtchev N., Ciavaglia L. Standardization of resilience & survivability, and autonomic fault-

management, in evolving and future networks: an ongoing initiative recently launched in ETSI. Design of Reliable Communication Networks (DRCN) 2013: Proceedings of the 9th International Conference. Budapest, Hungary, 4–7 March, 2013. IEEE, 2013. P. 331–341.

14. ETSI TS 103 195-2 V1.1.1. Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. May 2018. 149 p. URL: https://www.etsi.org/deliver/etsi_ts/ 103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf.

15. ETSI TS 103 194 V1.1.1. Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet. October 2014. 67 p. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ ts_103194v010101p.pdf.

16. ITU-T Rec. Y. 2614. Network reliability in public telecommunication data networks. August 2008. 20 p. URL: https://www.itu.int/rec/T-REC-Y.2614-201108-I/en.

17. Hariyawan M.Y. Comparison Analysis of Recovery Mechanism at MPLS Network. International Journal of Electrical and Computer Engineering (IJECE). 2011. Vol. 1, No. 2. P. 151–160. DOI: http://dx.doi.org/10.11591/ijece.v1i2.84.

18. Papán J., Segeč P., Palúch P. Analysis of existing IP Fast Reroute mechanisms. Information and Digital Technologies (IDT): Proceedings of the 2015 International Conference, Zilina, Slovakia, 7–9 July 2015. IEEE, 2015. P. 291–297. DOI: 10.1109/DT.2015.7222986.

19. Hussain I. Fault-Tolerant IP and MPLS Networks (Networking Technology). Indianapolis: Cisco Press, 2005. 336 p.

20. Koren I., Krishna C. Fault-Tolerant Systems. Morgan Kaufmann, 2007. 400 p.

21. RFC 7490. Remote Loop-Free Alternate (LFA) Fast Reroute (FRR). April 2015. 29 p. URL: https://tools.ietf.org/pdf/rfc7490.pdf.

22. RFC 7811. An Algorithm for Computing IP/LDP Fast Reroute Using Maximally Redundant Trees (MRT-FRR). June 2016. 118 p. URL: https://tools.ietf.org/pdf/rfc7811.pdf.

23. RFC 7812. An Architecture for IP/LDP Fast Reroute Using Maximally Redundant Trees (MRT-FRR). June 2016. 44 p. URL: https://tools.ietf.org/pdf/rfc7812.pdf.

24. Pavlik J., Komarek A., Sobeslav V., Horalek J. Gateway redundancy protocols. Computational Intelligence and Informatics (CINTI) 2014: Proceedings of

the IEEE 15th International Symposium. Budapest, Hungary, 19–21 November, 2014. IEEE, 2014. P. 459–464. DOI: 10.1109/CINTI.2014.7028719.

25. RFC 5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. March 2010. 40 p. URL: https://tools.ietf.org/pdf/rfc5798.pdf.

26. RFC 2281. Cisco Hot Standby Router Protocol (HSRP). March 1998. 17 p. https://tools.ietf.org/pdf/rfc2281.pdf.

27. First Hop Redundancy Protocol comparison (HSRP, VRRP, GLBP) with the diagram (2013). Cisco Networking Center. URL: http:// cisconetworkingcenter. blogspot.com/2013/01/first-hop-redundancy-protocol.html.

28. RFC 5714. IP Fast Reroute Framework. January 2010. 15 p. URL: https://tools.ietf.org/pdf/rfc5714.pdf.

29. RFC 4915. Multi-Topology (MT) Routing in OSPF. June 2007. 20 p. URL: https://tools.ietf.org/pdf/rfc4915.pdf.

30. RFC 1853. IP in IP Tunneling. October 1995. 8 p. URL: https://tools.ietf.org/ pdf/rfc1853.pdf.

31. RFC 6445. Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute. November 2011. 53 p. URL: https://tools.ietf.org/pdf/rfc6445.pdf.

32. RFC 4090. Fast Reroute Extensions to RSVP-TE for LSP Tunnels. May 2005. 38 p. URL: https://tools.ietf.org/pdf/rfc4090.pdf.

33. Tiso J., Teare D. Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide. Cisco press. 2011. 733 p.

34. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.

35. Janevski T. NGN Architectures, Protocols and Services. 1st Edition. Wiley, 2014. 366 p.

36. Chiu C.W., Huang K.S., Yang C.B., Tseng, C.T. An adaptive heuristic algorithm with the probabilistic safety vector for fault-tolerant routing on the (n, k)-star graph. International Journal of Foundations of Computer Science. 2014. Vol. 25, No. 06. P. 723–743.

37. Soleimany A., Azmoodeh S. More Improvement by Helping Ant to Fault-Tolerant Heuristic Routing Algorithm in Mesh Networks. Research Journal of Applied Sciences, Engineering and Technology. 2013. Vol. 6, No. 4. P. 622–630. DOI: 10.19026/rjaset.6.4172.

38. Arai J., Li Y. Fault-Tolerant Routing Algorithms for Hierarchical Dual-Nets with Limited and Arbitrary Number of Faulty Nodes. International Journal of Networking and Computing. 2015. Vol. 5, No. 2. P. 329–346.

39. Elhourani T., Gopalan A., Ramasubramanian S. IP fast rerouting for multi-link failures. IEEE/ACM Transactions on Networking. 2016. Vol. 24, No. 5. P. 3014–3025. DOI: 10.1109/TNET.2016.2516442.

40. Gopalan A., Ramasubramanian S. IP fast rerouting and disjoint multipath routing with three edge-independent spanning trees. IEEE/ACM Transactions on Networking. 2016. Vol. 24, No. 3. P. 1336–1349. DOI: 10.1109/TNET.2015.2440179.

41. Martins L., Gomes T., Tipper D. An efficient heuristic for calculating a protected path with specified nodes. Resilient Networks Design and Modeling (RNDM): Proceedings of the 8th International Workshop, Halmstad, Sweden, 13–15 September, 2016. IEEE, 2016. P. 150–157. DOI: 10.1109/RNDM.2016.7608281.

42. Antonakopoulos S., Bejerano Y., Koppol P. Full protection made easy: The DisPath IP fast reroute scheme. IEEE/ACM Transactions on Networking. 2015. Vol. 23, No. 4. P. 1229–1242. DOI: 10.1109/TNET.2014.2369855.

43. Kuang K., Wang S., Wang X. Discussion on the combination of loop-free alternates and maximally redundant trees for IP networks fast reroute. Communications (ICC): Proceedings of the International Conference, Sydney, NSW, Australia, 10–14 June, 2014. IEEE, 2014. P. 1131–1136. DOI: 10.1109/ICC.2014.6883473.

44. Menth M., Braun W. Performance comparison of not-via addresses and maximally redundant trees (MRTs). Integrated Network Management (IM 2013): Proceedings of the IFIP/IEEE International Symposium, Ghent, Belgium, 27–31 May, 2013. IEEE, 2013. P. 218–225.

45. Braun W., Menth M. Loop-free alternates with loop detection for fast reroute in software-defined carrier and data center networks. Journal of Network and Systems Management. 2016. Vol. 24, No. 3. P. 470–490. DOI: 10.1007/s10922-016-9369-9.

46. Braun W., Albert M., Eckert T., Menth M. Performance comparison of resilience mechanisms for stateless multicast using bier. Integrated Network and Service Management (IM): Proceedings of the IFIP/IEEE Symposium, Lisbon, Portugal, 8-12 ay, 2017. IEEE, 2017. P. 230–238. DOI: 10.23919/INM.2017.7987284.

47. Duong T.D., Kaneko K. Fault-Tolerant Routing Based on Approximate Directed Routable Probabilities for Hypercubes. In: Xiang Y., Cuzzocrea A.,

Hobbs M., Zhou W. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2011. Lecture Notes in Computer Science, Vol. 7016. Springer, Berlin, Heidelberg. P 106–116. DOI: https://doi.org/10.1007/978-3-642-24650-0_10.

48. Lu C., Hu D. A Fault-Tolerant Routing Algorithm for Wireless Sensor Networks Based on the Structured Directional de Bruijn Graph. Cybernetics and Information Technologies. 2016. Vol. 16, No. 2. P. 46–59. DOI: 10.1515/cait-2016-0019.

49. Yeh S.I., Yang C.B., Chen H.C. Fault-tolerant routing on the star graph with safety vectors. Parallel Architectures, Algorithms and Networks 2002 (I-SPAN'02): Proceedings of the International Symposium. Makati City, Metro Manila, Philippines, 22–24 May, 2002. IEEE, 2002. P. 301–306. DOI: 10.1109/ISPAN.2002.1004298.

50. Nishiyama Y., Hirai Y., Kaneko K. Fault-Tolerant Routing Based on Improved Safety Levels in Pancake Graphs. Parallel and Distributed Computing, Applications and Technologies (PDCAT) 2014: Proceedings of the 15th International Conference. Hong Kong, China, 9–11 December, 2014. IEEE, 2014. P. 76–81. DOI: 10.1109/PDCAT.2014.20.

51. Nishiyama Y., Sasaki Y., Hirai Y., Nakajo H., Kaneko K. Fault-tolerant Routing based on Routing Capabilities in a Hyper-Star Graph. Journal of Information Science and Engineering. 2017. P. 1–13.

52. Wang D., McNair J. Circulant-graph-based fault-tolerant routing for all-optical WDM LANs. GLOBECOM 2010: Proceedings of the Global Telecommunications Conference. Miami, FL, USA, 6–10 December, 2010. IEEE, 2010. P. 1–5. DOI: 10.1109/GLOCOM.2010.5683293.

53. Pióro M., Tomaszewski A., Żukowski C., Hock D., Hartmann M., Menth M. Optimized IP-based vs. explicit paths for one-to-one backup in MPLS fast reroute. NETWORKS 2010: Proceedings of the 14th International Telecommunications Network Strategy and Planning Symposium. Warsaw, Poland. 27–30 September, 2010. IEEE, 2010. P. 1–6. DOI: 10.1109/NETWKS.2010.5624923.

54. Addis B., Carello G., Mattia S. Survivable green traffic engineering with shared protection. Networks. 2017. Vol. 69, No. 1. P. 6–22. DOI: https://doi.org/10.1002/net.21717.

55. 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.

56. Liu V.Y., Tipper D. Spare capacity allocation using shared backup path protection for dual link failures. Computer Communications. 2013. Vol. 36, No. 6. P. 666–677. DOI: 10.1016/j.comcom.2012.09.007.

57. 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.

58. Gomes T., Tipper D., Alashaikh A. A novel approach for ensuring high end-to-end availability: The spine concept. Design of Reliable Communication Networks (DRCN) 2014: Proceedings of the 10th International Conference. Ghent, Belgium, 1–3 April, 2014. IEEE, 2014. P. 1–8. DOI: 10.1109/DRCN.2014.6816142.

59. Alashaikh A., Tipper D., Gomes T. March, 2016. Supporting differentiated resilience classes in multilayer networks. Design of Reliable Communication Networks (DRCN) 2016: Proceedings of the 12th International Conference. Paris, France. 15–17 March, 2017. IEEE, 2016. P. 31–38. DOI: 10.1109/DRCN.2016.7470832.

60. Zhang X., Cheng Z., Lin R., He L., Yu S., Luo H. Local Fast Reroute With Flow Aggregation in Software Defined Networks. IEEE Communications Letters. 2017. Vol. 21, No. 4. P. 785–788. DOI: 10.1109/LCOMM.2016.2638430.

61. Malik A., Aziz B., Adda M., Ke C.H. Optimisation methods for fast restoration of software-defined networks. IEEE Access. 2017. Vol. 5. P. 16111–16123. DOI: 10.1109/ACCESS.2017.2736949.

62. Rzym G., Wajda K., Chołda P. SDN-based WAN optimization: PCE implementation in multi-domain MPLS networks supported by BGP-LS. Image Processing & Communications. 2017. Vol. 22, No. 1. P. 35–48. DOI: https://doi.org/10.1515/ipc-2017-0004.

63. Wang N., Ho K., Pavlou G., Howarth M. An overview of routing optimization for internet traffic engineering. IEEE Communications Surveys & Tutorials. 2008. Vol. 10, No. 1. P. 36–56. DOI: 10.1109/COMST.2008.4483669.

64. 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.

65. 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.

66. 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.

67. 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.

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

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

70. Еременко А.С. Потоковая модель многопутевой маршрутизации по непересекающимся путям в телекоммуникационной сети. Проблеми телекомунікацій. 2015. № 1 (16). С. 85–93. URL: http://pt.journal.kh.ua/2015/1/1/151_yeremenko_disjoint.pdf.

71. Yeremenko O.S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the IEEE Second International Scientific-Practical Conference, Kharkiv, Ukraine, 13−15 October, 2015. Kharkiv: Kharkiv National University of Radio Electronics, 2015. P. 42–45.

72. Єременко О.С., Андрушко Д.В. Модель маршрутизації в телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами. Вісник Національного університету «Львівська політехніка». Серія: «Радіоелектроніка та телекомунікації». 2015. № 818. С. 181–188.

73. Lemeshko O.V., Arous K.M., Yeremenko O.S. Fault-Tolerant Unicast, Multicast and Broadcast Routing Flow-based Models. Scholars Journal of Engineering and Technology (SJET). 2015. Vol. 3, Issue 4A. P. 343–350.

74. Лемешко А.В., Еременко А.С., Тарики Н., Арус К.М. Повышение масштабируемости и производительности решений по отказоустойчивой маршрутизации в телекоммуникационных сетях. Системи обробки інформації. 2016. № 1(138). С. 152–156.

75. Lemeshko A.V., Yeremenko O.S., Tariki N. Improvement of flow-oriented fast reroute model based on scalable protection solutions for telecommunication network elements. Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 6. P. 477–490. DOI: 10.1615/TelecomRadEng.v76.i6.30.

76. Yeremenko O.S., Lemeshko O.V., Tariki N. Fast ReRoute Scalable Solution with Protection Schemes of Network Elements. Electrical and Computer Engineering (UKRCON): Proceedings of the First Ukraine Conference, Kiev, Ukraine, 29 May – 2 June 2017. IEEE, 2017. P. 783–788. DOI: 10.1109/UKRCON.2017.8100353.

77. Еременко А.С., Тарики Н., Евдокименко М.А. Оптимизационная модель отказоустойчивой маршрутизации с билинейными условиями защиты пути. Радиоэлектроника и информатика. 2017. № 2 (77). С. 9–14.

78. Yeremenko O., Lemeshko O., Tariki N., Hailan A.M. Research of Optimization model of Fault-Tolerant Routing with Bilinear Path Protection Criterion. Advanced Information and Communication Technologies (AICT): Proceedings of the 2nd International Conference, Lviv, Ukraine, 4–7 July, 2017. IEEE, 2017. P. 219–222. DOI: 10.1109/AIACT.2017.8020105.

79. Seok Yo., Lee Yo., Choi Ya., Kim C. A constrained multipath traffic engineering scheme for MPLS networks. International Conference on Communications ICC 2002 (Cat. No.02CH37333): Proceedings of the IEEE International Conference. New York, NY, USA, 28 April – 2 May, 2002. IEEE, 2002. P. 2431–2436. DOI: 10.1109/ICC.2002.997280.

80. Wang Y., Wang Z. Explicit routing algorithms for Internet Traffic Engineering Computer Communications and Networks: Proceedings of the Eight International Conference. Boston, USA, 11–13 October, 1999. IEEE, 1999. P. 582–588.

81. Lemeshko O., Yeremenko O. Enhanced method of fast re-routing with load balancing in software-defined networks. Journal of ELECTRICAL ENGINEERING. 2017. Vol. 68, Issue 6. P. 444–454. DOI: 10.1515/jee-2017-0079.

82. Lemeshko O., Yeremenko O., Hailan A.M. Two-level Method of Fast ReRouting in Software-Defined Networks. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fourth International Scientific-Practical Conference, Kharkov, Ukraine, 10–13 October, 2017. IEEE, 2017 P. 376–379. DOI: 10.1109/INFOCOMMST.2017.8246420.

83. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. Москва: Мир, 1973. 344 с.

84. Сингх М., Титли А. Системы: декомпозиция, оптимизация и управление. Москва: Машиностроение, 1986. 494 с.

85. Лемешко О.В., Єременко О.С. Розробка та дослідження лінійної оптимізаційної моделі швидкої перемаршрутизації з балансуванням навантаження в телекомунікаційних мережах. Радиоэлектроника и информатика. 2017. № 4 (79). С. 18–25.

86. Lemeshko O., Yeremenko O. Linear Optimization Model of MPLS Traffic Engineering Fast ReRoute for Link, Node, and Bandwidth Protection. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET): Proceedings of the 14th International Conference, Lviv–Slavske, Ukaine, 20–24 February, 2018. IEEE, 2018. P. 1–5. DOI: 10.1109/TCSET.2018.8336365.

87. Yeremenko O., Tariki N., Hailan A.M. Fault-tolerant IP routing flow-based model. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): Proceedings of the 13th International Conference, viv, Ukraine, 23–26 February, 2016. IEEE, 2016. P. 655–657. DOI: 10.1109/TCSET.2016.7452143.

88. Lemeshko O.V., Yeremenko O.S., Tariki N., Hailan A.M. Fault-Tolerance Improvement for Core and Edge of IP Network. Computer Sciences and Information Technologies (CSIT): Proceedings of the XIth International Scientific and Technical Conference, Lviv, Ukraine, 6–10 Sept. 2016. IEEE, 2016. P. 161–164. DOI: 10.1109/STC-CSIT.2016.7589895.

89. Lemeshko O., Yeremenko O., Tariki N. Solution for the Default Gateway Protection within Fault-Tolerant Routing in an IP Network. International Journal of Electrical and Computer Engineering Systems. 2017. Vol. 8, No. 1. P. 19–26.

90. Yeremenko O., Tariki N., Vavenko T. Default Gateway Protection Scheme in Fault-Tolerant IP Routing. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Third International Scientific-Practical Conference, Kharkiv, Ukraine, 4–6 Oct. 2016. IEEE, 2016. P. 223–226. DOI: 10.1109/INFOCOMMST.2016.7905389.