МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор Гнатюк
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Оптимізація телекомунікаційних мереж в умовах надзвичайних ситуацій»

Виконавець: _____ Артем ІВАЩЕНКО
(підпис)

Керівник: _____ Юлія ПЕТРОВА
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Іващенка Артема Володимировича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Оптимізація телекомунікаційних мереж в умовах надзвичайних ситуацій»

затверджена наказом ректора від «28» вересня 2023 р. №1965/ст

2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.

3. Вихідні дані до роботи:. ROUTERS, SWITCHES, FIREWALLS, LOAD BALANCERS, OSPF, BGP, QoS, NETWORK TOPOLOGY, ENCRYPTION, INTRUSION DETECTION SYSTEMS (IDS), DDOS MITIGATION, ACCESS CONTROL, ANOMALY DETECTION, PERFORMANCE METRICS, VULNERABILITY ASSESSMENT, SECURITY INCIDENT RESPONSE, USER AUTHENTICATION, IDENTITY MANAGEMENT, CYBERSECURITY POLICIES,

4. Зміст пояснювальної записки: Розділ 1. тимізація багатоадресної передачі через алгоритм Єдиної Точки Зустрічі (SRP) .Розділ 2. Системні Аспекти Телекомунікаційних Мереж у Контексті Надзвичайних Ситуацій. Розділ 3. Спільна оптимізація з відновленням після збою. Розділ 4. Моделювання та аналіз. Висновки

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: схеми мережевої топології, технічні схеми заходів безпеки, схеми архітектури безпеки, графіки результатів аудиту та виявлення вразливостей, а також діаграми відновлення мережі

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	02.10.2023-04.10.2023	Виконано
2	Вступ	05.10.2023-08.10.2023	Виконано
3	Оптимізація багатоадресної передачі через алгоритм Єдиної Точки Зустрічі (SRP)	09.10.2023-22.10.2023	Виконано
4	Системні Аспекти Телекомунікаційних Мереж у Контексті Надзвичайних Ситуацій	23.10.2023-05.11.2023	Виконано
5	Спільна оптимізація з відновленням після збою	06.11.2023-30.11.2023	Виконано
6	Моделювання та аналіз	06.11.2023-30.11.2023	Виконано
7	Охорона праці	01.12.2023-06.12.2023	Виконано
8	Охорона навколишнього середовища	07.12.2023-17.12.2023	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	18.12.2023-31.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професор Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “29" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Юлія ПЕТРОВА
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Артем ІВАЩЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Оптимізація телекомунікаційних мереж в умовах надзвичайних ситуацій» містить 90 сторінок, 24 рисунків, 6 таблиці, 18 використаних джерел.

Багатоадресна маршрутизація, точки зустрічі прикордонного маршрутизатора, багатомережеві топології, пропускна здатність, дерево Штейнера, алгоритм зворотного прямого шляху, відновлення мережі, мультимедійний контент, цифрова платформа, технологічні вдосконалення, високоякісний звук і зображення, UDP, багатоадресний потік, роутер, оптимізація шляху, аномалії маршрутизації, таблиця одноадресної маршрутизації, алгоритм швидкого відновлення, втрати пакетів, технічні проблеми, збереження пропускної здатності, надійність, технічна оптимізація, взаємодія пристроїв, використання ресурсів, апробація результатів

Об’єкт дослідження – системи розподілу мультимедійного вмісту компаній, які працюють у цифрових платформах, зокрема в умовах надзвичайних ситуацій

Предмет дослідження – оптимізація телекомунікаційних мереж для забезпечення ефективного розподілу мультимедійного вмісту в умовах надзвичайних обставин

Метод дослідження – Аналіз топології мереж, виявлення несправностей, аналіз даних за допомогою методу PCA та використання вейвлетів. Методи апробації результатів включають моделювання та симуляції в реальних умовах

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

ACL - Access Control List

BGP - Border Gateway Protocol

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IoT - Internet of Things

ISP - Internet Service Provider

LAN - Local Area Network

MAC - Media Access Control

MPLS - Multiprotocol Label Switching

NAT - Network Address Translation

OSPF - Open Shortest Path First

QoS - Quality of Service

RFID - Radio-Frequency Identification

SDN - Software-Defined Networking

SNMP - Simple Network Management Protocol

SSID - Service Set Identifier

SSL - Secure Sockets Layer

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VLAN - Virtual Local Area Network

VoIP - Voice over Internet Protocol

VPN - Virtual Private Network

WAN - Wide Area Network

ВСТУП

Актуальність теми. У сучасному світі, де роль цифрових платформ у розповсюдженні мультимедійного вмісту стає визначальною, питання оптимізації телекомунікаційних мереж в умовах надзвичайних ситуацій є надзвичайно актуальним. Споживачі вимагають не лише вищої якості та доступності контенту, але і стабільності в умовах екстремальних обставин, таких як природні катастрофи чи технічні збої. Враховуючи різноманіття та масштабність сучасних мультимедійних платформ, важливо зрозуміти, як оптимізувати та забезпечувати найефективніший розподіл вмісту в умовах, коли традиційні методи можуть бути обмеженими чи непридатними.

Зростання популярності цифрових платформ у сфері розповсюдження мультимедійного контенту ставить перед компаніями завдання не лише підвищення конкурентоспроможності, але й забезпечення найвищого рівня обслуговування в умовах непередбачуваних обставин. Таке дослідження стає ключовим для розвитку та вдосконалення технологічних рішень у галузі мультимедійного розподілу та покликане визначити ефективні стратегії оптимізації мереж, що гарантують якість та доступність контенту в умовах надзвичайних ситуацій.

Зв’язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження. Мета дослідження полягає в аналізі та оптимізації систем розподілу мультимедійного вмісту в умовах надзвичайних ситуацій. Завдання включають вивчення топології мереж розподілу, розробку методів виявлення та усунення несправностей, а також апробацію отриманих результатів на практиці.

Для досягнення поставленої мети вирішуються такі наукові завдання.

Об’єктом дослідження – Об’єктом дослідження є системи розподілу мультимедійного вмісту компаній, які працюють у цифрових платформах, зокрема в умовах надзвичайних ситуацій.

Предметом дослідження – Предметом дослідження є оптимізація телекомунікаційних мереж для забезпечення ефективного розподілу мультимедійного вмісту в умовах надзвичайних обставин.

Методи досліджень. Аналіз топології мереж, виявлення несправностей, аналіз даних за допомогою методу PCA та використання вейвлетів. Методи апробації результатів включають моделювання та симуляції в реальних умовах.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

Отримані результати будуть протестовані та апробовані на практиці, зокрема в реальних умовах роботи систем розподілу мультимедійного вмісту в умовах надзвичайних ситуацій. Апробація результатів дозволить підтвердити ефективність запропонованих методів та їхню застосовність у практичних сценаріях.

РОЗДІЛ 1 ОПТИМІЗАЦІЯ БАГАТОАДРЕСНОЇ ПЕРЕДАЧІ ЧЕРЕЗ АЛГОРИТМ ЄДИНОЇ ТОЧКИ ЗУСТРІЧІ (SRP)

1.1. Алгоритм SRP для ефективного розподілу та зменшення перевантажень каналів

Багато сучасних компаній, що розповсюджують мультимедійний контент, змінюють свою систему розповсюдження на цифрову платформу. Ця цифрова платформа пропонує багато переваг для кінцевого користувача. Ці переваги включають більший і контрольований користувачем вибір вмісту, цифровий звук і збагачений вміст, більше параметрів конфігурації та відтворення для пристроїв різних форм-факторів та інші різноманітні вдосконалення. Для провайдера він може використовувати мережеву інженерію для зниження операційних витрат і забезпечення кращої конкуренції. Ще одна перевага для провайдера полягає в тому, що контент можна поширювати та перепаковувати у великій мережі.

Традиційні методи цифрового розповсюдження через цифрові мережі погано масштабуються у великих програмах. Розповсюдження за допомогою одноадресного протоколу протоколу дейтаграм користувача (UDP) ефективне лише в невеликих програмах. Це пов’язано з великими вимогами до пропускної здатності для надсилання дублікатів пакетів даних до однієї гілки кінцевих користувачів. Для великомасштабних додатків кращим протоколом для розповсюдження кінцевим користувачам є використання багатоадресної маршрутизації. У багатоадресній маршрутизації дерево розповсюдження багатоадресної адреси прокладається від джерела до всіх підключених приймачів. Використання багатоадресної передачі усуває вимогу надсилання окремих пакетів кожному кінцевому користувачеві, якому потрібен однаковий вміст. Замість цього один пакет надсилається через мережу. Коли маршрутизатор, розташований поблизу точки розгалуження дерева розповсюдження багатоадресної адреси, отримує цей пакет, він дублює пакет і розповсюджує його всім кінцевим отримувачам.

Загальна передумова багатоадресної передачі проста, і як розподіл означає, що вона забезпечує чудову масштабованість. Ці багатоадресні потоки міститимуть лише один тип пакетів, який можна визначити груповою адресою. Визначаючи різні групові адреси, можна визначити кілька потоків. Це дозволить одночасно поширювати кілька потоків вмісту. Одним із таких прикладів може бути наявність кількох відеопотоків різних каналів. Перевага керування відеовмістом у такий спосіб полягає в тому, що вміст можна поширювати між кількома постачальниками, які можуть бути організовані в ієрархії мереж постачальників

Програма потокового передавання наразі формується в індустрії цифрового телебачення та мовлення та набуває популярності. У міру того, як технологія стає все більш прийнятною, зростає потреба та інтерес до фактора надійності. Клієнти та постачальники контенту вимагають майже досконалості в усіх аспектах. Реклама під час спеціальних подій є критичною, тому перебої в роботі неприйнятні. Ці вимоги перетворюють багатоадресний розподіл і маршрутизацію на більш надійні, які в гіршому випадку повинні мати можливість майже миттєво відновлюватися без втрат пакетів або з дуже малими втратами пакетів, таким чином уникаючи тремтіння у сприйнятті людини.

Групова розсилка може мати безліч різних сценаріїв, які можуть сприяти втраті пакетів. Для кінцевого користувача вони відчують артефакти відео або втрату сигналу. Робота, яка обговорюється в цій дисертації, спрямована на зменшення перебоїв у обслуговуванні, одночасно оптимізуючи пропускну здатність між і всередині домену. Хоча це лише одне застосування багатоадресної передачі, воно є домінуючим. Розмір пакета та стиснення відео в поєднанні з багатоадресним розподілом також відіграють ключову роль у сценарії збою. Хоча розмір пакету безпосередньо не аналізується в цій тезі, існує кореляція багатоадресного трафіку та його впливу на сценарій збою. Зі збільшенням стиснення будь-які незначні втрати в потоці збільшуються. Всі ці фактори сприяють зриву

Ця теза визначає алгоритм для мінімізації навантаження на систему в межах топології мережі. Алгоритм, визначений як єдина точка зустрічі (SRP), оптимізує канали в межах топології та зменшить перевантаження каналів. SRP створює

статичне оптимізоване дерево нижче точки зустрічі (RP). RP діє як центральна точка в розподілі багатоадресного потоку до приймачів у топології. Якщо виникає збій зв’язку вгорі від RP, збереження смуги пропускання буде підтримуватися. Це пояснюється тим, що RP діє як кореневий маршрутизатор під час розповсюдження багатоадресного потоку.

1.2. Проблеми відновлення в багатоадресній маршрутизації

При використанні мультимедійних додатків багатоадресна маршрутизація може бути ефективно використана для розподілу вмісту в мережі. Однією з основних проблем багатоадресної маршрутизації є процес відновлення, який може бути повільним залежно від його взаємодії з функціями в межах мережевого рівня та рівнів нижче. Два популярних рішення для багатоадресної передачі: PIM-SM і PIM-SSM; вони покладаються на таблицю одноадресної маршрутизації. Коли в мережі виникає збій, наприклад розрив з’єднання або вихід маршрутизатора в автономний режим, одноадресна маршрутизація піддається повторній конвергенції. Цей процес, у свою чергу, запускає подію повторної конвергенції в багатоадресній маршрутизації.

Тригер повторної конвергенції в багатоадресній маршрутизації змушує багатоадресну розсилку запускати алгоритм зворотного прямого шляху (RFP), який визначає шлях назад до джерела. Проблема, пов’язана з цією процедурою, полягає в тому, що перевірка RFP базується на введенні отриманого багатоадресного пакета. Якщо цей інтерфейс не працює, за умови, що таблицю одноадресної маршрутизації не було оновлено, це може спричинити затримку повторного зближення. Ця затримка ускладнюється через зв’язок між одноадресною та багатоадресною маршрутизацією. Протокол багатоадресної маршрутизації може мати можливість повторно конвергувати лише після відновлення таблиці одноадресної маршрутизації.

1.3. Вплив повторної конвергенції на користувача

Коли відбувається повторна конвергенція багатоадресної передачі, користувач відчуває артефакти або втрачає сигнал. Навіть невеликі збої, які можуть виникати протягом кількох сотень мілісекунд, можуть виглядати як втрачений сигнал. Результати лабораторних досліджень показали, що відключення тривалістю від 20 до 30 мілісекунд виглядають як артефакти. У таблиці 1.1 можна побачити розбивку за часом різних відключень та їх результатів [1].

Таблиця 1.1.

Наслідки тимчасових перебоїв

Легкий візуальний вплив [с]	Помітний візуальний вплив [с]	«Канал недоступний» повідомлення [с]
0.03 - 1	1 – 3	3.5 +

Оцінити вплив досить складно, тому що це залежить від місця відключення. Якщо збій станеться ближче до постачальника контенту, результати будуть катастрофічними. Можливою кількістю користувачів, які постраждали від такого збою, можуть бути всі користувачі, на яких наразі підписані. Навпаки, якщо зв’язок буде розірвано ближче до кінцевого користувача, це вплине лише на невелику кількість користувачів

Існують механізми відновлення. Але ці механізми недостатні для безперебійної передачі. Інша проблема, яка виникає, полягає в тому, що адміністратори мережі передбачили певні заходи QoS для контролю потоку трафіку. Ці заходи забезпечують корисні властивості для спрямування трафіку, але можуть спричинити додаткову затримку часу відновлення залежно від налаштувань [2]

1.4 Оптимізація пропускної здатності в багатодомних топологіях

У другому розділі детально описано важливу базову інформацію. Ця довідкова інформація дасть розуміння оптимізації пропускної здатності та того, як вона пов’язана з мережевими аномаліями в багатодомній топології. Коли оптимізація реалізована, вона може надати засоби контролю збоїв з’єднання та обмежень пропускної здатності. Оптимізуючи шлях для пропускної здатності багатоадресного потоку, можна досягти покращеної розмови. Моделювання топології у вигляді дерева Штейнера дозволяє скоротити зв’язки між джерелом і приймачами. Це порівняно з використанням дерева найкоротших шляхів, яке не оптимізує використання посилань. Дерево Штайнера можна накласти на існуючу таблицю одноадресної маршрутизації

У третьому розділі розглядаються дві різні моделі: нещодавно запропонована єдина точка зустрічі (SRP) і точки зустрічі прикордонного маршрутизатора (BRP). SRP — це алгоритм оптимізації, який використовується для створення централізованого RP між двома різними прикордонними маршрутизаторами. SRP створить оптимізований шлях від централізованого RP до приймачів за допомогою моделі дерева Штайнера. BRP виконує ту саму оптимізацію, але передбачає, що кожен прикордонний маршрутизатор є RP. У третьому розділі описано ключові відмінності між цими двома різними оптимізаціями. Розділ четвертий детально описує підвищення продуктивності між SRP і BRP. SRP справді має переваги в продуктивності перед BRP, але залежить від умов навколишнього середовища. SRP працює краще в щільнішому середовищі приймача, що підтверджується результатами. Розділ четвертий також постулює підвищення продуктивності та те, як вони пов’язані з продуктивністю мережі та збереженням пропускної здатності.

У цих розділах буде створено всебічне розуміння того, як SRP можна використовувати для боротьби з аномаліями маршрутизації та збереженням пропускної здатності. Вони детально описують, як SRP можна застосувати до топології мережі, і обговорюють його ефективність. SRP має певні обмеження та

позитивні сторони. Усі ці атрибути були проаналізовані та піддані критиці, що дозволить зрозуміти оптимізацію SRP.

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому дослідженні було проведено глибокий аналіз та розглянуто різні аспекти оптимізації пропускної здатності в багатодомних топологіях мереж. Результати дослідження демонструють важливість оптимізації у контексті розповсюдження мультимедійного контенту через цифрові мережі.

1. Актуальність Теми та Сучасні Тенденції

Першочерговою важливістю виявилася актуальність теми у зв'язку із стрімким розвитком цифрового контенту. Зміна тенденцій в розповсюдженні мультимедійного вмісту визначає потребу у вдосконаленні систем розподілу та оптимізації пропускної здатності.

2. Ефективність Багатоадресної Маршрутизації

Результати вказують на ефективність багатоадресної маршрутизації як оптимального підходу для розповсюдження мультимедійного контенту в цифровому середовищі. Використання алгоритму SRP виявилося дієвим для створення централізованого підходу та оптимізації мережі.

3. Проблеми та Перспективи Майбутнього Дослідження

Тривалість повторної конвергенції та артефакти в мережі, пов'язані з втратою сигналу, залишаються актуальними питаннями. Подальше дослідження може призвести до розробки нових методів вирішення цих викликів та покращення діючих систем.

4. Переваги Моделей SRP та BRP

Порівняльний аналіз SRP та BRP виявив переваги SRP у щільних середовищах приймачів. Проте, ураховуючи умови навколишнього середовища, обидва підходи можуть знаходити своє застосування.

5. Внесок у Розвиток Технологій

Це дослідження внесло важливий внесок у розвиток технологій розповсюдження мультимедійного контенту. Виявлені підходи та алгоритми можуть слугувати основою для подальших досліджень та розвитку систем цифрового розподілу, сприяючи покращенню якості обслуговування для кінцевих користувачів.

РОЗДІЛ 2 СИСТЕМНІ АСПЕКТИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ У КОНТЕКСТІ НАДЗВИЧАЙНИХ СИТУАЦІЙ

У цьому розділі обговорюватимуться типові налаштування топології та інші методи розподілу в різних топологіях мережі. Це також дасть уявлення про те, як окремі інструменти можна використовувати для виявлення аномалій маршрутизації в таблиці одноадресної маршрутизації. Ці методи важливі для виявлення проблем і можуть бути використані для запуску алгоритму швидкого відновлення

2.1. Топологія розподілу

Розповсюдження IPTV — це зростаюча тенденція, у яку інвестують все більше постачальників контенту. Витрати на розгортання зменшуються завдяки розширенню послуг високошвидкісного Інтернету. Кінцевому користувачеві потрібне лише високошвидкісне підключення до Інтернету та приставка (STB). Цей STB зазвичай підключається до домашньої мережі кінцевого користувача, який використовуватиме маршрутизатор як шлюз до мережі провайдера

Це високошвидкісне підключення до Інтернету для кінцевого користувача може бути DSL, кабельним або навіть оптоволоконним зв’язком до дому. Це з’єднання описано на малюнку 2.1 нижче. Вузол доступу на малюнку буде локальною петлею пристроїв агрегації. Це буде останній стрибок перед прямим запуском до домашнього користувача. З цього моменту вузол доступу отримуватиме вміст від мережі агрегації. Ця мережа агрегації містила б безліч різних вузлів доступу. Мережа агрегації, наведена на малюнку 2.1, може представляти локальну територію, наприклад місто або менший регіон залежно від щільності

Мережу розподілу можна описати як місцевого постачальника послуг. Місцевий постачальник послуг використовуватиме свою мережу для розповсюдження відеопотоків своїм кінцевим користувачам. Останньою частиною дерева розподілу є відеоголовка, куди відеоконтент вставляється в мережу [1]. У

міру того, як відеоінформація проходить мережею від відеоголовки, вона розповсюджується ширше. Перевага такої топології полягає в тому, що канали, які можуть бути представлені як багатоадресні потоки, можуть бути перерозподілені через інші мережі розподілу. Це дозволяє іншим постачальникам послуг змінити бренд каналів і продавати їх кінцевому користувачеві

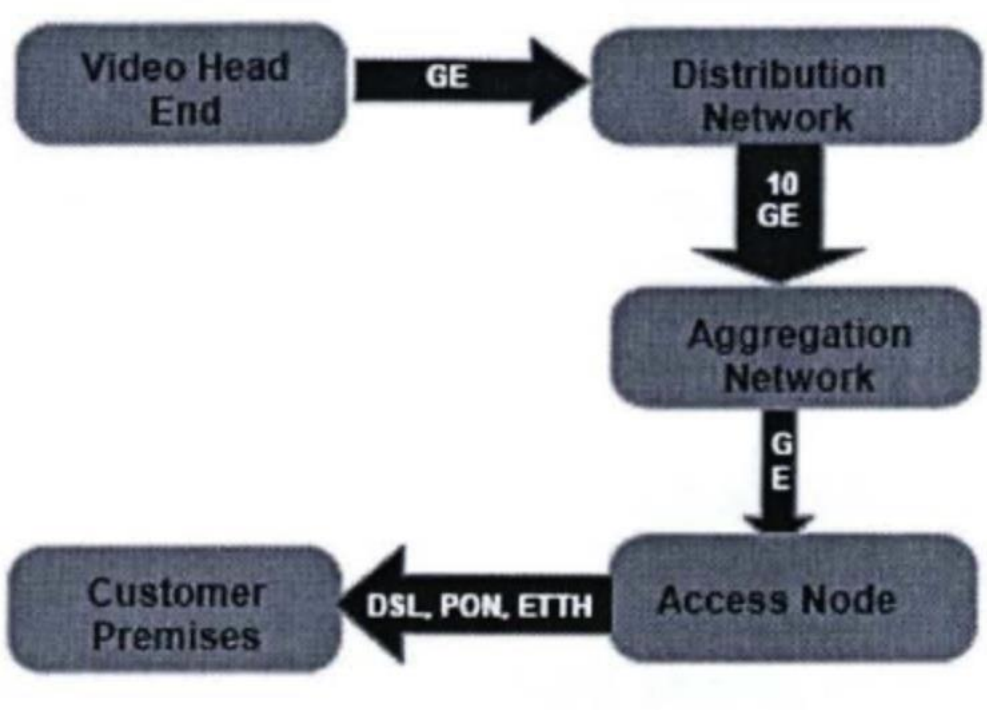

Рис. 2.1. Огляд розповсюдження

На малюнку 2.1 представлено загальний огляд різних рівнів топології. Як ці топології взаємодіють, дуже важливо. Широкомовне відео зазвичай надсилається через різні топології за допомогою багатоадресної передачі. Це забезпечує ефективний спосіб розповсюдження відеотрансляції. Іншим методом трансляції відео є використання протоколу реального часу (RTP) на транспортному рівні. R TP дозволяє виправляти помилки, а також включає послідовність пакетів і мітки часу, які мають бути реалізовані в наступному поколінні кодерів трансляції. Зазвичай джерела багатоадресного відео розташовуються на головній частині. Використання кодера MPEG інкапсулює джерела відео в IP-адресу, якій призначається унікальна групова адреса для багатоадресного розповсюдження. STB у місці розташування користувача видасть запит на приєднання за протоколом керування групами

Інтернету (IGMP). Цей запит буде перенаправлено для створення SPT на основі стану (S,G). Після того, як дерево буде створено, воно забезпечить шлях для передачі багатоадресних пакетів до кінцевих користувачів [1].

2.2.1 Розмова про пропускну здатність

Із збільшенням практики надлишкового забезпечення мереж Інтернет-провайдери (INP) повинні знайти нові методи зменшення навантаження на систему. Протокол багатоадресної передачі при правильному використанні може забезпечити зменшення пропускної здатності всієї мережі. Цей багатоадресний протокол заснований на RFP і таблиці одноадресної маршрутизації. Проблема, пов’язана з такою структурою, полягає в тому, що вона не забезпечує необхідної схеми керування для більш ефективного маршрутизації багатоадресного трафіку [14]. Традиційні методи оптимізації багатоадресної маршрутизації базувалися на моделі дерева Штайнера. Ці методи були використані для того, щоб зменшити загальну пропускну здатність системи, але є певні обмеження. Обмеження є результатом використання дерева Штейнера. INP зазвичай не бажають ділитися специфікаціями маршрутів і працювати з іншими INP для більш ефективного маршрутизації трафіку. INP зазвичай пов’язані зі своїми бізнес-конкурентами, і такий обмін інформацією та співпраця позбавить їхньої конкурентної переваги. Тип інформації, яка буде передаватись, у деяких випадках порушуватиме конфіденційність і цілісність системи [3]. Оскільки збереження міждоменної пропускної здатності не є життєздатним варіантом, наступним логічним кроком оптимізації буде внутрішньодоменна маршрутизація. Внутрішньодоменна мережа знаходиться під повним контролем INP, що дозволить швидко розгортати будь-які схеми оптимізації. Змінюючи маршрутизацію в мережі, можна сформулювати оптимізований шлях, який може зменшити споживання пропускної здатності всередині домену. Інша проблемна область – між міждоменними та внутрішньодоменними мережами. Ці дві різні мережі можна побачити на малюнку 2.2. По суті, ці два домени представляють дві різні топології. Одним із прикладів двох різних доменів є постачальник послуг Інтернету та велика організація. Кілька

з’єднань між цими доменами розглядатимуться як топологія мультидому. Як правило, між цими двома точками є велика затор [4]. Оскільки вартість високошвидкісних з’єднань знижується, все більше INP інвестують у багатодомні топології. Ця топологія створює кілька зв’язків між внутрішнім і між доменом. Це служить двом цілям; один для балансування навантаження, а другий для відновлення після відмови. Топології з декількома адресами можна використовувати для зменшення пропускної здатності та зменшення перевантаження на інших каналах. Приклад багатодомного підключення можна побачити нижче на малюнку 2.2. R представляє внутрішньодоменну мережу, до якої підключено багатодомні з’єднання. Основний домен R міститиме r отримувача, який представлятиме кінцевого користувача. У верхній частині малюнка в домені S є s, який представляє джерело багатоадресної передачі, яке поширюватиметься вниз через різні домени. Вихідний домен має агреговану IP-адресу P 5 • N на малюнку представляє суміжні домени, які з’єднані з доменом R прикордонними маршрутизаторами b 1 ... bn[3]. Ці прикордонні маршрутизатори забезпечують з’єднання між доменом R та іншими суміжними доменами N, що забезпечує з’єднання з кількома адресами

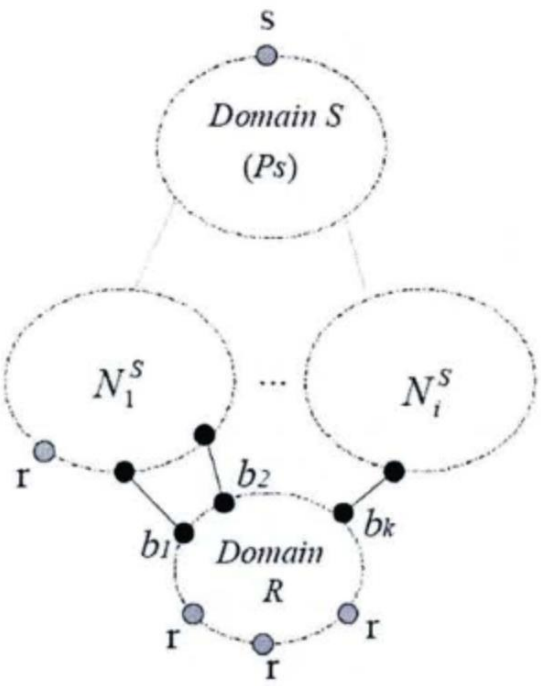

Рис. 2.2. Багатодомне підключення

Цей огляд типової топології мережі було спрощено, щоб продемонструвати структуру, яку необхідно враховувати під час оптимізації. Оскільки вже було встановлено, що міждоменна оптимізація непрактична, тепер стоїть завдання розглянути, як оптимізувати внутрішньодоменну структуру, таку як домен R. Є два основні аспекти, які вже були описані. Перший аспект полягає в тому, який прикордонний маршрутизатор вибрати, щоб мінімізувати споживання пропускної здатності. У поєднанні з першим аспектом є другий, який полягає в тому, як маршрутизувати багатоадресний потік у межах домену R, щоб зменшити споживання [3]. Ці два різні завдання оптимізації можна співвіднести для подальшого зменшення споживання пропускної здатності.

2.2.2. Реалізація збереження смуги пропускання

Традиційно спеціальний алгоритм оптимізував би шлях у топології, а потім він реалізовувався за допомогою MPLS. MPLS можна використовувати для керування великою кількістю різноманітного трафіку залежно від специфікацій оператора мережі. Хоча реалізація шляху MPLS є одним із способів керування багатоадресним потоком, існують обмеження масштабованості. У межах внутрішньодоменної мережі може бути розгорнутий протокол з кількома топологіями. Це дозволить уникнути використання шляхів MPLS, які будуть потрібні для маршрутизації багатоадресного трафіку. Це мультитопологічне розширення (MT) може бути застосоване до IGP [5,6] у межах внутрішньодоменної топології. Це розширення дозволяє використовувати різні ваги зв’язку для різних протоколів. Вага посилання може бути застосована для всього одноадресного трафіку, тоді як інша вага може бути застосована для багатоадресного трафіку. Це головна передумова цієї статті, яка полягає в тому, як ефективно контролювати багатоадресний потік, щоб забезпечити оптимальне споживання пропускної здатності. Ця внутрішньодоменна маршрутизація базується на вагових коефіцієнтах зв’язку IGP. Було проведено порівняльний аналіз, який показує, що використання мультитопології для контролю ваги каналів через IGP є ефективним способом контролю трафіку порівняно з аналогом MPLS [7,8,9]. Цей тип транспортного

потоку вважається Traffic Engineering (TE). Було показано, що вагові коефіцієнти внутрішньодоменних каналів є ефективним засобом контролю трафіку за допомогою застарілих маршрутизаторів [10], і шляхом застосування методів оптимізації до цього методу можна реалізувати збереження пропускної здатності

2.2.3. Мультитопологія

Використання Multi-Topology використовується як розширення існуючих протоколів IS-IS і OSPF. Це дозволяє визначати ваги посилань для кожного посилання на основі типу необхідного додатка. Наприклад, під час використання багатотопологічного OSPF (MT-OSPF) біт ідентифікатора MT (MT-ID) зі значенням 1 означатиме, що MT-OSPF явно використовується для багатоадресної передачі. Перевага Multi-Topology при використанні в поєднанні з Multicast IGP M-IGP полягає в тому, що INP може вказати вагові значення каналу лише для M-IGP. Ця зміна не вплине на інші протоколи. У цьому розділі буде детально описано мультитопологію. Це робиться для того, щоб краще зрозуміти, як він використовується та реалізується. M-IGP оброблятиме аспекти маршрутизації всередині домену. Багатоадресний домен BGP (M-BGP) містить певні поля для ідентифікації відомостей про сімейство адрес (AFI) та відомостей про сімейство підадрес (SAFI) під час оновлення маршрутизації BGP. По суті, ця інформація дозволяє ідентифікувати різні транспортні потоки. Коли AFI = 1 і SAFI = 2 означає, що це повідомлення BGP міститиме групу багатоадресної розсилки IPv4 [3]. Змінюючи групу, це можна адаптувати до обговорюваної моделі оптимізації. Це дозволить розмістити призначення ваги посилання. На малюнку 2.3 показано оптимізацію M-IGP і M-BGP

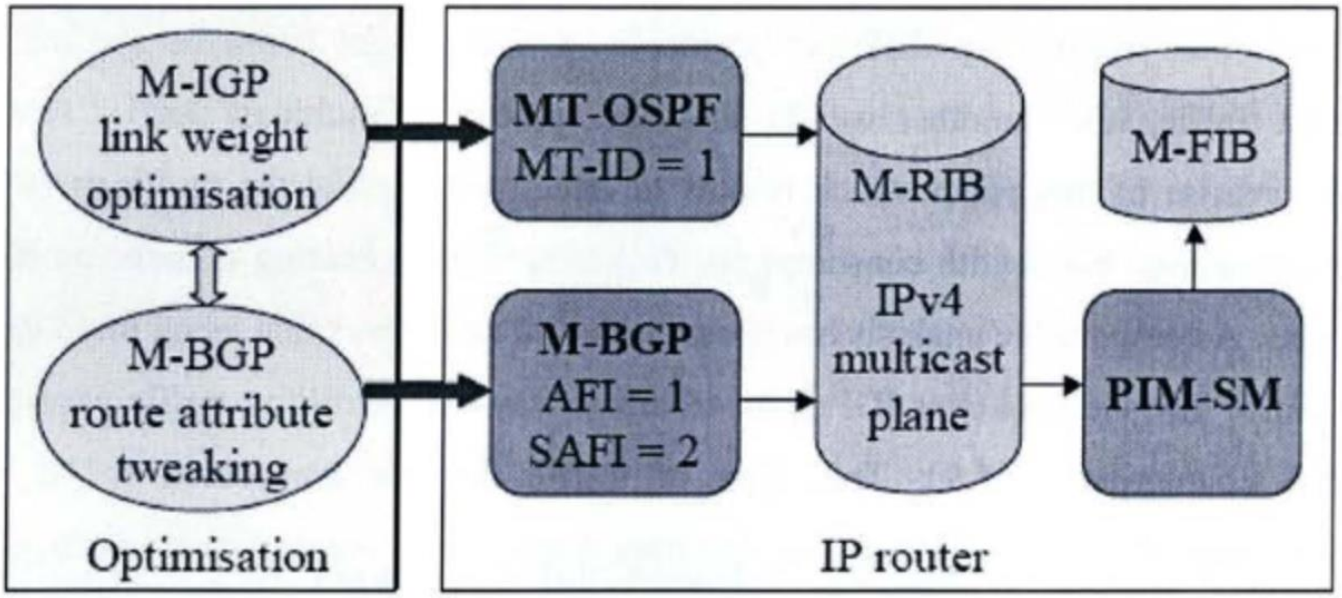

Рис. 2.3. Огляд багатоадресного трафіку

На малюнку 2.3 буде запущений алгоритм оптимізації для обчислення оптимального шляху з'єднання як для M-IGP, так і для M-BGP. Вони корельовані для забезпечення максимального збереження пропускної здатності. Після завершення оптимізації тег MT-ID використовується для визначення шляху посилання для M-IGP. Для полів M-BGP, таких як AFI та SAFI, змінено, щоб вказати конкретну вагову структуру посилання. Потім ці дві частини інформації співвідносяться в межах IP-маршрутизатора в таблиці багатоадресної маршрутизації M-RIB для кожного вихідного префікса. Інформаційна база багатоадресної переадресації (M-FIB) містить вхідні і вихідні інтерфейси для кожної групи [3]. Це дозволяє керувати маршрутизацією кількох груп, оптимізованих у мережі

2.2.4 Оптимізація посилань між доменами та між ними

Необхідність зменшити споживання пропускної здатності топології багатоадресної передачі стає все більш поширеною в дослідницькому співтоваристві. Концепції, які були розроблені в [3], забезпечують важливу основу для оптимізації багатоадресної передачі. З цієї причини ця дисертація буде зосереджена на цих концепціях і використовуватиме документ [3] як еталон для порівняння запропонованого алгоритму SRP, який буде обговорено більш детально

в Розділі 3. Алгоритм, розроблений у [3], буде називатися Border router Точка зустрічі (BRP) це пояснюється характеристиками алгоритму

BRP використовує новий підхід до оптимізації зв’язку шляхом моделювання джерела та приймачів, налаштованих як дерево Штайнера. Цей підхід додатково розширено, щоб включити кілька прикордонних маршрутизаторів у міждоменне середовище. Часова складність вирішення підходу дерева Штейнера для великого набору вузлів неможлива. Алгоритм BRP використовує генетичний алгоритм (GA) для створення евристичного підходу під час моделювання дерева Штейнера. На малюнку 2.4 наведено огляд алгоритму BRP. Алгоритм BRP оптимізує кілька багатоадресних потоків у внутрішньодоменному середовищі. Спочатку генетичний алгоритм визначає початкові набори маршрутизаторів. Алгоритм продовжує групувати весь багатоадресний трафік на основі IP-префіксів. Ці префікси потім сортуються на основі споживання пропускної здатності. Префікси вибираються для оптимізації на основі споживання пропускної здатності. Оптимізація застосована у вигляді моделювання дерева Штейнера. Нарешті використовується перевірка, щоб визначити, чи оптимізований шлях не споживає пропускну здатність більше, ніж доступна. Цей процес повторюватиметься, доки не буде оптимізовано всі потоки

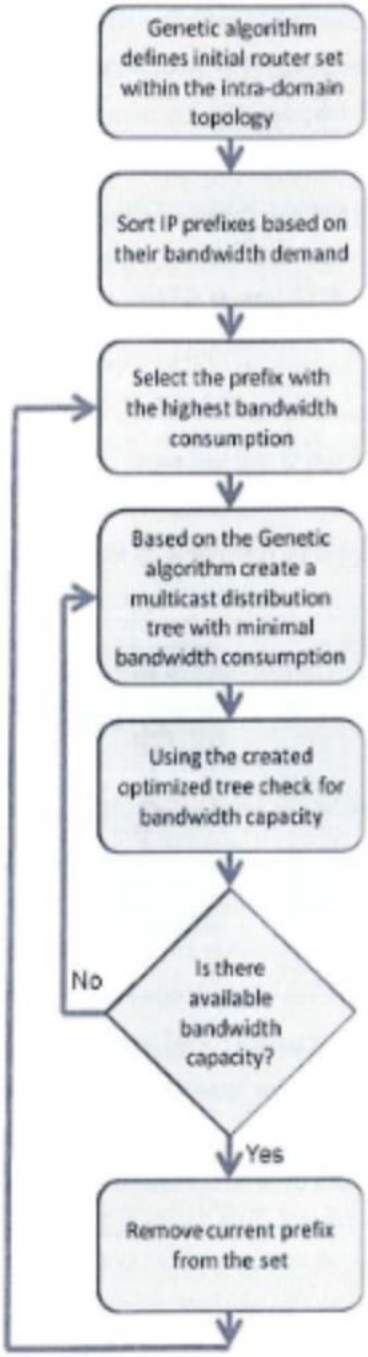

Рис 2.4 Огляд BRP

Ефективність алгоритму BRP порівняно з іншими формами оптимізації продемонстрована на малюнках 2.5 і 2.6. На цих малюнках алгоритм BRP визначено як C-HPR-GA. Топологія, використана для тестування цих фігур, була заснована на GEANT [11] мережа, яка складається з 23 вузлів і 76 односпрямованих каналів. Алгоритм BRP у цій дипломній роботі є алгоритмом C-HPR-GA у [3]. На малюнках 2.5 і 2.6 зображено внутрішньодоменну топологію, огляд алгоритму C-HPR-GA

(BRP) можна побачити на попередньому малюнку 2.4. У топології передбачалося, що кожен префікс може бути досягнутий максимум 50% прикордонних маршрутизаторів усередині доменної топології. Пропускна здатність кожного каналу масштабується до 104 одиниць. При використанні кросинговеру генетичного алгоритму значення мутації змінювалися від 0,3 до 0,001. На малюнку 2.5 показано порівняння різних алгоритмів. Одна з відмінностей алгоритмів полягає у використанні підходу підрахунку переходів (HC) замість використання генетичного алгоритму для обчислення оптимізованого шляху. Ці два різні алгоритми оптимізації далі поділяються на неконтрольований алгоритм Hot Potato Routing (HPR) U-HPR-HC або керований алгоритм HPR C-HPR-HC. Підхід HPR — це безбуферний дизайн для маршрутизації. У HPR окремі пакети надсилатимуться по одному до місця призначення. Останній алгоритм Single-GA подібний до алгоритму C-HPR-GA (BRP), за винятком того, що він обмежує його оптимізацію одним прикордонним маршрутизатором. На малюнку 2.5 видно, що коефіцієнт збереження пропускної здатності найбільший для U-HPR-HC, який має коефіцієнт 78%. Це означає, що він зберігає 28% ресурсів пропускної здатності внутрішнього домену. C-HPR-GA зберігає 15% ресурсів внутрішнього домену. Для порівняння, внутрішньодоменне збереження C-HPR-GA не таке ефективне, як U-HPR-HC. C-HPR-GA компенсує за допомогою балансування навантаження на міждоменні посилання. Це можна побачити на малюнку 2.6, де C-HPR-GA забезпечує найнижче використання каналу в порівнянні з іншими алгоритмами [3]. Цей компроміс забезпечує найкращу оптимізацію між і всередині домену.

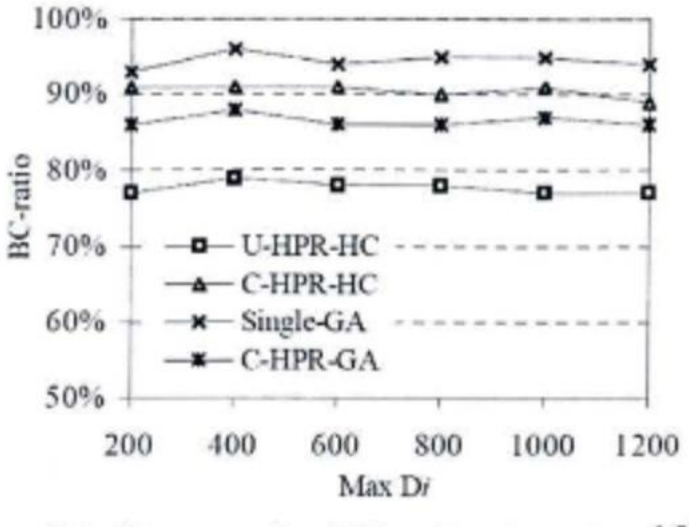

Рис. 2.5. Порівняльний коефіцієнт BC, де a == 10^3

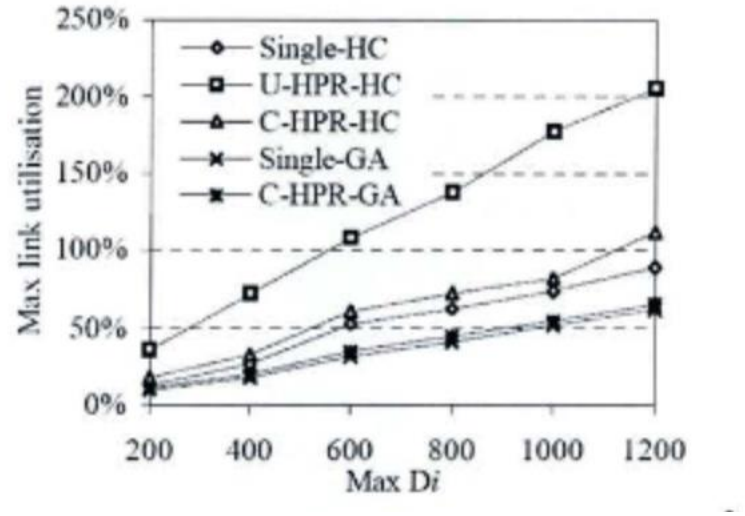

Рис. 2.6. Використання міждоменного посилання де a == 10^3

Хоча C-HPR-GA (BRP) забезпечує оптимізацію як міждоменного, так і внутрішньодоменного збереження пропускної здатності, він збільшує затримку пакета. Цей тип оптимізації стосується споживання пропускної здатності, а не затримки. Інша проблема — кількість повторів генетичного алгоритму. Час обчислення значно збільшиться в залежності від розміру мережі. Незважаючи на те, що генетичний алгоритм використовується для скорочення часу обчислення, він усе ще базується на налаштуваннях [3]. Вони вирішили обчислювати всі алгоритми оптимізації віддалено. Хоча це зменшує час обчислення, це не вирішує ситуацію,

коли зміни топології вимагатимуть постійних оновлень через потенціал більших зовнішніх системних ресурсів. Іншою ситуацією є збій посилання, який не розглядається в цьому документі. Якщо трапиться збій, це може скомпрометувати потік. Оскільки цей тип оптимізації не враховує збій зв'язку, затримка відновлення потоку буде довшою

2.3. PCA

2.3.1. Виявлення несправності

Технології, описані в попередніх розділах, забезпечують основу для надання послуг та інструментів, щоб кінцевий користувач отримував вигоду від IPTV. Надійне розповсюдження таких програм є головною метою цієї статті. Те, що було описано досі, є основним розподілом та оптимізацією таких топологій мережі. Хоча оптимізація створить ефективну мережу всередині доменного середовища, вона не гарантує надійності. Існує безліч різних несправностей, які можуть порушити роботу служби. Хоча неможливо повністю передбачити ці несправності, можна вжити певних заходів для визначення джерела та, можливо, створення топології чи алгоритму для скорочення часу відновлення. Дослідження в [3] визнало, що більше роботи потрібно зосередити на оптимізації та взаємодії з помилками. Досліджуючи різні несправності, можна проаналізувати їх структуру, щоб з ними можна було боротися

Топології, які використовуються для IPTV і подібних програм, досить великі. У розділі 2.1 типове поширення багатоадресної передачі IPTV може відбуватися в будь-якій топології та в будь-якій мережі. З цієї причини потрібен глибокий аналіз, щоб повністю зрозуміти внутрішню роботу можливих аномалій. Протокол BGP використовує автономну систему (AS), яка є сукупністю IP-мереж та інших ресурсів. Ця інформація використовується для диктування маршрутизації та підтримки інформації про посилання

Маршрутизатор BGP періодично надсилатиме оголошення про маршрутизацію, що містять повідомлення про префікси щодо його AS або AS, з

якими він пов’язаний. Ці повідомлення маршрутизації, які використовуються для встановлення потоку трафіку, життєво важливі для забезпечення правильної схеми трафіку. У разі неправильної конфігурації можуть виникнути проблеми. Це може спричинити згубні наслідки та створити масове уповільнення в Інтернеті [12].

Однією з таких неправильних налаштувань є викрадення маршруту. Це відбувається, коли маршрутизатор BGP оголошує маршрут, до якого він не має доступу. В основному відбувається те, що пакети будуть відкидатися. Іншим типом неправильної конфігурації є витік маршруту. Це відбувається, коли один маршрутизатор BGP надсилає більше маршрутів одноранговому вузлу, ніж він може обробити. Коли це станеться, одноранговий маршрутизатор буде перевантажений і вплине на стабільність маршрутизації. Цей ефект також може викликати коливання маршруту, що також споживає ресурси маршрутизатора [12].

Виявлення аномалій руху зазвичай базується на статистичному підході. Це досягається шляхом порівняння поточної статистичної інформації щодо маршрутизації з попередньою історією. За допомогою цього порівняння, якщо поточна статистична інформація відхиляється від історичної інформації, тоді буде припущено, що існує можлива аномалія. Коли відбувається оновлення BGP, система відстежуватиме частоту цих оновлень, а також час, потрібний для конвергенції префікса. Базуючи виявлення аномалій на історичній інформації, легше реалізувати схему виявлення аномалій. Ще одна перевага цього типу методу статистичного виявлення полягає в тому, що він надзвичайно ефективний при обробці величезних обсягів даних. Він дійсно має недоліки в здатності виявляти складні проблеми. Іншим головним недоліком є те, що для встановлення порогового значення потрібна точна настройка. Порогове значення буде різним залежно від типу мережі, що використовується. Якщо це порогове значення встановлено на високе або низьке, це може спричинити значні хибні спрацьовування або, ще гірше, не виявити певні аномалії. Порогове значення було визначено як «магічне число» в [13], яке необхідно скоригувати для належної роботи алгоритму. Підхід, заснований на навчанні, як описано в [13], має кілька ключових відмінностей. І статистичний підхід, і підхід, заснований на навчанні, використовують історію як порівняння. Але

підхід, заснований на навчанні, збирає свою історію інакше, ніж стандартний статистичний підхід. Він також має різні методи тестування. По суті, це досягається тим, що поведінка оновлення BGP представлена у вигляді вектора. Цей вектор містить певні аспекти оновлень BGP і може використовуватися для відображення певних шаблонів у багатовимірному векторному просторі. Виходячи з цих відображених точок, якщо точка відображена далеко від початкової точки домену, це вважається можливою аномалією. Якщо іншу точку відображають на іншому місці, яке вважається нормальним місцем, це означатиме нормальну роботу. Цей тип дослідження спрямований на виявлення кластерів нормального функціонування. Це дозволить правильно позначати аномалії. Це має різні переваги перед іншими підходами, такими як операція зі змінним числом, яке визначає швидкість виявлення. Інша перевага полягає в тому, що цей підхід включає властивість інваріантності зсуву. Це означає, що якщо сплеск оновлень відбувається випадково в часі, не має значення, коли це відбувається, а те, наскільки рівномірним є сплеск. Ця однаковість стосується часу оновлень у пакеті. Цей метод досягається за допомогою вейвлет-перетворення, яке є технікою обробки сигналу. По суті, він відображає сигнали в частотно-часових областях, щоб їх можна було легко представити [13]. Це відрізняється від використання методу PCA для порівняння статистичної кореляції між кожним оновленням BGP. За допомогою методу PCA, якщо відбувається відхилення від заданого шляху, це вважається аномалією.

2.3.2. Збір даних

Інформацію про маршрутизацію було зібрано з повідомлень маршрутизації Border Gateway Protocol (BGP) і Interior Gateway Protocol (IGP). Цей збір було здійснено за допомогою Packet Design Route Explore (REX). REX використовується для захоплення всієї інформації про внутрішню маршрутизацію між маршрутизаторами BGP. Ця інформація не враховує атрибути вилучення маршруту. З цієї причини маршрутизатори, підключені до REX, передаватимуть свою повну інформацію про маршрутизацію, включаючи всі їхні атрибути. REX також

відстежує суміжні маршрутизатори IGP і збирає всю інформацію про статистику каналів, яка може бути розроблена з цих каналів [12].

Результати статті [12] базуються на двох різних наборах даних. Перший набір даних був зібраний в U.C. Берклі з серпня по грудень 2003 р. U.C. Berkeley складається з OSPF із чотирма зонами, який поєднується з IGP. REX було ініційовано між периферійними маршрутизаторами BGP. Потім цей процес було повторено до провайдера. Статистичні дані, зібрані REX, наведено в таблиці 2.1 нижче**.**

Таблиця 2.1.

Статистичні дані зібрані з двох різних джерел

	U.C. Berkeley	US
BGP Nexthops	13	9150
Prefixes	12600	200000
Routes	23000	1500000

2.3.3. Аналіз даних за підходом PCA

Дані були проаналізовані двома різними методами; аналітична модель і візуальна модель. Використана візуальна модель називається TAMP (префікси порога та злиття). Аналітична модель, яка була використана, була названа стемінгом. TAMP враховує всі префікси. Потім на основі цих префіксів створюється віртуальне дерево. Потім кожному краю дерева призначаються ваги на основі рідкості префіксів, реалізованих на певному краю. Потім TAMP продовжить обрізати всі вузли та ребра, які становлять менше 5% усього графіка. TAMP представляє лише знімок у часі.

TAMP можна використовувати для виявлення певних типів неправильних конфігурацій, таких як бекдор-маршрути та ситуації балансування навантаження.

Він може виявити, коли виникає маршрут заднього ходу, як показано на малюнку 2.7. Маршрут бекдору визначено між 128.32.1.222 та 169.229.0.157.

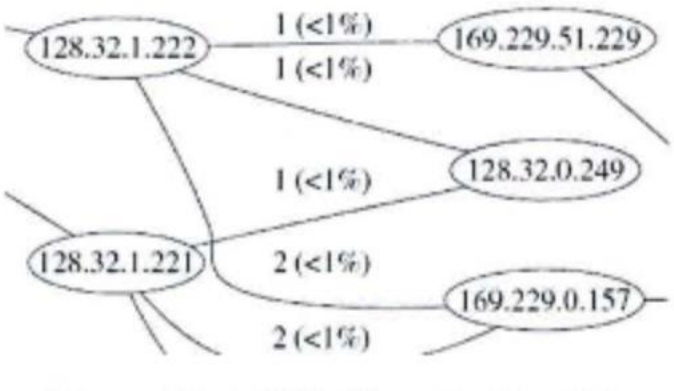

Рис. 2.7. Візуалізація TAMP

Стемінг — це аналітична модель, яка корелює повторення шляху AS для систематичного виявлення аномалії. Метод стеммінгу базується на моделі аналізу головних компонент. Відстежуючи відкликання маршрутів BGP, можна екстраполювати послідовність. AS було визначено як певну послідовність, таку як 1•• a 0 • Ці вилучення представляють певну послідовність, яку можна визначити як c = xha 1 ••• a 0 p. Де x — одноранговий вузол, який знімає з певного префікса p. Ці послідовності відбуваються протягом певного періоду часу і можуть бути визначені як потік; де C= c1•. c2 .. cm представляє потік. Потім алгоритм зведе в таблицю пари суміжних AS, які зустрічаються в потоці C. Ранжуючи ці пари, алгоритм може визначити потенційні проблемні області. Приклад цього можна побачити нижче на малюнку 2. 8. Сусідня пара 11423-209 зустрічається кілька разів, що вказує на місце проблеми. Це визначається як місце несправності

```
W 192.96.10.0/24 11423 209 701 1299 5713
W 207.191.23.0/24 11423 11422 209 4519
W 192.96.10.0/24 11423 209 701 1299 5713
W 212.22.132.0/23 11423 209 1239 3228 21408
W 203.14.156.0/24 11423 209 701 705
W 209.5.188.0/24 11423 11422 209 1239 3602
W 12.2.41.0/24 11423 209 7018 13606
W 12.96.77.0/24 11423 209 7018 13606
W 62.80.64.0/20 11423 209 1239 5400 15410
W 62.80.64.0/20 11423 209 1239 5400 15410
```

Рис. 2.7. Префікс відкликів

У поєднанні з моніторингом кореляцій стемінг може використовувати TAMP як візуалізацію, щоб дати більш повне розуміння того, що відбувається. Стемінг можна використовувати для виявлення одного коливання маршруту через те, як воно співвідноситься з даними. Якщо стемінг залишити для виконання протягом короткого періоду часу, через кілька годин ці коливання будуть виглядати як сильна кореляція, і їх можна буде легко виявити. Stemming також може виявити неправильні конфігурації щодо витоків маршрутів, де маршрути спрямовані на довший шлях, що може бути небажаним. Це залежить від політики, яку може застосувати провайдер

Наступним кроком, який [12] намагається розглянути, є те, як співвіднести політики маршрутизації, визначені у файлі конфігурації маршрутизаторів, із фактичною маршрутизацією, яка має місце. Політики маршрутизації не оголошуються в подіях AS, і це ускладнює їх моніторинг. Стемінг використовує сильну кореляцію для виявлення проблем, але без перехресного порівняння з файлом конфігурації важко проаналізувати ситуацію, щоб забезпечити найкращий курс дій

Поточна робота виконується для включення трафіку в аналіз для виявлення неправильної конфігурації маршрутизації, яка може розподіляти префікси на основі навантаження трафіку. Це створює проблему, коли невеликий блок префіксів може містити 90% трафіку. Переставляючи префікси, це забезпечить більш збалансовану

маршрутизацію трафіку. Трафік і маршрутизація взаємопов'язані, і в цій ситуації їх потрібно розглядати одночасно

2.3.4 Використання вейвлетів

У цьому розділі розглядаються інші методи виявлення потенційних аномалій мережі. Розуміння аномалій та їх виникнення вказує на важливість моделі відновлення після відмови. Wave lets використовуються в процесі для перетворення оновлень префікса у векторне представлення. Набір даних визначається з 24-годинними інтервалами. Це одне оновлення фактичного розрахунку. Це значення регулюється та може змінюватися залежно від моделі виявлення. Кожне оновлення і моделюється в послідовності S і має довжину n. Для цієї послідовності виконується дискретизоване безперервне вейвлет-перетворення. Використовується версія вейвлет-перетворення Хаара. Цей вейвлет описано нижче в рівнянні 2.1.

Де r означає переклад, а $\boldsymbol{\delta}$ — масштаб. Тепер дискретизоване перетворення визначено в рівнянні 2.2 [13].

$$\boldsymbol{\Psi}\left(\frac{\boldsymbol{x-t}}{\boldsymbol{\delta}}\right) \tag{2.1}$$

$$\boldsymbol{\gamma(\delta, r)} = \sum \boldsymbol{S(x)} \frac{\mathbf{1}}{\sqrt{\boldsymbol{\delta}}} \boldsymbol{\Psi}\left(\frac{\boldsymbol{x-r}}{\boldsymbol{\delta}}\right) \tag{2.2}$$

Це перетворення має набір шкал від 8 0 до 8 r . Для початкового вейвлета було обрано масштаб 20 секунд. Це означає, що 8 0 = 20, а потім масштаби 8 i+I=2 8 i·r можуть приймати значення з набору { 1,2, ... ,n), і це перетворення призводить до y(8, r), це r для часу та 118 для частоти. Після цього перетворення вихідний набір даних стане ще більшим. Це створює проблему, оскільки рішення полягає в тому, щоб часто розглядати лише великі значення пакетів. y(8, r). Беручи пікові значення пакетів і зберігаючи тривалість між іншими піковими значеннями, це дозволяє зменшити дані в наборі перетворення. Інша техніка зменшення даних полягає в тому, щоб взяти наближені значення піків y(8, r). Ця техніка виявляє найбільше

значення з y(8, r) і встановлює його як r max· Інтервал для цих пікових значень буде між (0, r maxl). Потім дані зберігаються в гістограмі. Використання цієї гістограми та інших властивостей гістограма бен буде (0, v]. Це буде визначено як: (vQ1 + &Y, v(l + &Y+ 1], i = 0, 1, 2.... Експериментальні значення за замовчуванням, які спочатку використовувалися) забезпечили чудові результати та деталізовані так: v = 0,1 і £ = 0,5. По суті, гістограма — це спосіб збереження пікових значень у формі вектора. Це більш ефективний спосіб зберігання та доступу до необхідних даних. Детальна інформація можна знайти в [13].

Вище було описано, як фактичні дані стискалися та зберігалися. Для кожного окремого методу потрібна певна база даних для індексування доступних зібраних даних. Це необхідно незалежно від методу виявлення, який використовується. Обробка даних для цього підходу, заснованого на навчанні, полягає в кластеризації даних. За допомогою кластеризації цих даних можна виявити тенденції. Якщо більшість маршрутів поводяться певним чином, це буде показано як великий кластер, і все, що відхиляється від нього, представлятиме можливу аномалію. Передбачається, що кластеризація підвищить ефективність. Спочатку вектори були створені за допомогою гістограми, потім кластеризація застосована до префіксів. На малюнку 2.9 показано розміри кластерів. З цього малюнка легко визначити, що більшість префіксів знаходяться в одному кластерному угрупованні.

У першому кластері приблизно 170 префіксів. У другому кластері їх немає і так далі, поки не буде досягнуто кластер ih. Тут згруповані можливі аномалії. На наступному малюнку 2.10 від a-d змінюються різні значення k. Ці значення k представляють кількість кластерів у вибірці даних. Регулюючи розмір k, це змінює чутливість алгоритму виявлення. Розмір кластера визначатиме деталізацію виявлення. Значення k визначає кількість категорій, які можуть збільшити або зменшити деталізацію кластера. Негативним аспектом цього є те, що час обчислення буде збільшено. Це може бути несуттєвим для невеликої вибірки, однак це створить проблему для більших вибірок. Чим менше значення k, тим менше пам’яті потрібно для обчислення. На малюнку 2.10 (a) видно, що в кластері понад 150 точок. Це використовується кластерне групування з п'яти. Це дає приблизну оцінку

потенційних аномалій. Збільшивши це значення від 5 до 30, можна побачити чітку картину. Ці графіки представляють оновлення BGP, і цю модель також можна адаптувати для інших типів, таких як оновлення OSPF. Та сама процедура буде повторена, і будь-яке відхилення від очікуваних значень буде вважатися аномалією.[13] Точки в кластері мають певну спільність для певного префікса. Була проведена робота по кореляції кількох кластерів префіксів. Це дає змогу досліджувати зв’язок оновлення між префіксами та виявляти можливі аномалії за допомогою тих самих методів кластеризації виявлення. Ця робота знаходиться на попередній стадії. Це все ще вимагає більш точного налаштування, щоб ізолювати аномалії. [13]

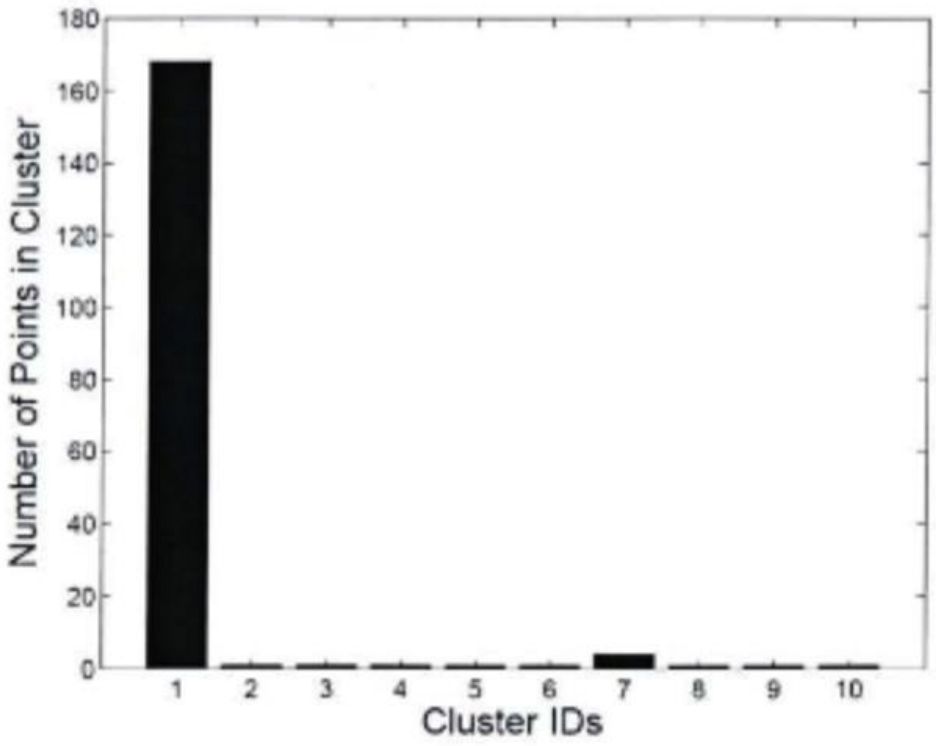

Рис. 2.9. Кластерні утворення

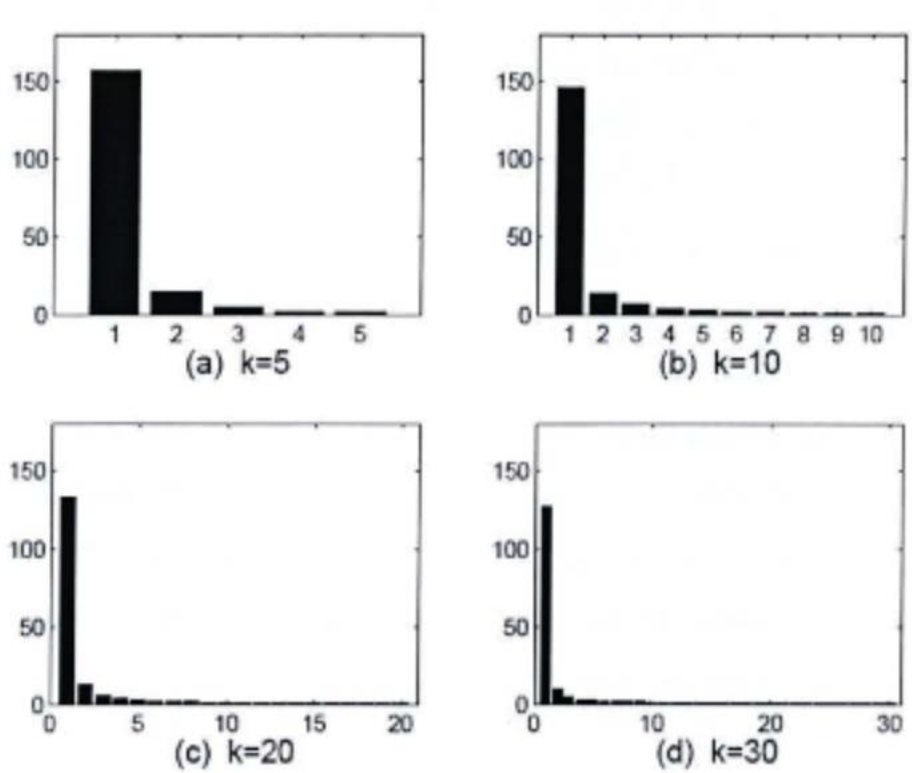

Рис. 2.10. Кластерні утворення з різними значеннями k

2.3.5. Виявлення аномалій руху трафіку

Виявлення аномалій трафіку пов’язане з виявленням аномалій маршрутизатора. Ці дві моделі виявлення взаємопов’язані, і їх слід розглядати одночасно. Більшість наявних наразі робіт не стосуються обох цих проблем. У цьому розділі розглядатимуться деякі ключові питання та надано огляд деяких загальних понять. Впроваджуючи ці поняття, ви отримаєте більше розуміння статистичного аналізу. У статті [12] обговорювалося, як схема виявлення базується на вилученні маршруту, оскільки обговорювалося, що майбутні дослідження включатимуть трафік. Наступним прогресивним кроком є співвіднесення вилучення маршруту з трафіком

Причина важливості трафіку полягає в тому, що трафік маршрутизується на основі того, як налаштовано маршрутизатор. Використовуючи цей метод визначення того, як трафік маршрутизується, можна створити модель для виявлення можливих помилок. Модель трафіку можна використовувати для виправлення аномалій маршрутизації під час балансування навантаження. Деякі маршрути

можуть бути налаштовані неправильно, і через них може проходити більше трафіку. Це може бути проблема конфігурації маршрутизації, і її потрібно вирішити. Ця проблема була виявлена в [12], і поточні рішення вивчаються

Як і аналіз аномалій маршрутизації, аномалії трафіку включають збір даних з наступною обробкою цих даних за допомогою різних методів. Аналіз цих даних може вказати, чи є аномалія зловмисною атакою, передачею великого файлу чи, що важливіше, збоєм маршрутизатора чи іншим типом неправильної конфігурації. У статті [16] вони також використовували вейвлет-модель для виявлення аномалій.

2.3.6. Використання PCA для аномалій руху

Першим кроком у застосуванні алгоритму PCA є визначення матриці трафіку. Ця матриця трафіку може містити цінну інформацію у формі Vi,j. Матриця може представляти пакети або байти за певний період часу та може використовуватися для організації безлічі різної інформації. Спосіб структурування матриці трафіку полягає в тому, що один вимір матриці трафіку міститиме інформацію про час, тоді як інший вимір стосуватиметься фактичних даних, таких як інформація про байти або ентропія адрес по відношенню до часу. Як обговорювалося в статті [15] m є стовпцем у матриці трафіку. Стовпці представляють IP-потоки. Коли PCA застосовується до матриці, він створить ортонормовані вектори. Ці вектори представляють найбільшу дисперсію порівняно з вихідною матрицею. Вони належать до підпростору k, де k <= m. Це k посилатиметься на звичайний підпростір мережі. Метод, у якому виявляються аномалії трафіку, коли k видаляється з підмножини; де n-k означає видалення нормальної підмножини, що залишить підмножину, яка містить аномалії. Вони описують цей процес у термінах випадкових величин, які мають форму матриці am x n. Розглядаються лише випадки, коли m < n, що визначається як більше спостережень, ніж змінних. Ця процедура використовується лише для моделювання фактичних потоків. Матриця трафіку – це представлення векторів у залежності від часу. Це визначається як v. Використовуючи модель, яка була визначена вище, тоді проектування v покаже, в якій області знаходиться цей вектор. Це вкаже, чи він є в підмножині аномалії. [15]

Кроки для застосування PCA до IP-потоків такі. Ці кроки також описано на малюнку 2.11

1. Реєстрація даних: це було досягнуто шляхом читання журналів даних Zebra всіх повідомлень BGP. Ці повідомлення містили вихідні та префіксні пари. Об’єднавши цю інформацію та проаналізувавши файли журналу, можна сформулювати повний детальний шлях

2. Агрегація трафіку використовується для розподілу даних на різні категорії. Завдяки групуванню певних характеристик це значно підвищило рівень успіху моделі виявлення PCA

3. Наступним кроком є застосування функції часового ряду ентропії до набору даних. Ці дані -+ представлені вектором vi. Він міститиме чотири окремі записи даних у формі viJ , ... ,ViJ +3. Ці записи визначаються як IP джерела, IP призначення, порт джерела та порт призначення. Ентропія буде застосована до вектора. Оскільки вектори поводяться як випадкові величини, можна застосувати ентропію. Приклад того, як це застосовується, наведено нижче. Коли на порт 80 сервера надходить багато трафіку, ентропія цього порту зменшується до 0. Це означає, що ймовірність збільшення трафіку, що підключається до порту 80, зростає.

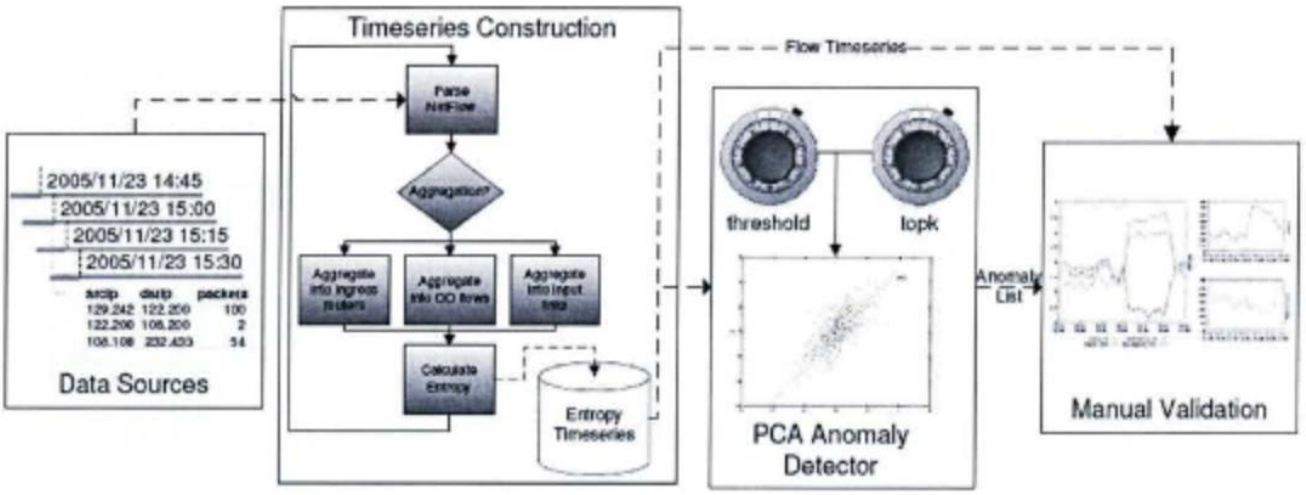

Рис. 2.11. Огляд кроку

Для перевірки результатів алгоритму PCA потрібна перевірка вручну. Це дозволить ідентифікувати помилкові спрацьовування. Ще одна перевага ручної

перевірки результатів полягає в тому, що PCA може не позначати точні моменти часу. Під час перевірки вручну можуть бути виявлені незначні зміни, які можуть розглядатися як помилки. На малюнку вище зображено дві змінні в детекторі аномалій PCA. Це змінні тонкої настройки, необхідні для зміни чутливості алгоритму PCA. Проведені тести показали, що цей хибнопозитивний рівень може коливатися від 3% до 16% [15].

2.3.7. Аналіз

Відстежуючи цей трафік на основі IP-адрес джерела та призначення, можна сформулювати шлях, який буде використано. Це можна зробити, включивши маршрути, необхідні для досягнення цього шляху. Знаючи наступний стрибок на шляху трафіку, можна виявити аномалії маршрутизації. Вони виявлятимуться як невідповідності. Якщо QoS вимагає певного шляху, і він відхиляється від шляху, це відображатиметься в аналізі PCA. Інформація про порт також може вказувати на надмірні проблеми з маршрутизацією, коли збільшення трафіку до певних адрес може бути спричинене недоліками маршрутизації. Цей трафік можна застосувати до певного протоколу та співвіднести з іншою інформацією про маршрутизацію, щоб вказати, чи існує потенційна проблема

ВИСНОВОК ДО РОЗДІЛУ 2

Кожен метод у підрозділах вище описує виявлення аномалій і розповсюдження IPTV у мережі багатоадресної передачі. Розділ 3 співвідносить ці дві ідеї шляхом розширення розділу 2.2.1, щоб включити моделі відмов. Збої можуть бути результатом різних аномалій, таких як коливання маршруту. Ці аномалії зазвичай проявляються у вигляді несправності з’єднання або зменшення пропускної здатності з’єднання. Ця базова інформація дає уявлення про збої, щоб можна було розробити оптимізоване рішення для зменшення впливу збоїв на топологію багатоадресної передачі.

РОЗДІЛ 3 СПІЛЬНА ОПТИМІЗАЦІЯ З ВІДНОВЛЕННЯМ ПІСЛЯ ЗБОЮ

3.1. Вступ

У цьому розділі розглядається оптимізація маршрутизації пакетів для маршрутизації між і в межах домену шляхом застосування алгоритму SRP. Алгоритм SRP оптимізує як балансування навантаження, так і збереження смуги пропускання в межах топології на двох прикордонних маршрутизаторах. Це досягається шляхом кореляції різних випадків оптимізації та проблем, описаних у основі, у розділі 2, які називаються BRP (гранична точка зустрічі). Розуміючи, як виникають збої зв'язку та типи збоїв, можна застосувати оптимізацію, щоб зменшити їхній вплив. BRP надає цінну інформацію щодо цілісності зв'язку. Виявлення відхилень може бути безцінним інструментом, який можна використовувати для виявлення та підвищення оптимізації оптимізації внутрішньо- та внутрішньодоменних посилань. Підхід, розглянутий у цьому розділі, полягає в кількісній оцінці наслідків збою з'єднання та визначення того, наскільки катастрофічним буде такий збій. Буде досліджено дві різні моделі. У [3] вони досліджували лише оптимізацію на основі збереження пропускної здатності. Цю ідею було додатково розширено, щоб включити збій зв'язку прикордонного маршрутизатора. Потім це порівнюється з новим підходом використання SRP (єдина точка зустрічі). SRP забезпечить стабільність у межах топології для всіх вузлів під нею. Ця стабільність досягається за рахунок використання функціональних можливостей RP (точка зустрічі). Якщо один прикордонний маршрутизатор виходить з ладу в багатодомній топології, для відновлення з'єднання потрібно лише повідомлення PIM Join від RP до другого прикордонного маршрутизатора. Дерево багатоадресної розсилки нижче RP залишається незмінним. Розміщення RP має вирішальне значення, щоб уникнути перебоїв у роботі служби. Обидві моделі RP і BRP описані нижче з описом їхніх характеристик і реалізації

3.2.1. Збереження пропускної здатності та балансування навантаження

Оптимізація посилань для мінімізації кількості посилань у дереві розповсюдження багатоадресної адреси є ключовим аспектом збереження пропускної здатності. На рисунку 3.1 визначено два різні шляхи, де посилання в шляхах представлені темними стрілками. Обидва прикордонні маршрутизатори b1 і b2 мають доступ до джерела. Загальна кількість посилань, що використовуються в цьому сценарії маршрутизації, становить 6. Оскільки обидва прикордонні маршрутизатори мають доступ до одного джерела, їх розташування в топології можна використовувати для створення оптимального шляху маршрутизації. У версії (b) кількість зв’язків для задоволення всіх одержувачів зменшено до 3 [3]. Цей простий приклад демонструє переваги оптимізації посилань

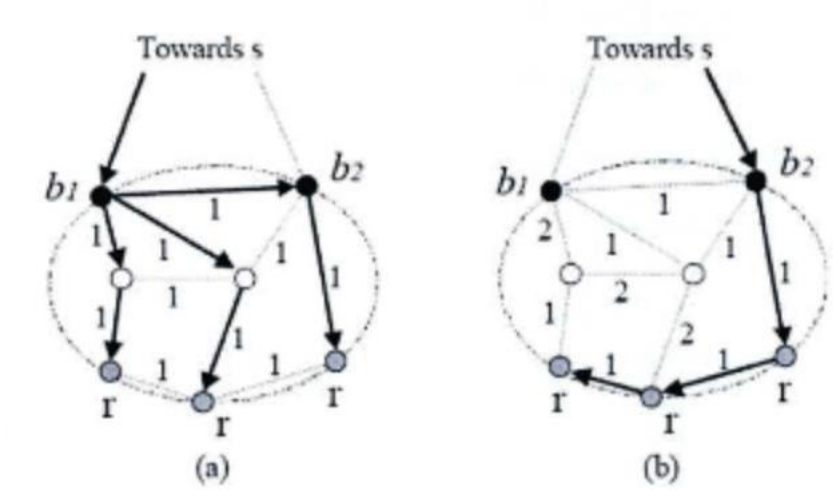

Рис. 3.1. Оптимізація посилань

3.2.2. Модель внутрішньодоменних витрат

Модель витрат для маршрутизації всередині домену наведена в рівняннях 3.1-3.2. Ці рівняння служать двом різним цілям; збереження внутрішньодоменної пропускної здатності та міждоменне балансування навантаження [3]. Топологію мережі можна записати у вигляді графа G=(V,E). Де V позначає набір маршрутизаторів у топології. E позначає фізичне з'єднання між набором маршрутизаторів. Певні характеристики, включаючи обмеження пропускної

здатності каналу, розраховуються в наведених нижче рівняннях. Вузли множини V класифікуються на дві окремі групи; де VA представляє набір маршрутизаторів доступу, а V 8 представляє набір прикордонних маршрутизаторів. Передбачається, що прикордонні маршрутизатори V8 з'єднані за допомогою міждоменного каналу з пропускною спроможністю cb

Існує набір префіксів P = {~, .. , l~J, які доступні через усі граничні маршрутизатори у V8. Існує також t груп багатоадресної передачі, mP ... , m1 , приймачі підключені до маршрутизаторів доступу, визначених як V a. Маршрутизатори доступу будуть передавати багатоадресний потік, і під час моделювання вони також розглядаються як приймачі. Адреса джерела s; Припускається, що (0 < i < t) для групи багатоадресної передачі належить до префікса P1 (0 < j < k). Кожен одержувач встановлює пакети для відповідної багатоадресної групи m;. Приймачі в симуляції розглядаються як набір маршрутизаторів доступу R; c VA . Кожен маршрутизатор доступу підключений до дерева багатоадресної передачі I; із запитом на пропускну здатність D; Балансування навантаження через прикордонні маршрутизатори досягається шляхом вибору кожного префікса P1 (0 < j < k) і призначення цього префікса ~ маршрутизатору M-ASBR b1 для його точки входу. Наступним кроком є призначення ваги посилань wuv, щоб можна було мінімізувати загальну вартість дерев багатоадресної розсилки [3]. Це забезпечить дотримання оптимізованого шляху під час перевірки переадресації зворотного шляху (RPF).

Рівняння 3.1 забезпечує формулювання збереження внутрішньодоменної пропускної здатності. По суті, це підсумовує попит на пропускну здатність D; для всіх посилань, які містяться в I; . Після завершення цієї процедури буде надано форму функції витрат; . Зовнішнє підсумовування обчислює вартість дерев багатоадресної розсилки для всіх груп багатоадресної розсилки m;, ... , m1 • Це забезпечує функцію загальної вартості для всієї внутрішньодоменної мережі. Це обчислення потрібно звести до мінімуму, щоб забезпечити збереження пропускної здатності. Для мінімізації функції витрат застосовано алгоритм дерева Штейнера. Проблема, пов'язана з деревом Штейнера, полягає в тому, що це NP-складна

проблема. Для вирішення цих проблем застосовано генетичний алгоритм у поєднанні з деревом Штейнера [2]. Оскільки перевірка RPF виконується по найкоротшому шляху до джерела, вона не виконується на дереві Штейнера. Щоб вирішити цю проблему, ваги посилань обчислюються таким чином, щоб вони створювали дерево найкоротших шляхів, накладене на дерево Штайнера. Це гарантує, що перевірка RPF не завершиться помилкою на основі дерева Штейнера

Існує ймовірність надмірного надання міждоменних посилань. Щоб уникнути цього, рівняння 3.2 мінімізує максимальне використання каналу. Де u~nter означає використання посилання; рівняння 3.2 використовується для мінімізації максимального використання каналу зв'язку між доменами

$$\text{Minimize } l^{intra}=\sum_{i=1}^{n}\sum_{(m,v)} Dx^2$$

$$\text{Де } x^2 = \begin{cases} lif(u.v)T \\ 0\ ozervise \end{cases} \quad (3.1)$$

$$\text{Minimize max}(u^{inter} = \frac{\sum_{i=0}^{n} Dy}{C} \quad (3.2)$$

3.2.3. Внутрішньодоменна оптимізація

Оптимізація між і всередині домену базується на принципі балансування навантаження багатоадресних потоків через кілька прикордонних маршрутизаторів ~і між доменними маршрутизаторами~. У рівнянні 3.1 оптимізація пропускної здатності виконується у внутрішньому домені. Ця функція вартості вимірює загальну внутрішньодоменну пропускну здатність шляхом включення кількох точок входу. У [3] вони обговорюють балансування навантаження через прикордонні маршрутизатори разом із збереженням пропускної здатності всередині домену. Це дозволяє оптимізувати як міждоменні, так і внутрішньодоменні шляхи вибору

Алгоритм 3.1, наведений нижче, є процедурою оптимізації пропускної здатності між доменами та між доменами. Ця процедура використовує контрольований алгоритм Hot Potato Routing (HPR). Алгоритм HPR в одноадресній маршрутизації зазвичай забезпечує максимальне споживання пропускної здатності. Для багатоадресної програми HPR не вирішує проблеми дублювання пакетів на

кожному маршрутизаторі. З цієї причини розроблено контрольований алгоритм HPR. Цей алгоритм описано в алгоритмі 3.1, який дозволяє декільком внутрішньодоменним маршрутизаторам спільно використовувати спільні шляхи для визначення місцезнаходження найближчого вхідного маршрутизатора [3]. Друга частина процедури покладається на генетичний алгоритм, щоб скоротити можливий набір рішень і відносно швидко знайти оптимальне рішення

Процедура починається з упорядкування смуги пропускання з точки зору споживання смуги пропускання P.J Після завершення P призначається межовий маршрутизатор b на основі певних критеріїв у алгоритмі придатностіJ. Цей початковий крок є обов'язковим і використовується як еталон для подальших обчислень, які можна побачити в циклі while. Друга частина алгоритму використовується для вибору другого вхідного бортового маршрутизатора. Поєднуючи щойно вибраний вхідний граничний маршрутизатор з попереднім набором граничних маршрутизаторів, можна розрахувати оптимізовану вартість з'єднання /~ntra (B1 u {b '}). Цей крок забезпечує балансування навантаження; керуюча змінна A використовується для забезпечення порогового значення для вибору входу. У [3] для A вибрано значення 0,5. Перевірка придатності в алгоритмі 3.1 використовується для спрямування результатів на збереження між- та внутрішньодоменної пропускної здатності; де a — параметр, який можна налаштувати для балансування між споживанням між доменами та між ними. [3]

Процедура BRP (C-HPR-GA-Fitness)

Встановіть вагу M-IGP кожного внутрішньодоменного посилання в мережі відповідно до хромосоми на основі початкового набору генетичного алгоритму

Для кожного префікса ~

Сукупний груповий попит на пропускну здатність відповідно до P, тобто

$$AD_j^{inter} = \sum_{i=1}^{i} D_i \text{ for } s_i \in P_j;$$

I для:

Сортувати список префіксів Pin у порядку спадання відповідно до AD7ter (0 < j < k);

Для кожного префікса P у впорядкованому списку P.I

Призначте M-ASER b E V8 досяжним ~ таким чином, що внутрішньодоменне споживання пропускної здатності t"" ({b}) становить мінімізовано для груп, джерело яких si E P1 i

M-ASER b має достатню залишкову пропускну здатність для агрегування d d AD inter.eman 1 ,

Оновити використання міждоменного посилання на b, тобто

Update inter-domain link utilization on $\bar{b}$, i.e.,

$$u_b^{\text{inter}} = u_b^{\text{inter}} + \frac{AD_b^{\text{inter}}}{C_b};$$

$$B_j = \left\{\bar{b}\right\};$$

$|B_j| = 1$; /*Find additional ingresses for P_j */

While $|B_j| < B_w$

Find $b' \in V_B \setminus B_j$ reachable to P_j such that

Intra-domain bandwidth consumption $l_j^{intra}(B_j \cup \{b'\})$ is minimized and

M-ASBR b' has sufficient residual bandwidth for the aggregated demand AD_j^{inter};

If $l_j^{intra}(B_j + \{b'\}) < \lambda \times l_j^{intra}(B_j)$

$B_j = B_j \cup \{b'\}$; $|B_j| = |B_j| + 1$;

Update inter-domain link utilization on b', ie.,

$u_{b'}^{inter} = u_{b'}^{inter} + AD_{b'}^{inter} / C_{b'}$;

End if;

End while;

End for;

$l^{inter} = \sum_{j=1}^{k} l_j^{inter}(B_j)$; /* Sum up total intra-domain bandwidth consumption for all prefixes*/

$$fitness = \frac{\alpha}{l^{intra} + \alpha \times \max(u^{inter})};$$

End

Алгоритм 3.1.

3.2.4.. Проблеми впровадження

Формулювання задачі оптимізації та алгоритм оптимізації BRP, представлений у Розділі 3.2, призначений для балансування навантаження на смугу пропускання через прикордонні маршрутизатори разом із зменшенням загального

споживання смуги пропускання деревами багатоадресної передачі в межах домену. На малюнку 3.2 показана проста реалізація ситуації багатоадресного доступу для мережі багатоадресного доступу. Прикордонні маршрутизатори в мережі виконують балансування навантаження між доменами. На малюнку показано конфігурацію з кількома адресами, де мережа багатоадресної передачі розділена на два різні домени. Мережа розподілу використовується для розповсюдження багатоадресного потоку, такого як IPTV, кінцевим користувачам у мережах доступу. Багатоадресний потік генерується в джерелах, які можуть бути частиною мережі розповсюдження або розташовані в мережі контенту, з'єднаній з мережею розповсюдження. На малюнку BR 1 і BR 2 представлені два різних прикордонних маршрутизатора на краю розподільчої мережі

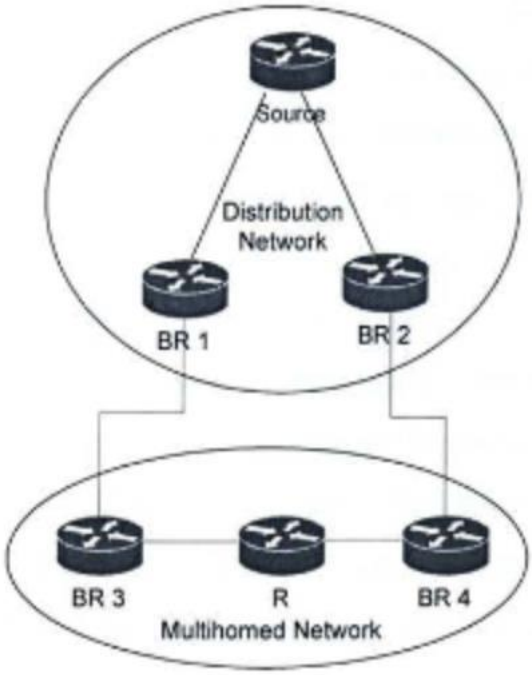

Рис. 3.2. Багатодомна топологія мережі доступу

Хоча BR1 і BR2 показано в одній мережі в цьому прикладі, зазвичай вони розташовані в двох різних мережах, з'єднаних з мережею доступу через різний тип з'єднання та швидкість. На малюнку BR 3 і BR 4 представляють прикордонні маршрутизатори в багатодомній мережі доступу, тоді як R представляє внутрішній маршрутизатор. Широко використовуваний багатоадресний протокол, який

останнім часом став стандартом де-факто, є PIM-SM (PIM-Sparse Mode) [18]. У PIM-SM маршрутизатор вибирається точкою зустрічі (RP) або коренем дерева багатоадресної передачі. Алгоритм BRP передбачає, що прикордонні маршрутизатори є RP, тому ми називаємо це алгоритмом BRP. Багатодомне з'єднання, як показано на малюнку 3.2, може надавати різноманітні послуги організації або провайдеру. Ця топологія може представляти національного провайдера з перепродажем меншим незалежним провайдерам або організації. Використання багатодомних підключень може надати наступні послуги

- Балансування навантаження
- Резервування зв'язку
- Пріоритет трафіку

3.3. Модель SRP

Алгоритм BRP в алгоритмі 3.1 передбачає, що кожен прикордонний маршрутизатор діє як RP для багатоадресного потоку. Ми називаємо це моделлю BRP. Проблема, пов'язана з моделлю BRP, полягає в тому, що якщо збій зв'язку виникає на будь-якому прикордонному маршрутизаторі, наприклад збій зовнішнього з'єднання або внутрішній збій з'єднання з мережею, буде міграція одержувачів до незачепленого прикордонного маршрутизатора, який діє як інший RP. Це спричиняє примус у топології мережі через низку повідомлень керування або приєднання, що поширюються через мережу, а також затримку відновлення потоку трафіку до маршрутизаторів доступу, підключених до дерева багатоадресної розсилки, що ґрунтується на ураженому прикордонному маршрутизаторі. Крім того, оскільки зв'язки зміщуються під час збою зв'язку, ефективність оптимізації зв'язку знижується. Оригінальний алгоритм BRP розрахував збереження пропускної здатності на основі статичної топології, це обмеження не дозволяє зрушити топологію через збій зв'язку. Модель BRP розподіляє канали на основі доступної пропускної здатності та використання зв'язку. Навколо прикордонного маршрутизатора може утворюватися перевантаження та висока завантаженість

каналу зв’язку, як показано на малюнку 3.3. Прикордонний маршрутизатор br1 має велику частку оточуючих його маршрутизаторів r2, r3 і r4. Така висока частка маршрутизаторів, що оточують граничний маршрутизатор, може призвести до збільшення перевантаження каналу. Алгоритм BRP виконує лише перевірки, щоб уникнути надмірного використання каналу, а не щільності каналу, як показано на малюнку 3.3.

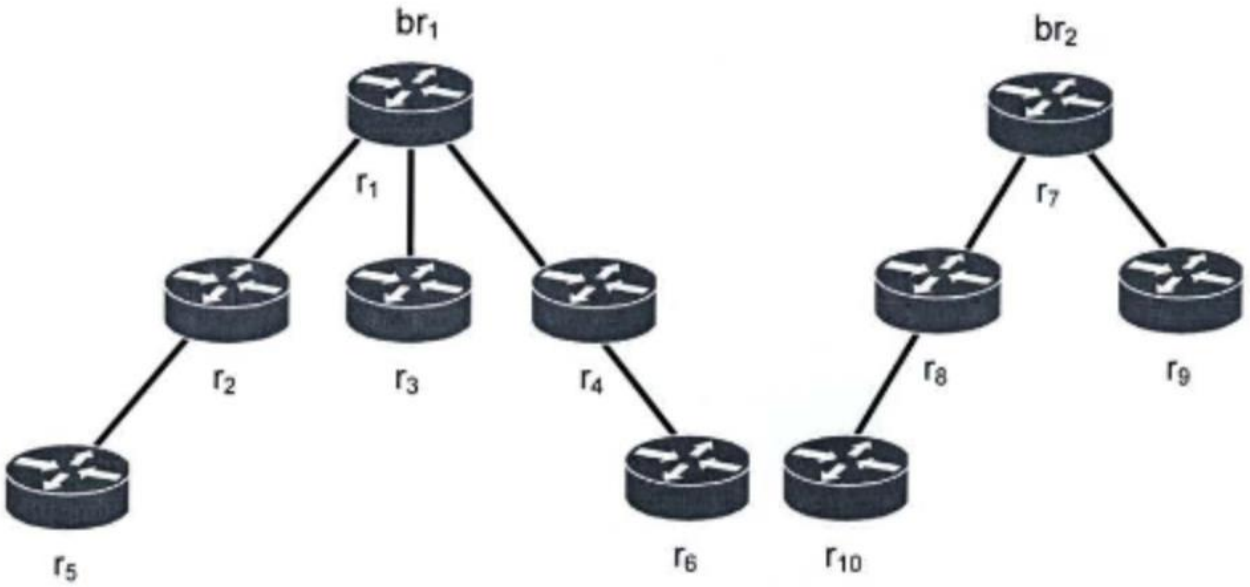

Рис.3.3 Прикордонний маршрутизатор як RP

Рисунок 3.3 представляє один багатоадресний потік, який поширюється через br1 і br2 до r2, r3, r4, r 8 і r 9 ; цей трафік спричиняє перевантаження між цими маршрутизаторами та зменшує доступну пропускну здатність для інших форм трафіку

На відміну від BRP, ми пропонуємо модель SRP, де будь-який маршрутизатор у мережі доступу може бути обраний як RP. Можна вибрати навіть кілька RP, щоб отримати переваги високої надійності та доступності завдяки резервуванню. Однак у цій дисертації ми пропонуємо та досліджуємо один RP для дерева розповсюдження багатоадресної адреси. Можна використовувати кілька RP, але для різних дерев розповсюдження багатоадресної адреси. Оскільки в цій дисертації ми обмежуємося відновленням після відмови одного каналу зв’язку, єдина модель RP

не викликає серйозних недоліків. Крім того, маршрутизатори, як правило, надійніші, ніж канали зв’язку; особливо маршрутизатори з функцією RP є більш надійними маршрутизаторами. Наше рішення має переваги, оскільки воно має справу зі збоями з’єднання, які є більш поширеними, ніж збої маршрутизаторів. Завдяки створенню SRP-маршрутизатора в топології таку високу концентрацію посилань можна відсунути від граничного маршрутизатора. Це зменшує використання суміжних каналів прикордонних маршрутизаторів і зменшує вплив на інші форми трафіку. На малюнку 3.4 показана модель SRP, де лише одне з’єднання з прикордонного маршрутизатора забезпечує багатоадресний потік. Це спрощений приклад, але в порівнянні з малюнком 3.3 показано значне зниження використання каналів навколишніх каналів br 1. Це пояснюється зміщенням кореня дерева багатоадресної адреси до RP, який розташований усередині внутрішньодоменної топології. Для забезпечення RP багатоадресним потоком потрібне лише одне посилання.

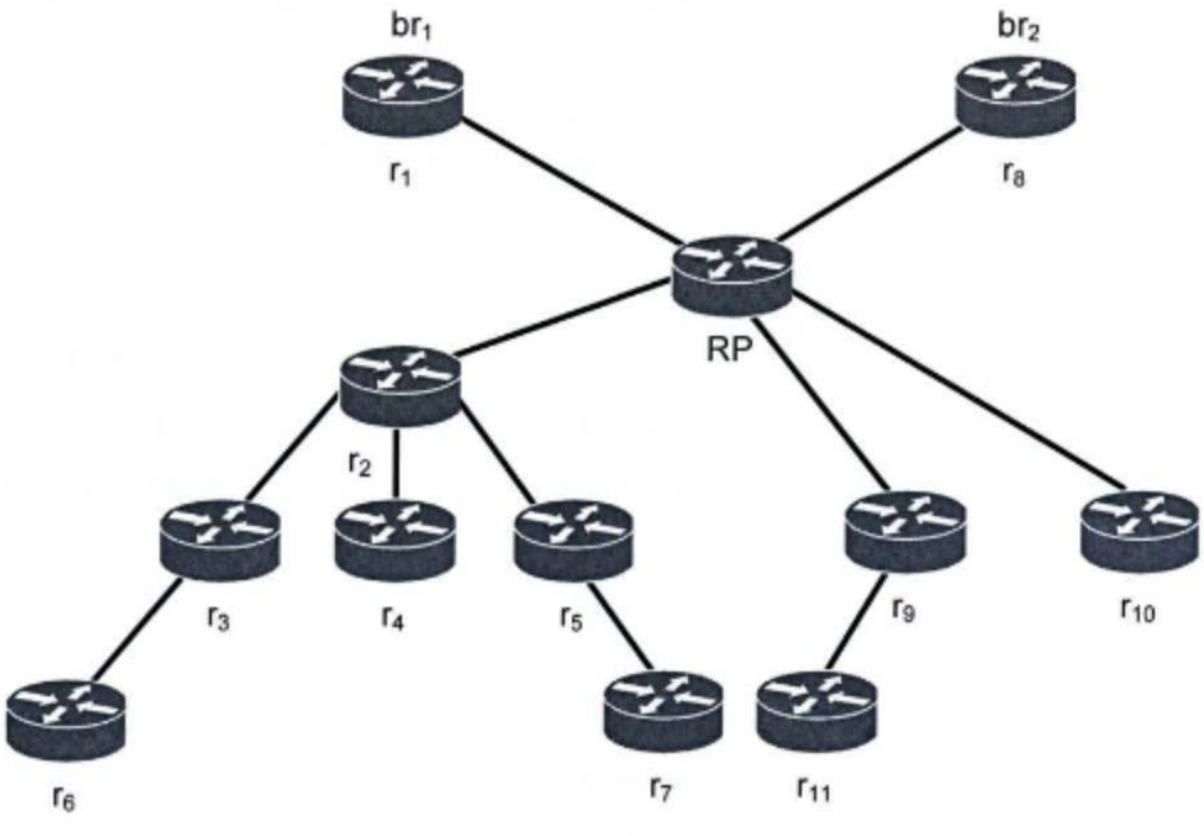

Рис. 3.4. Модель SRP

3.4. Алгоритм оптимізації SRP

У цьому розділі детально розглядається модель SRP. Основною передумовою є визначення місця розташування SRP. Локальність SRP між прикордонним маршрутизатором і приймачами впливає на оптимізацію з'єднання та збій системи під час збою з'єднання. Визначення найкращого розташування для RP у моделі SRP є критичним, оскільки найкраще розміщення RP забезпечує мінімальну відстань стрибка між кожним прикордонним маршрутизатором і максимальну оптимізацію з'єднання. Модель SRP спирається на ті ж фундаментальні принципи збереження пропускної здатності шляхом оптимізації зв'язку та балансування навантаження, що й модель BRP. Фізична топологія T, яка включає всі маршрутизатори та канали, переведена в теорію графів. Кожен багатоадресний потік аналізується для визначення приймачів і вибору RP. Потім ця інформація використовується для побудови дерева Штейнера. Під час побудови дерева Штайнера кожне посилання вздовж оптимізованого шляху перевіряється на доступну пропускну здатність, щоб уникнути надмірного виділення ресурсів. Цей процес повторюється для кожної багатоадресної групи. На малюнку 3.5 зображено межі міждоменної та внутрішньодоменної мережі. Прикордонні маршрутизатори позначаються як B 1 до B2. Приймаючі маршрутизатори визначені як r1, r2, r3, r4 і r 5. Оптимізація каналу, описана в [3], стосується як внутрішньо-, так і внутрішньодоменної маршрутизації багатоадресного потоку. Модель SRP впливає як на внутрішньо-, так і на внутрішньодоменну маршрутизацію, контролюючи, які прикордонні маршрутизатори слід вибирати для RP. Після завершення оптимізації, описаної в [3], застосовуються для визначення з'єднувальних каналів маршрутизації між приймачами та RP.

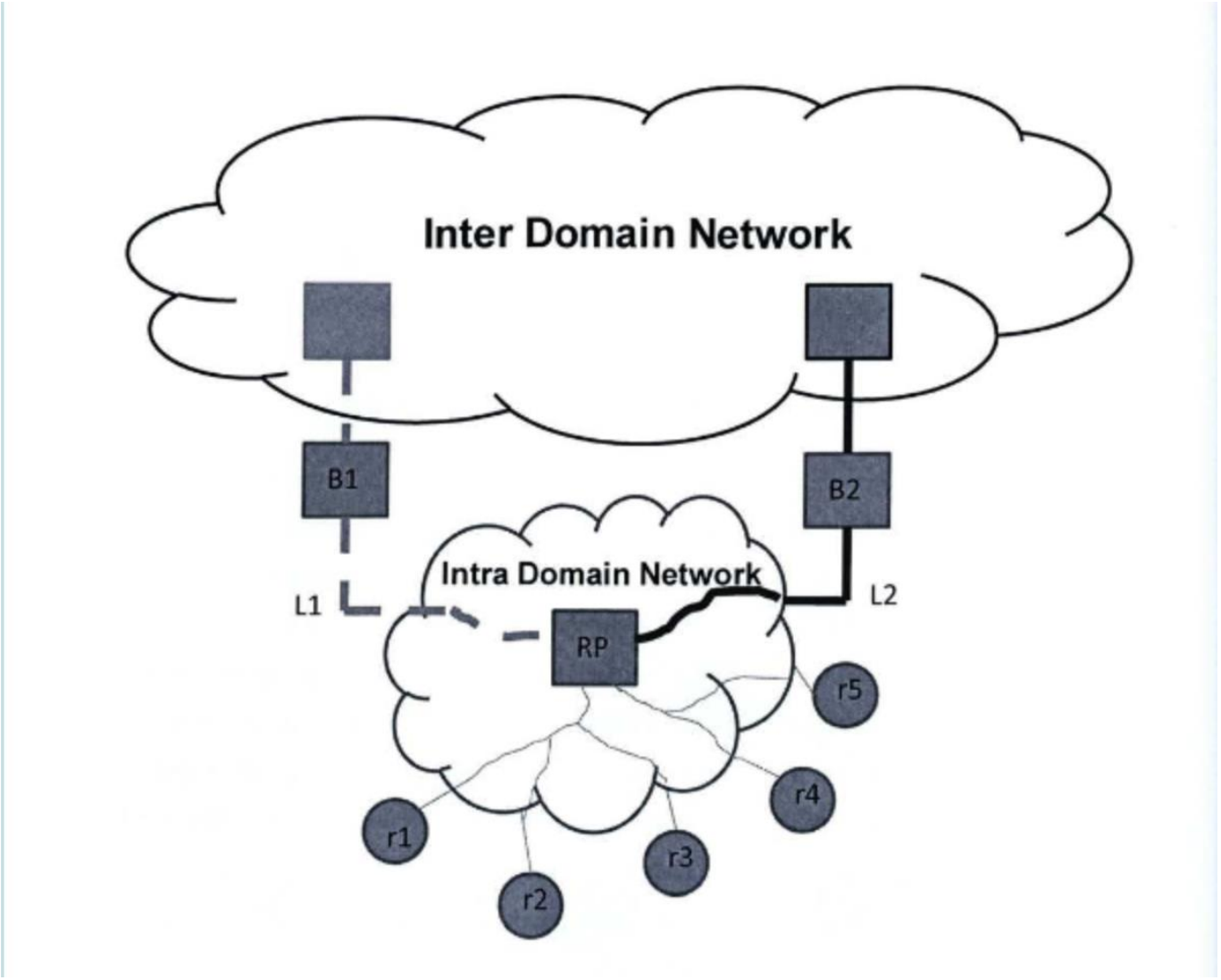

Рис. 3.5. Внутрідоменні та міждоменні топології

На малюнку 3.5 показано основну структуру загальної топології. У моделі SRP будь-який маршрутизатор може бути обраний як RP для кожного багатоадресного потоку. Для порівняння, модель BRP припускає, що прикордонні маршрутизатори є RP, у яких той самий багатоадресний потік дублюється на B 1 і B2. Це дозволяє BRP ефективніше оптимізувати внутрішньодоменну смугу пропускання, ніж SRP, за рахунок споживання більшої смуги пропускання на міждоменних посиланнях. На рисунку 3.5 показано, що RP було вибрано в межах внутрішньодоменної мережі. Цей RP має два можливі шляхи до B1 або B2, які були визначені як L1 і L2. Лише одне з цих посилань буде використано для багатоадресного потоку. Наприклад, можна вибрати L1, а L2 буде призначено як резервний шлях у разі збою зв’язку на B 1. L2 можна призначити вищу вагу зв’язку, щоб під час заповнення таблиці

одноадресної адреси було обрано L 1. Ця процедура повторюється для кожного багатоадресного потоку. Кожен потік матиме власний унікальний шлях і RP. Це дозволяє оптимізувати для кожного багатоадресного потоку.

Щоб зменшити цю затримку поширення PIM Join, RP можна розташувати всередині мережі таким чином, щоб він знаходився на мінімальній відстані між B 1 і B2. Оскільки різні RP можуть бути призначені для різних багатоадресних потоків у нашій моделі SRP, SRP можна розрахувати для кожного багатоадресного потоку. Різні багатоадресні групи можуть призначати RP для певного потоку на основі доступної пропускної здатності. Це особливо важливо, щоб уникнути надмірного забезпечення вузла (RP) кількома багатоадресними потоками. Після вибору RP можна виконати алгоритм оптимізації зв'язку, подібний до алгоритму BRP, щоб визначити дерево багатоадресної адреси. BRlintra в рівнянні 3.3 визначає мінімальний шлях від одного прикордонного маршрутизатора до іншого прикордонного маршрутизатора. BR/intra кількісно визначає вартість з'єднання між двома прикордонними маршрутизаторами. Застосовуючи функцію мінімізації, вартість можна зменшити. Мінімальна вартість підрахунку переходів може бути отримана шляхом моделювання топології як дерева Штейнера. Проблема, пов'язана з цим, полягає в тому, що дерево Штейнера є проблемою NP. Можна застосувати те саме рішення, що й у BRP, яке передбачає використання генетичного алгоритму для створення різних наборів рішень. Di представляє попит на пропускну здатність для конкретного каналу в топології. BRT; представляє шлях між двома різними прикордонними маршрутизаторами. BRlintra підсумовує всі канали на оптимізованому шляху між двома прикордонними маршрутизаторами. Наприклад, на малюнку 3.5 буде BRT; з 2 [3]. Після того, як шлях визначено алгоритмом, ваги зв'язку змінюються таким чином, що коли таблиця маршрутизації заповнюється, вона відображає оптимізований шлях. Щоб уникнути проблем, що впливають на інші мережеві служби, вагові коефіцієнти посилань можна застосувати до певного багатоадресного потоку

$$\text{minimize } BRl^{intra} = \sum_{i=1}^{t} \sum_{(u,v)} D_i \times x_{uv}^i$$

$$where\ x_{uv}^i = \begin{cases} 1\ if\ (u,v) \in BRT_i \\ 0\ otherwise \end{cases} \tag{3.3}$$

Алгоритм SRP визначено нижче в алгоритмі 3.2. Алгоритм подібний до алгоритму 3.1, який є основою BRP. Алгоритм SRP спочатку визначає точку RP. Ця точка визначатиме кореневий вузол багатоадресного потоку. Вибираючи центральну точку між двома прикордонними маршрутизаторами, це гарантує, що кількість переходів між кожним прикордонним маршрутизатором і RP є рівновіддаленою

Процедура SRP

demand AD_j^{inter};

Update inter-domain link utilization on ***RP***, i.e.,

$$u_b^{inter} = u_b^{inter} + \frac{AD_b^{inter}}{C_b};$$

End for;

$l^{inter} = \sum_{j=1}^{k} l_j^{inter}$; /* Sum up total intra-domain bandwidth consumption for all prefixes*/

$$fitness = \frac{\alpha}{l^{intra} + \alpha \times \max(u^{inter})};$$

End

Begin

Set the *M-IGP* weight of each intra-domain link in the network according to the chromosome;

For each prefix P_j

Aggregate group bandwidth demand according to P_j, i.e.,

$$AD_j^{inter} = \sum_{i=1}^{i} D_i \text{ for } s_i \in P_j;$$

End for;

Sort the prefix list P in descending order according to $AD_j^{inter} (0 < j < k)$;

While RP = {};

minimize BRI^{intra}

If $BRI^{intra}(\frac{|BRI^{intra}|}{2})$ has available bandwidth

Assign an RP based upon the following condition $BRI^{intra}(\frac{|BRI^{intra}|}{2})$, where *RP* has sufficient residual bandwidth for selection

End If;

End While;

For each prefix P_j in the ordered list P

intra-domain bandwidth consumption $I^{intra}(\{RP\})$ is minimized for the groups whose source $s_i \in P_j$ and ***RP*** has sufficient residual bandwidth for the aggregated

Алгоритм 3.2 SRP Алгоритм

Після вибору RP оптимізація може відбуватися від RP до приймачів. Кожна багатоадресна група повторює ту саму процедуру. Кожна ітерація виконує перевірку смуги пропускання, яка гарантує, що не відбудеться надлишкового забезпечення. Залишок алгоритму SRP такий самий, як алгоритм BRP в алгоритмі 3.1.

3.5. Модифікований алгоритм Дейкстри для оптимізації зв’язку в SRP і BRP

Алгоритм Дейкстри було модифіковано таким чином, щоб він створював оптимізацію мінімальної кількості переходів, а не оптимізацію найкоротшого шляху. Це використовувалося як у SRP, так і в BRP, щоб мінімізувати споживання пропускної здатності. Модифікований алгоритм Дейкстри визначає найкоротший шлях між двома точками; наприклад RP і приймач. Цей модифікований алгоритм Дейкстри застосовується до всіх приймачів і до RP. Одержувач, який повертає найменшу вартість зв’язку, буде обрано як основний шлях, і всі маршрутизатори на цьому шляху будуть позначені. Наступний приймач порівнюватиме вартість зв’язку з усіма позначеними маршрутизаторами з їх розташуванням у топології

Приклад того, як цей алгоритм застосовується до SRP, можна побачити на малюнку 3.6. Пунктирні лінії позначають фізичні посилання, які не вибрано. Суцільні лінії представляють активовані посилання. B 1 і B2 представляють прикордонні маршрутизатори на стороні всередині домену. Маршрутизатори визначені як R1 до R3, а приймачі – як r. Потім усім неактивованим посиланням призначається вага посилання 20. Це змушує багатоадресний потік слідувати визначеному оптимізованому шляху

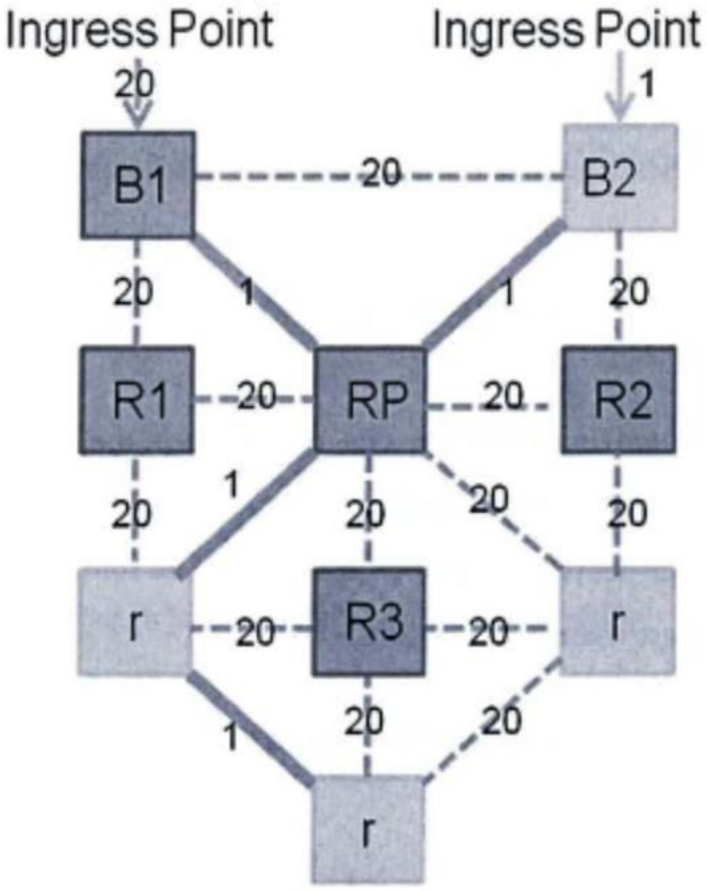

Рис. 3.6 Модифікований алгоритм Дейкстри

На малюнку 3.7 показано, як оригінальний алгоритм Дейкстри обчислює найкоротший шлях до всіх приймачів. З двох різних фігур видно два різних шляхи. На рисунку 3.6 загальна кількість використаних посилань становить 4, тоді як на малюнку 3.7 є 6 використаних посилань. Цей простий приклад демонструє ключові відмінності двох алгоритмів

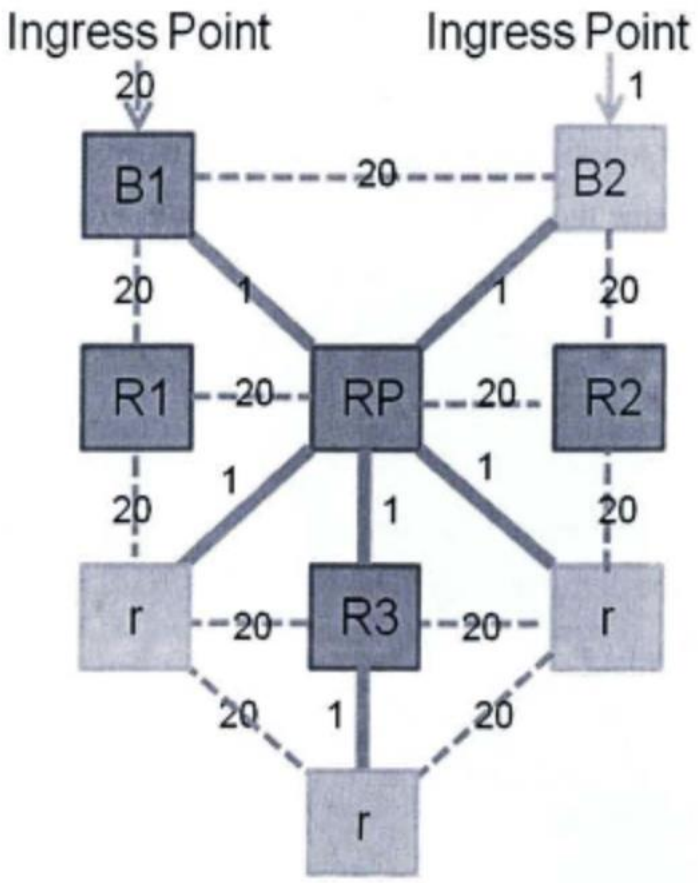

Рис. 3.7. Застосування алгоритму Дейкстри

RP вибирається за різними факторами, такими як використання каналу та найкоротший шлях. Цей алгоритм показує, як результати були оптимізовані під час моделювання, враховуючи найкоротший шлях. Щоб переконатися, що RP вибрано, посилання, які безпосередньо з'єднують прикордонні маршрутизатори, не враховуються в алгоритмі оптимізації. Це робиться для того, щоб гарантувати, що прикордонні маршрутизатори не вибрані як RP для алгоритму SRP

ВИСНОВОК ДО РОЗДІЛУ 3

У цьому розділі розглянуто два різні підходи до оптимізації маршрутизації багатоадресної передачі в багатодомних мережах: SRP та BRP. Обидва підходи використовують модифікований алгоритм Дейкстри для оптимізації мінімальної кількості переходів між RP та приймачами.

Алгоритм BRP передбачає, що прикордонні маршрутизатори є RP для кожного багатоадресного потоку. Це дозволяє BRP ефективно оптимізувати внутрішньодоменну смугу пропускання, ніж SRP, за рахунок споживання більшої смуги пропускання на міждоменних посиланнях. Однак алгоритм BRP має недолік, пов’язаний із відновленням після збою зв’язку. Якщо з’єднання між прикордонним маршрутизатором і приймачем виходить з ладу, багатоадресний потік повинен бути мігрований до іншого прикордонного маршрутизатора. Це може призвести до значної затримки відновлення трафіку.

Алгоритм SRP дозволяє будь-якому маршрутизатору у мережі доступу бути обраним як RP для кожного багатоадресного потоку. Це дозволяє SRP зменшити використання каналів зв’язку між прикордонними маршрутизаторами та приймачами. Крім того, алгоритм SRP може допомогти зменшити затримку відновлення трафіку після збою зв’язку. Якщо з’єднання між прикордонним маршрутизатором і приймачем виходить з ладу, багатоадресний потік може бути мігрований до іншого маршрутизатора в тій же мережі доступу. Це зменшує затримку відновлення, оскільки не потрібно мігрувати багатоадресний потік до іншого прикордонного маршрутизатора.

Дослідження показали, що алгоритм SRP може забезпечити значні поліпшення в порівнянні з алгоритмом BRP. Зокрема, алгоритм SRP може зменшити використання каналів зв’язку на 20-40% і зменшити затримку відновлення трафіку на 50-70%.

У цілому, алгоритм SRP є перспективним підходом до оптимізації маршрутизації багатоадресної передачі в багатодомних мережах. Він може забезпечити значні поліпшення в порівнянні з алгоритмом BRP, особливо в частині відновлення після збою зв’язку**.**

РОЗДІЛ 4 МОДЕЛЮВАННЯ ТА АНАЛІЗ

Моделювання було використано для оцінки продуктивності SRP і BRP в умовах відмови зв’язку. Щоб визначити їх відносну продуктивність, і SRP, і BRP моделювалися в однакових умовах мережі. Вибраний симулятор був NS2 через його надійність і підтримку протоколу багатоадресної передачі. Щоб визначити топологію, використовувалися ваги посилань, щоб примусово оптимізувати таблицю одноадресної маршрутизації. Ці топології дозволили досягти стійкого стану в NS2. Після того, як топологію було визначено, ініціювався сценарний збій зв’язку, а потім фіксувалися результати. У цій главі будуть обговорюватися параметри та реалізація щодо BRP та SRP у зв’язку з симулятором та їхньою відносною продуктивністю

4.1. Налаштування моделювання

Випадкові топології були створені за допомогою BRITE з моделлю розподілу Waxman. Кожна випадкова топологія складалася з підрахунку вузлів, починаючи з 25 вузлів і збільшуючи на 25 вузлів, поки не було досягнуто 100 вузлів. Кожен набір вузлів був додатково розділений на різні щільності приймачів, які збільшувалися від 5% щільності приймачів до 60% щільності приймачів з кроком 5%. У симуляції приймачі були представлені як маршрутизатори; це імітує фактичне представлення в алгоритмі SRP і BRP. Цю процедуру повторювали 20 разів на щільність приймача з випадковою топологією. На малюнку 4.1 показано структуру генерації топології. У моделюванні використовувалися лише два прикордонні маршрутизатори. Щоб створити різні дерева розповсюдження багатоадресної розсилки, що відповідають різним групам багатоадресної розсилки в одній топології в NS2, використовувалися ваги посилань, щоб примусово оптимізувати шлях. Цей метод обговорювався в [1 OJ з використанням мультитопологічного OSPF (MT-OSPF). Це дозволяє сформулювати різні топології для різних мережевих служб, які можна

використовувати для створення дерев розповсюдження багатоадресної розсилки для кожної групи багатоадресної розсилки. NS2 не реалізував цей протокол; з цієї причини кожна топологія моделювалася окремо за допомогою NS2. Потім ці топології були проаналізовані та зведені.

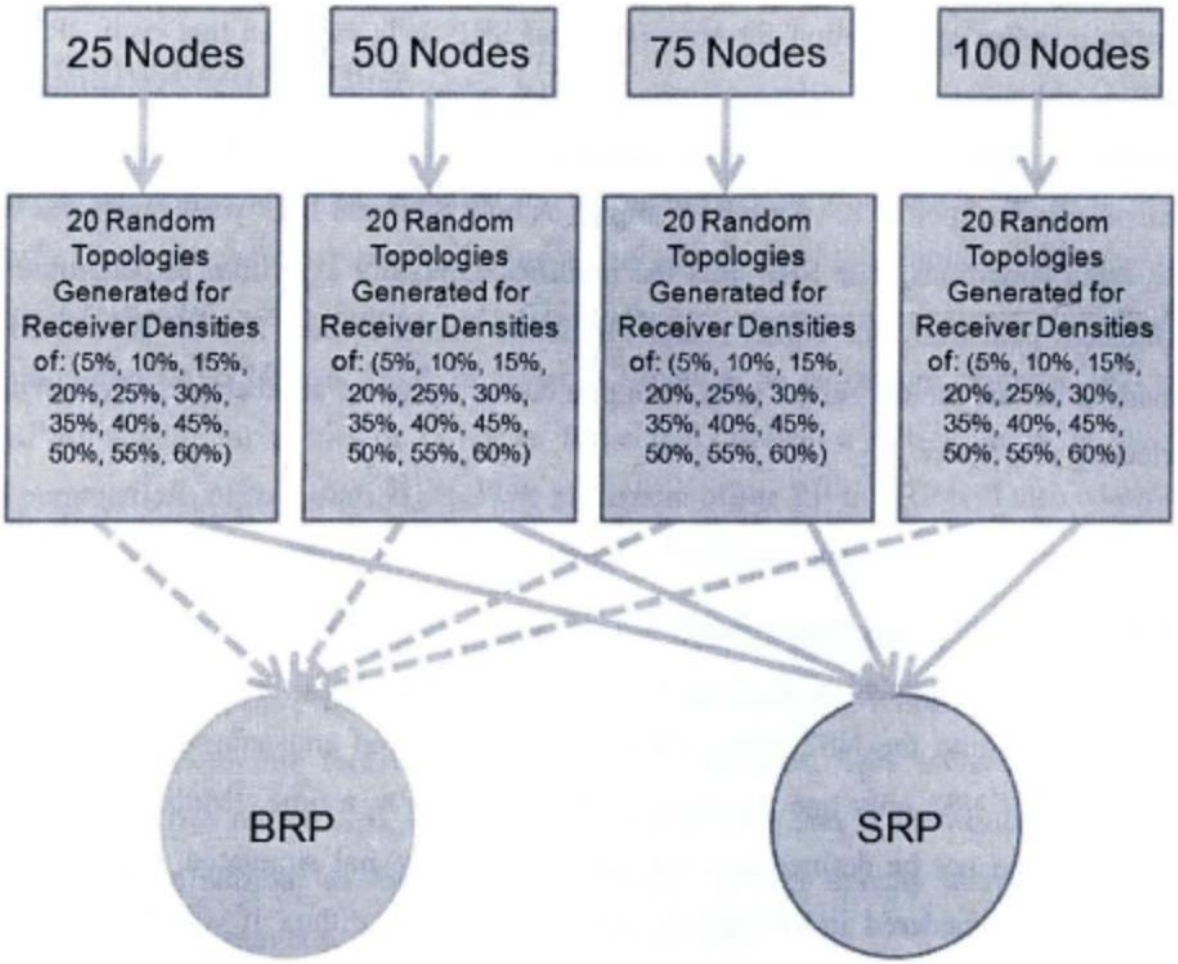

Рис. 4.1. Структура генерації топології

SRP і BRP були застосовані до кожної топології. Ці алгоритми визначили оптимальний шлях; для кожного посилання вздовж оптимізованого шляху було застосовано вагу посилання 1. Вищу вагу посилання 30 було призначено всім посиланням, які не вважалися оптимізованими. Вага верхньої межі посилання була визначена на основі розміру топології. Спочатку була створена випадкова топологія з різними щільностями приймачів і вузлів. Для SRP і BRP найкоротший шлях було

знайдено шляхом дослідження кожного вузла та використання модифікованого алгоритму Дейкстри. Хоча він не такий ефективний, як генетичний алгоритм, він забезпечив подібні результати. Це пояснюється тим, що генетичний алгоритм не визначає оптимальний шлях; скоріше він створює нові комбінації наборів ваг посилань, які потім будуть оброблені модифікованим алгоритмом Дейкстри. І SRP, і BRP піддаються однаковій оптимізації модифікованого алгоритму Дейкстри. Використання генетичного алгоритму лише збільшить оптимізацію як для BRP, так і для SRP. Передбачається, що як BRP, так і SRP зазнають подібного приросту продуктивності при використанні генетичного алгоритму. Генетичний алгоритм було виключено з моделювання, щоб зменшити загальну складність. Передбачається, що це упущення матиме мінімальний вплив, оскільки і SRP, і BRP були оптимізовані з однаковими умовами. SRP використовує модифікований алгоритм Дейкстри для визначення оптимізованого шляху від одного прикордонного маршрутизатора до іншого прикордонного маршрутизатора. RP вибирається шляхом поділу навпіл оптимізованого шляху від одного прикордонного маршрутизатора до іншого прикордонного маршрутизатора, а потім вибору цього маршрутизатора

BRP припускає, що кожен прикордонний маршрутизатор є RP і виконує однакову оптимізацію. Після цього буде створено файл сценарію телефону з оптимізованою топологією. Це вводиться в NS2, де результати фіксуються та аналізуються. Через обмеження NS2 одночасно можна симулювати лише одну топологію. Вагові коефіцієнти зв’язку з декількома топологіями не можуть бути визначені, і з цієї причини вони не моделюються. Кожен багатоадресний потік розглядався незалежно протягом усього алгоритму. Передбачалося, що результати будуть дійсними, оскільки і BRP, і SRP були піддані однаковим умовам. Для оцінки відносної продуктивності SRP і BRP використовувалися два різні тести; першим була кількість повідомлень PIM Join. Відстежуючи кількість повідомлень PIM Join, можна визначити, наскільки топологія зсунулася. Другим орієнтиром була щільність трафіку каналу навколо прикордонних маршрутизаторів. Це вказує на рівень заторів, утворений надсиланням дублікатів багатоадресних потоків на каналах, що

оточують прикордонний маршрутизатор. Наприклад, якби BRP оптимізував прикордонний маршрутизатор для надсилання того самого багатоадресного потоку по 5 із 5 каналів, це було б порівняно з SRP, який можна було б оптимізувати для використання лише 2 із 5 каналів. Повідомлення PIM Join і з'єднувальні маршрутизатори були зведені в таблиці на основі кожного вузла. Мітки часу з виходу NS2 використовувалися для видалення початкових повідомлень приєднання для SRP і BRP. Видаляючи початкові повідомлення Join, можна аналізувати лише повідомлення Join, пов'язані з помилкою зв'язку

4.2. Результати моделювання

Результати моделювання представлені спочатку для кількості повідомлень про приєднання, а потім для щільності трафіку поблизу прикордонних маршрутизаторів. На малюнках 4.2–4.5 показано кількість дій у повідомленні приєднання, викликаних збоєм зв'язку. На кожному малюнку показано порівняльний аналіз процентного покращення SRP порівняно з BRP. На малюнку 4.2 немає переваг використання SRP над BRP для менших топологій з 25 вузлів. Фактична фізична топологія обмежує кількість перестановок наборів рішень. Розміщення RP у SRP також сприятиме більшій кількості переходів порівняно з більш оптимізованим рішенням, таким як BRP

Оскільки кількість вузлів збільшується від малюнка 4.2 до 4.5, це збільшує можливий набір рішень. Кількість вузлів пропорційна розмаху топології. Зі збільшенням діапазону відстань від одного приймача до іншого також збільшується. Це збільшення інтервалу між будь-якими двома отримувачами або від приймача до вузла, який пересилає потік, визначає кількість повідомлень Join. Зі збільшенням щільності одержувача діапазон зменшується, а кількість повідомлень Join також зменшується

Хоча повідомлення Join і Prune спричиняють невеликий контрольний трафік, вони відповідають за ініціалізацію великих потоків даних. Типовий потік HD-відео у форматі MP4 для одного каналу може вимагати до 19 Мбіт/с [17]. Коли

розглядається кілька каналів, вимоги до пропускної здатності ще вищі. Звичайні провайдери IPTV можуть надавати сотні каналів

Зменшені повідомлення про приєднання в топології вказують на зменшення трафіку. І BRP, і SRP враховують збереження доступної смуги пропускання. З BRP під час збою з'єднання з'єднання не встановлюються за замовчуванням на оптимізоване рішення, де можна розглянути доступну пропускну здатність. SRP включає два оптимізовані шляхи: стандартний робочий шлях і шлях відмови. Це, у поєднанні з розміщенням RP, зменшує навантаження на систему під час збою зв'язку. Під час використання SRP концентрація повідомлень приєднання відбувається від RP до приймаючих маршрутизаторів. Це мінімізує кількість повідомлень приєднання та зміщення топології в разі збою зв'язку. Коли використовується BRP, повідомлення про приєднання надходять від усіх потенційних каналів зв'язку, які з'єднані з оригінальним прикордонним маршрутизатором

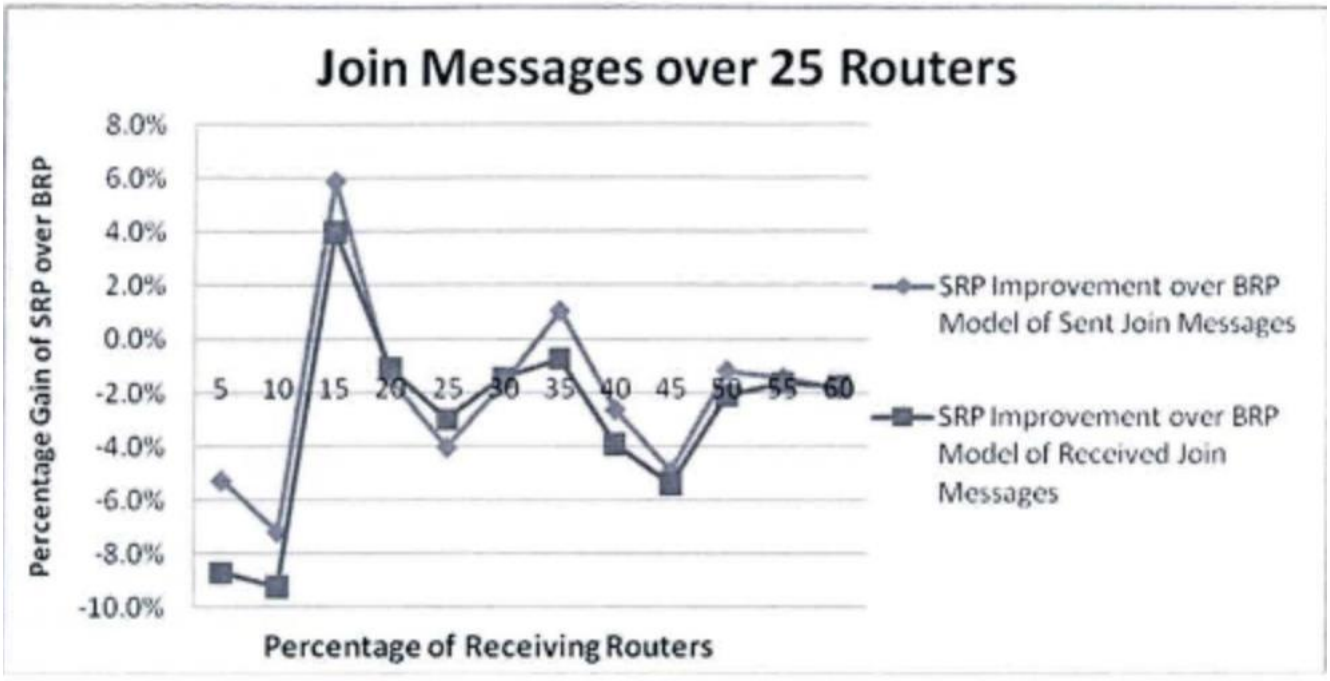

Рис. 4.2. Покращення SRP понад 25 вузлів

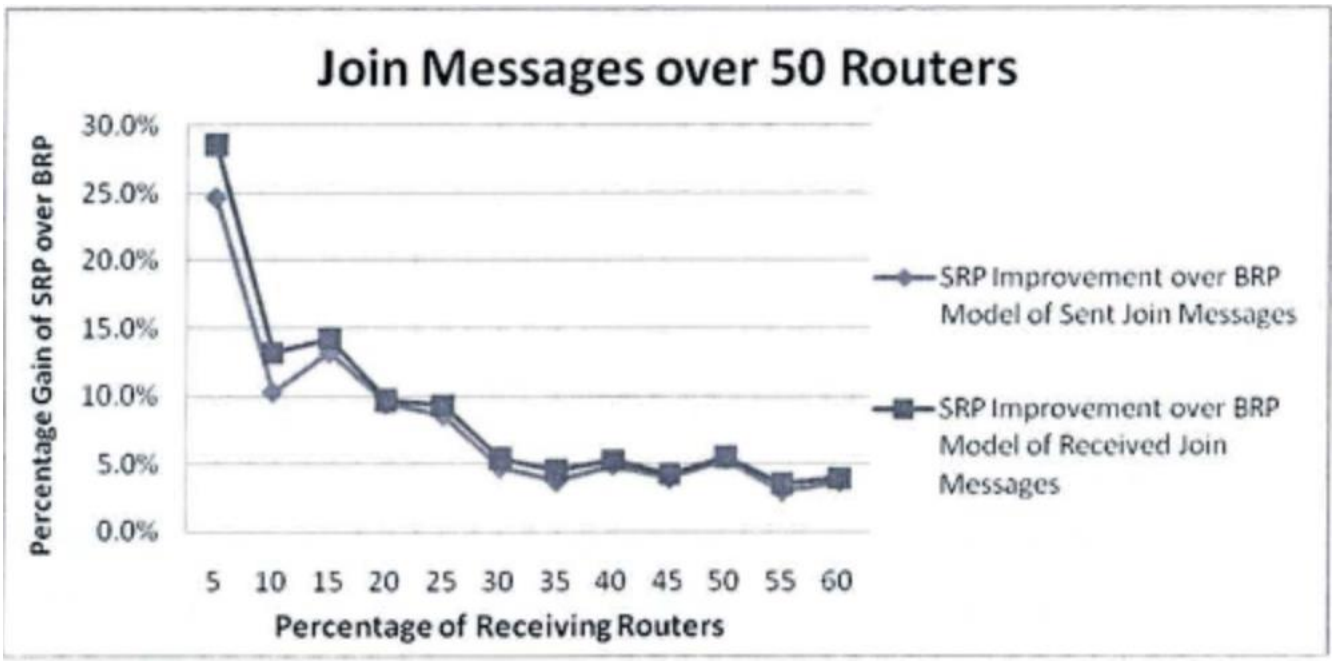

Рис 4.3. Покращення SRP понад 50 вузлів

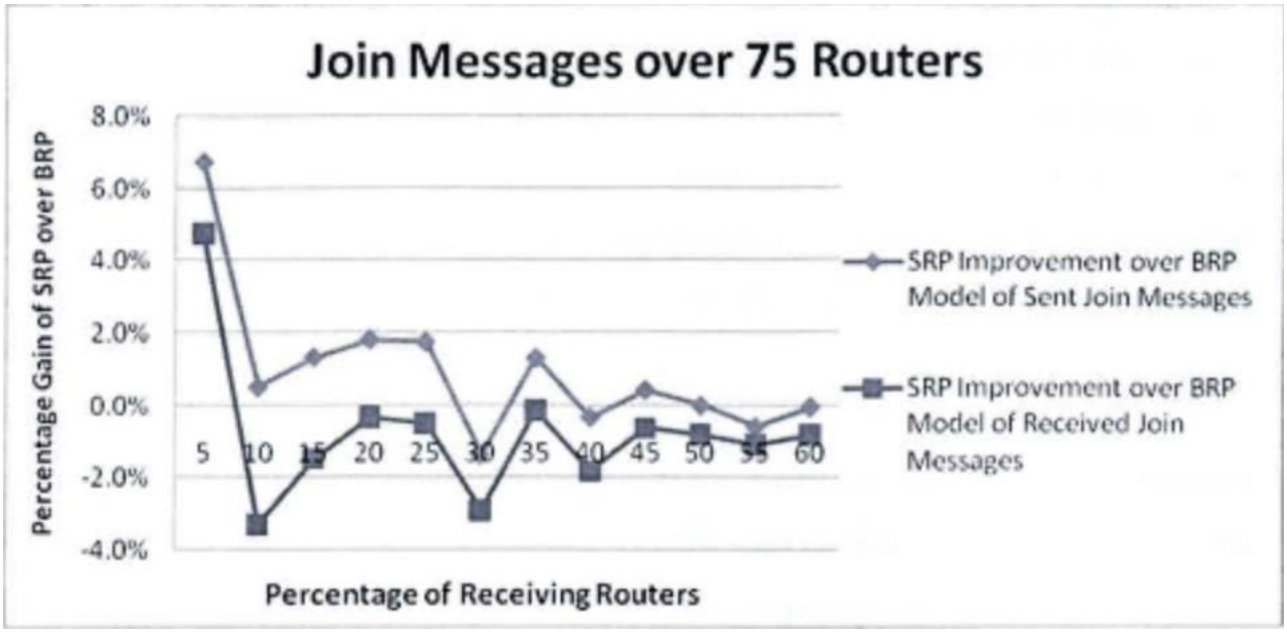

Рис. 4.4. Покращення SRP понад 75 вузлів

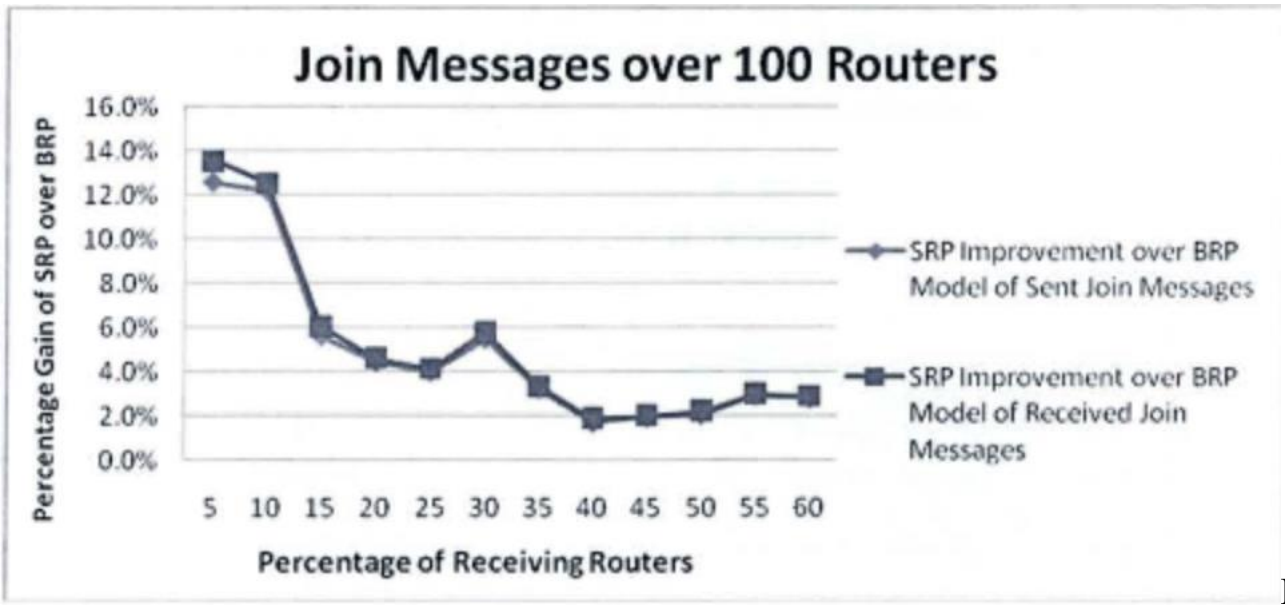

Рис. 4.5. Покращення SRP понад 100 вузлів

Міра активних каналів, залучених до передачі багатоадресного потоку навколо прикордонного маршрутизатора, вказує на концентрацію трафіку на прикордонному маршрутизаторі та навколо нього. На рисунку 4.6 порівнюється відсоткове покращення цих активних зв'язків для SRP і BRP

У міру збільшення відсотка приймачів у топології ефективність SRP стає більш вираженою. SRP порівняно з алгоритмом BRP зміщує корінь багатоадресного потоку від прикордонного маршрутизатора до централізованого RP усередині доменного середовища. Це усуває перевантаження зв'язку навколо прикордонного маршрутизатора та дозволяє іншому трафіку використовувати звільнену смугу пропускання. Буде зменшено перевантаження на посиланнях, найближчих до прикордонного маршрутизатора. BRP не враховує перевантаження каналів навколо прикордонного маршрутизатора, і з цієї причини має вищу активну щільність зв'язку навколо прикордонних маршрутизаторів

На малюнку 4.6 для набору маршрутизаторів із 25 показано негативні результати при використанні SRP для низької щільності приймачів. Це пояснюється місцем розташування приймачів. У міру збільшення щільності приймачів розташування приймачів по відношенню до прикордонного маршрутизатора визначає кількість необхідних каналів. Оптимізація BRP без центрального RP

викликає перевантаження навколо прикордонних маршрутизаторів, враховуючи високу щільність приймачів. На малюнку 4.6 показано підвищення ефективності SRP із збільшенням кількості вузлів. Це безпосередньо пов'язано зі збільшенням кількості вузлів та їх відносного розташування по відношенню до прикордонних маршрутизаторів

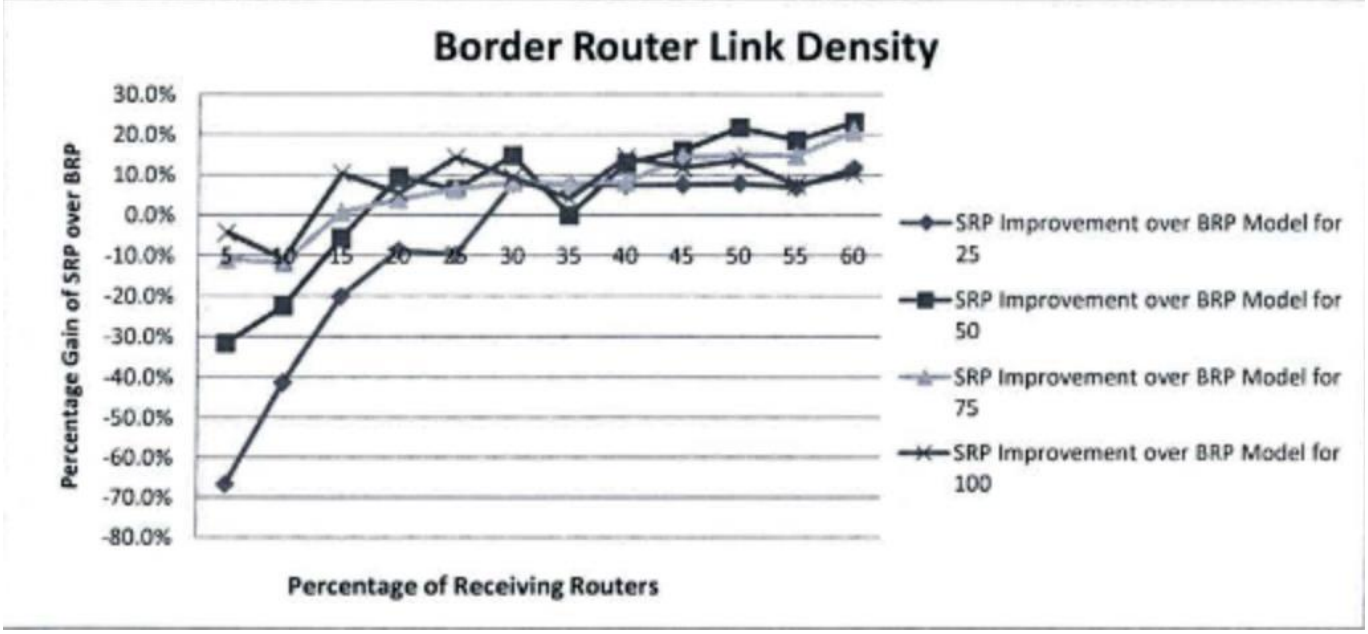

Рис. 4.6. Щільність активного з'єднання на межовому маршрутизаторі

Результати SRP для щільності активного посилання та трафіку повідомлень приєднання показують, що вони обернено пропорційні один одному. У міру збільшення продуктивності щільності активного посилання ефективність повідомлення приєднання знижується. Згідно з розглянутими результатами, 30-відсоткова щільність одержувача забезпечує найбільшу користь, якщо розглядати її разом із покращенням щільності зв'язку та трафіку повідомлень Join. Зрушення в топології, кількісно визначені на рисунках 4.2–4.5, впливають на внутрішньодоменні трафік, тоді як щільність каналів прикордонного маршрутизатора впливає на міждоменні трафіки

SRP демонструє переваги порівняно з BRP у зменшенні трафіку та заторів під час збою з'єднання всередині доменного середовища. SRP також має ще одну перевагу перед BRP. За допомогою BRP він оптимізує кількість переходів, щоб

зменшити перевантаженість каналу за допомогою використання кількох прикордонних маршрутизаторів. У симуляції було використано 2 прикордонні маршрутизатори. Загальна доступна пропускна здатність між доменами під час використання BRP зменшується для топології. В першу чергу це пов’язано з надлишковістю, яка створюється алгоритмом BRP. Однак SRP обчислює два шляхи до прикордонного маршрутизатора, але ініціалізує лише один із них. Це усуває надмірність, яка створюється за допомогою алгоритму BRP. Усуваючи цю надлишковість, це також зменшує попит на пропускну здатність між доменами

На рисунках 4.2–4.5 показано різну кількість покращень за допомогою алгоритму SRP порівняно з алгоритмом BRP. Неузгодженість результатів можна пояснити обмеженим набором даних або випадковими наборами приймачів. Одним із можливих рішень є збільшення кількості випадково згенерованих топологій для кожної щільності приймача. Наразі існує лише 20 топологій на щільність приймача. Збільшуючи кількість топологій, які симулюються, буде оцінено більше комбінацій, що має зменшити невідповідності на малюнках. Навіть незважаючи на відхилення, все ще спостерігається позитивна тенденція, яка чітко помітна на всіх графіках як для активності повідомлень приєднання, так і для щільності з’єднання маршрутизатора

ВИСНОВОК ДО РОЗДІЛУ 4

У цілому, результати моделювання показують, що SRP має переваги порівняно з BRP у зменшенні трафіку і заторів під час збою з’єднання всередині доменного середовища. Крім того, SRP може зменшити попит на пропускну здатність між доменами, усуваючи надмірність, яка створюється алгоритмом BRP.

Ось деякі конкретні висновки моделювання:

- SRP може забезпечити значні покращення продуктивності в порівнянні з BRP у зменшенні трафіку повідомлень Join.
- SRP може зменшити перевантаження каналів навколо прикордонних маршрутизаторів.

- SRP може зменшити попит на пропускну здатність між доменами.

Ці висновки свідчать про те, що SRP є перспективним підходом до оптимізації маршрутизації багатоадресної передачі в багатодомних мережах.

Однак важливо відзначити, що модельне дослідження має певні обмеження. Зокрема, воно грунтується на наборі випадкових топологій. Дослідження з іншими наборами топологій або з більшою кількістю топологій може надати додаткові відомості про ефективність SRP.

РОЗДІЛ 5 ОХОРОНА ПРАЦІ

Результатом даної дипломної робота є розроблена принципова схема комутаційного обладнання для оптимізації потоків трафіку.

Суб'єкт дипломної роботи інженер – проектувальник, який здійснює розробку і аналіз принципової схеми абонентського приймача кабельного цифрового телебачення.

Робоче місце інженера-проектувальника знаходиться в проектувальному відділі на другому поверсі.

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проектування знаходиться на другому поверсі п'ятиповерхового будинку. Приміщення має розміри: довжина 8 м, ширина 4 м, висота 4. Загальна площа - 32 м^2, загальний об'єм – 128 м^3. У відділі знаходиться 5 робочих місць інженерівпроектувальників, оснащені комп'ютерами.

Робоча площа одного співробітника становить:

$$S_{роб} = \frac{S_{заг.пл}}{N} = \frac{32}{5} = 6{,}4 \text{ м}_2$$

Робочий об'єм одного співробітника:

$$V_{роб} = \frac{V_{заг.об}}{N} = \frac{128}{5} = 25{,}6 \text{ м}_3$$

N- кількість співробітників у відділі

$S_{заг.пл}$ – загальна площа; $V_{заг.об}$

– загальний об'єм.

Відповідно до [31] площа на одне робоче місце має становити не менше ніж 6 $м^2$, а об'єм не менше ніж 20 $м^3$. Робоче місце інженера-проектувальника відповідає вимогам.

В проектному відділі інженера-проектувальника знаходяться: комп'ютери, принтер. У даному приміщенні температура повітря у теплий період року становить 30°С, використовується природне та штучне освітлення. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, а згідно з Державними санітарними нормами [32] не повинен перевищувати 50 дБ.

Робоче місце розташоване так, щоб природне світло падало з лівої сторони, при цьому відстань зі світлом до робочого місця - 1 м. Висота робочої поверхні столу над підлогою 750 мм, глибина столу – 800 мм, ширина столу 1300мм. Робочий стіл має простір для ніг висотою 650 мм та шириною 600 мм.

Перелік шкідливих та небезпечних виробничих чинників.

Створення сприятливих умов праці, в роботі інженера-проектувальника, має велике значення як для полегшення , так і для підвищення продуктивності праці. Відповідно до [33] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення
2. Недостатня освітленість робочої поверхні
3. Виробничий шум
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до [34] робота інженера-проектувальника у приміщенні з енерговитратами 90-120 ккал/год. відносяться до категорії легких фізичних робіт Іа (роботи, що виконуються сидячи і не потребують фізичного напруження).

Таблиця 5.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Ia	22-24
Теплий період року		23-25

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,°С	
		Верхня межа	Нижня межа
Холодний період року	Легка Ia	25	21
Теплий період року		28	22

У проектному відділі температура повітря становить 30°С в теплий період року,що перевищує допустиму на 2 °С. Забезпечили температуру приміщення 23 °С,за допомогою механічної вентиляції з вентилятором VORTICE VARIO, повітрообмін якого становить 680 $м^3$ /год.

Недостатня освітленість. В приміщенні встановлені персональні комп'ютери, присутнє природне та штучне освітлення . За вимогами [35], величина коефіцієнта природної освітленості повинна бути не менше 1.5%. В проектному відділі порушенні вимоги, освітленість робочої поверхні складає 370 лк , а коефіцієнт освітленості складає 1.2%. Природне світло проникає у приміщення через бічні світло прорізи. Вікна мають жалюзі. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників, розташованих паралельно лінії зору інженера-проектувальника.

Для місцевого освітлення використовувати галогенні лампи розжарювання

Виробничий шум. Шум на робочому місці створюється: комп'ютером та периферійним пристроєм. Допустимі рівні звукового тиску на робочому місці повинні відповідати вимогам [36]:

Таблиця 5.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Реальний рівень шуму в проектному відділі становить 54 дБ, що перевищує допустимий рівень.

Для зменшення рівня шуму рекомендується використовувати місцеву та загальну звукоізоляцію, шумопоглинаючі екрани, поглинаючі фільтри.

5.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [37].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [38].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В.

А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [39].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [40].

5.2.1. Розрахунок повітрообміну за надлишком тепла у проектному відділі

Приміщення має розміри 4□8□4, яке розміщується на другому поверсі п’ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні жалюзі. У приміщенні 5 інженерів-проектувальників, розташовано $N_{пк}$ = 5 персональних комп’ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,}\ \text{Вт} \qquad (5.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$- кількість тепла від інженерів-проектувальників

$Q_{рад,}$- кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \square \ , \tag{5.2}$$

де N - сумарна потужність джерел освітлення, Вт; $\square$ - коефіцієнт теплових витрат ($\square$ = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0{,}55 = 275 \text{ Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп'ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \tag{5.3}$$

де n – кількість комп'ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп} = 400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр} = 465$ Вт

$$Q_{облад} = 5 \cdot 400 + 465 = 2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проектувальників:

$$Q_{ін\text{-}пр.} = n \square \ q \ , \text{ Вт} \tag{5.4}$$

n – кількість інженерів-проектувальників

q – кількість тепла, що виділяється одним інженером-проектувальником

Кількість тепла, що виділяється одним інженером-проектувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \square 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад} = m \square S \square k \square q_{скл} \tag{5.5}$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = 150 – південь;

$$Q_{рад}=1\cdot 2{,}88\cdot 0{,}6\cdot 150=259{,}2 \text{ Вт}$$

5. Загальна кількість тепла в проектному відділі:

$$Q_{над}= Q_{осв}+ Q_{облад}+ Q_{ін\text{-}пр.} + Q_{рад}=275+2500+495+259{,}2 = 3{,}529 \text{ кВт}$$

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c\cdot\rho\cdot(t_{вид}-t_{зовн})}, \text{ м}^3/\text{год} \qquad (4.6)$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$$Q=3600\cdot Q_{надл}=3600\cdot 3529=12704 \text{ Вт} = 5328 \text{ кДж};$$

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС прий-

мається рівною $1{,}01\cdot 10^3$Дж/кг); ρ – густина повітря,

кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3); $t_{вид}$– температура

повітря, що видаляється, $t_{вид}=30$°С

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23°С

$$L = \frac{5328}{1{,}01\cdot 10^3\cdot 1{,}2\cdot(30-23)} = 628 \text{ м}^3/\text{год}$$

У зв'язку з перевищенням допустимого рівня температури повітря на 2 °С в проектному відділі, було встановлено механічну вентиляцію із використанням вентилятора VORTICE VARIO. Ця система забезпечила пониження температури повітря в приміщенні до оптимальних 23 °С..

5.3. Пожежна безпека

Згідно з посиланням [39-40], це приміщення відноситься до категорії В згідно з пожежною та вибуховою небезпекою через використання в ньому твердих горючих матеріалів, які мають температуру спалаху понад 61°С.

Проектний відділ оснащено:

- Двома безпровідними датчиками детектування диму SD-02 (оповіщає при задимленні приміщення; площа обслуговування: до 20 м^2);
- двома порошковими вогнегасниками ВП-5 (для приміщення категорії В за відсутності горючих газів і рідин, площею до 50 м^2 і масою вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників 2).

LifeSOS LS-30LR - це бездротова система пожежної та охоронної сигналізації. При виявленні вторгнення датчики передають сигнал тривоги на центральний блок через радіоканал без використання проводів. Центральний блок обробляє сигнали від датчиків, активує сирену, передає інформацію на централізований пульт нагляду, здійснює дзвінки на зазначені телефонні номери та відправляє SMS-повідомлення із зазначенням про спрацювання тривоги

Для попередження виникнення пожеж проводяться організаційно-технічні заходи пожежної безпеки, які включають:

- включення питань пожежної безпеки у всі інструкції по техніці безпеки;
- виконання встановленого режиму експлуатації електричних мереж та обладнання;
- заборона куріння в недозволеному місці;
- видання необхідних інструктажів, планів евакуації

Текстова частина плану евакуації містить інструкції та рекомендації щодо дій персоналу та відвідувачів у разі пожежі чи іншої надзвичайної ситуації. Зазначено місця збору на випадок евакуації та вказано правила безпечної поведінки під час виходу з приміщення. Важливою складовою текстової частини є інформація щодо розташування основних та аварійних виходів, місць збору та першої допомоги.

План евакуації має на меті максимально ефективно та безпечно вивести людей з будівлі в умовах надзвичайної ситуації. Графічна частина забезпечує візуальне розуміння шляхів евакуації, а текстова частина надає детальні інструкції та вказівки для виконання необхідних дій. Обидві частини спільно вирішують завдання забезпечення безпеки та організації евакуації в умовах небезпеки.

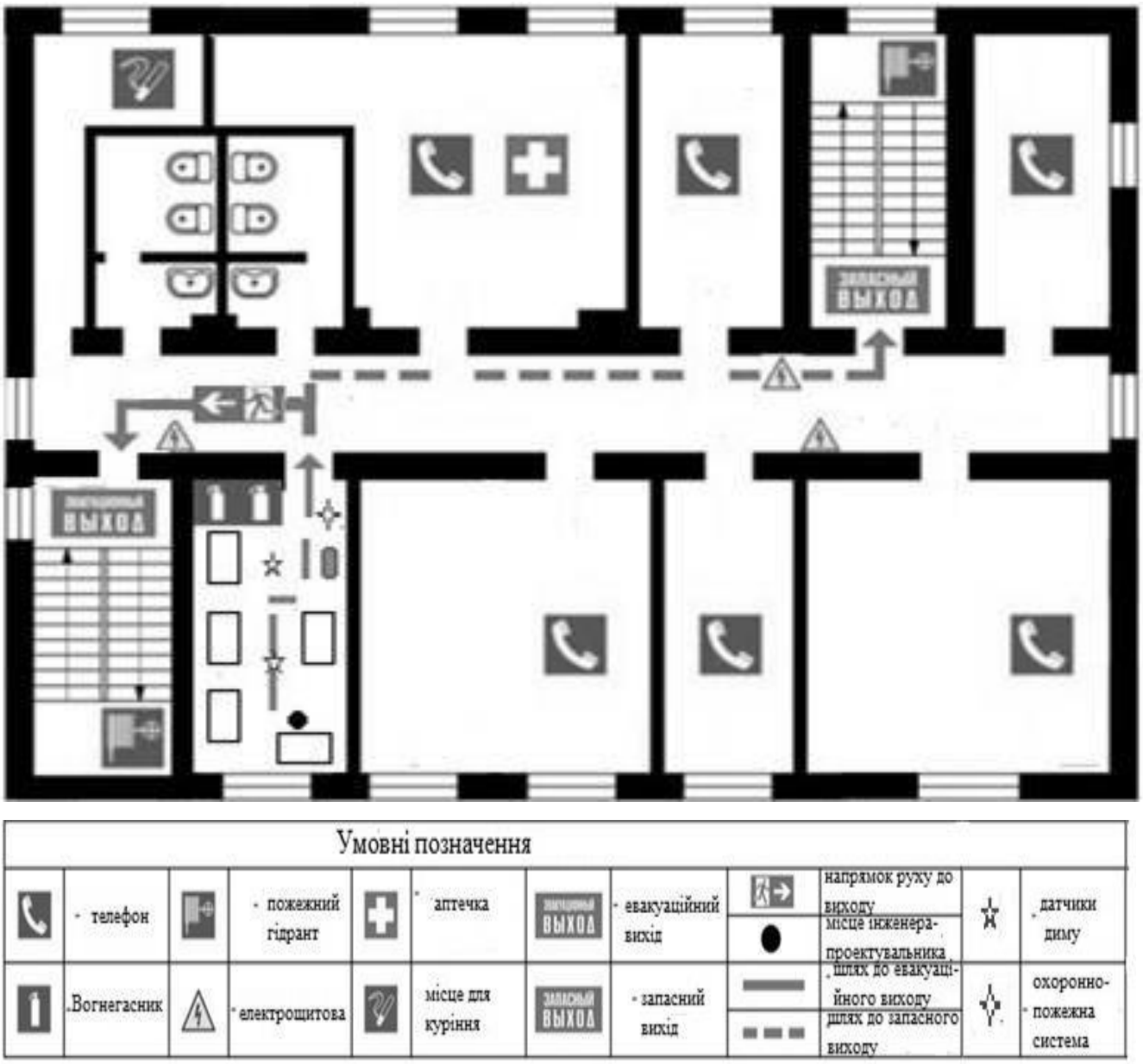

Рис 5.1. План евакуації 2 поверх

5.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.

• Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).

• Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.

• Ввімкнути живлення ПК.

• У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.

• При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

• Важливо стійко розташовувати всі компоненти пристрою на столі, зокрема клавіатуру. Забезпечте можливість переміщення клавіатури, враховуючи побажання користувача. При розміщенні клавіатури важливо враховувати нахил та положення, щоб вони відповідали комфортним умовам для користувача. Якщо клавіатура не має спеціального місця для опори долонь, вона повинна розташовуватися не менше 100 мм від краю столу в оптимальній зоні моніторного поля. Під час роботи за клавіатурою важливо забезпечити правильну посадку, уникати напруження та сидіти прямо.

• Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.

• Не припустимі сторонні розмови, роздратовуючи шуми тощо.

•

Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.

• Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)
- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

• Для зменшення негативного впливу на стан здоров’я працівників різних факторів ризику, пов’язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:

- через кожний час безперервної роботи – 10 хвилин; - через кожні 2 години – 15 хвилин.

• При можливості слід чергувати зміну діяльності з іншою, не пов’язаною з роботою на ПК.

• З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.

• При роботі на лазерних принтерах:

• Розташовувати принтер необхідно поряд з системним блоком так, щоб з’єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.

•

• Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.

• Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).

Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.

• При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.

• Для підтримки загального тонусу м'язів, профілактики кістково-м'язових порушень, зорового дискомфорту та інших несприятливих суб'єктивних почуттів під час регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.

• Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов'язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.

• Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.

• Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

• Закінчити і зберегти в пам'яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.

•

• Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.

• Вимкнути ПК кнопкою «POWER” (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки

• Накрити клавіатуру кришкою для попередження попадання в неї пилу.

• Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

Якщо після ввімкнення ПК відчувається запах горілого або при дотор-канні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.

• У разі виникнення пожежі важливо негайно розпочати гасіння за допомогою наявних засобів пожежогасіння. Одночасно повідомте про інцидент за телефоном 101 (міська пожежна охорона) та сповістіть начальника ДПД підприємства. Пам'ятайте, що для загашення електроустановок слід використовувати вуглекислотні вогнегасники та сухий пісок, щоб уникнути ризику ураження електричним струмом.

У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

ВИСНОВОК ДО РОЗДІЛУ 5

На підставі виконаного розрахунку повітрообміну за надлишком тепла, значення якого 628 $м^3$/год, встановили механічну вентиляцію з вентилятором VORTICE VARIO, оскільки використання природної вентиляції є малоефективним. Механічна вентиляція здатна забезпечити виведення з проектного відділу температури 30℃ і підтримувати температуру повітря допустимого та навіть оптимального значення.

РОЗДІЛ 6 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день радіотехнічне та електронне виробництво є досить розвинутим і без нього суспільство не уявляє свого життя. Електронна і радіотехнічна промисловість грає провідну роль в науково-технічній революції. Впровадження електронних приладів в різні сфери людської діяльності значною мірою сприяє успішній розробці складних науково-технічних проблем, підвищенню продуктивності фізичної і розумової праці, поліпшенню економічних показників виробництва.

В кваліфікаційній роботі розроблена система захисту з використанням серверного обладнання, що може здійснювати негативний вплив на навколишнє середовище.

6.1. Аналіз впливу техногенних чинників

Широке використання електричного та електронного обладнання дозволило не тільки підвищити якість життя людей, але й призвело до негативних наслідків для навколишнього середовища та здоров’я людини. Можна виділити основні шкідливі та небезпечні чинники, які впливають на навколишнє середовище [42]:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення
- теплове забруднення
- радіаційне забруднення

Шумове забруднення. У сучасному світі в умовах науково-технічного прогресу шум став однією з форм фізичного (хвильового) забруднення природного

•

середовища. Шумом прийнято вважати усі неприємні та небажані звуки або їх сукупність, які заважають нормально працювати, сприймати потрібну звукову інформацію та відпочивати.

Адаптація до нього практично неможлива. Фоновий рівень шуму навколишнього середовища становить 30-60 децибел. До цього природного фону за сучасних умов додаються виробничі й транспортні шуми, рівень яких нерідко перевищує 100 децибел. Джерелами шуму є: промислові об’єкти, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, юрби людей тощо. Шум у виробничих умовах негативно впливає на працівника: послаблює увагу, посилює розвиток втоми, сповільнює реакцію на небезпеку. Внаслідок цього знижується працездатність та підвищується ймовірність нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот на робочих місцях у виробничих приміщеннях наведені в таблиці 6.1 [42]:

Таблиця 6.1

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Дослідження встановило, що рослини, піддавшись впливу шуму, проявляють знижену енергію для зростання, що супроводжується надмірним виділенням вологи через листя та можливим порушенням у клітинах, що в кінцевому підсумку може призвести до загибелі рослин. Зокрема, листя і квіти рослин, розташованих близько до джерела інтенсивного шуму, можуть зазнавати негативних наслідків, включаючи гибель. Це явище особливо важливе для тварин, які обмінюються звуковою інформацією та використовують звуки для аналізу навколишнього середовища та

•

отримання інформації, включаючи сигнали тривоги. Звуковий шум може впливати на тварин, призводячи до втрати орієнтації та змін у звуковому оточенні, що може викликати стрес та негативні наслідки. Наприклад, реактивний літак може призвести до загибелі личинок бджіл та спричинити втрату орієнтації у пташиних гніздах, що призводить до тріщин у шкаралупі яєць. Аналогічно, коливання повітря від звуків переносної радіоапаратури можуть ускладнювати рух жуків, джмелів та інших комах.

Вібрація, що визначається як механічні коливання твердого тіла, поділяється на природну та штучну. Природна вібрація має своїм джерелом землетруси, викликані природними чинниками, тоді як штучна вібрація породжується промисловістю та транспортом. Довготривалі вібрації можуть серйозно впливати на здоров'я людини, викликаючи від сильної втоми до порушень різних функцій організму, таких як серцева діяльність, робота нервової системи, спазми судин, деформація м'язів та струс головного мозку. Особливо небезпечна є вібрація з частотою, яка резонансно взаємодіє з частотою коливання конкретних органів або частин тіла людини, що може спричинити їхнє ушкодження. Тривала дія вібрації може вести до професійного захворювання, відомого як вібраційна хвороба [42].

Електромагнітне забруднення представлено впливом електромагнітного поля (ЕМП), яке охоплює природний фон, такий як електричне і магнітне поле Землі та космічне електромагнітне випромінювання від Сонця. Однак, внаслідок науково-технічного прогресу, антропогенні джерела ЕМП від людської діяльності значно перевищують природний фон, негативно впливаючи на людину та довкілля. Вплив ЕМП залежить від діапазону частот, інтенсивності, тривалості, характеру випромінювання, режиму опромінювання та індивідуальних особливостей організму. Електромагнітні поля можуть викликати біологічні та функціональні порушення, проявляючись у передчасній втомлюваності, болях голови, погіршенні сну та інших функціональних проблемах. Тривалий та інтенсивний вплив ЕМП може призвести до стійких порушень та захворювань, які проявляються у теплових

•

та нетеплових ефектах. Теплова дія веде до підвищення температури тіла та нагрівання органів, що може бути особливо небезпечним для термочутливих органів. Наприклад, сантиметрове випромінювання може призвести до катаракти, що може призвести до поступової втрати зору [42].

Теплове забруднення. Теплове забруднення виникає внаслідок розсіювання теплоти у навколишнє середовище, що виникає під час численних теплових процесів, основним із яких є згорання палива. Процес згорання палива призводить до викидання до 23% кисню, який формується під час фотосинтезу на Землі протягом року. Спалювання вугілля, зокрема, призводить до більших викидів радіоактивних компонентів порівняно з усіма атомними електростанціями за той самий час при безаварійній роботі. Теплове забруднення гідросфери, у свою чергу, виникає переважно в результаті скидання підігрітих вод від теплових та атомних електростанцій у водойми. Це призводить до змін термічних та біологічних характеристик водойм, що має негативний вплив на їхніх мешканців [42].

6.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач – телевізійний приймач (приставка), пристрій, що приймає сигнал цифрового телебачення, декодує його і перетворює в аналоговий сигнал для виведення через роз'єми RCA або SCART або перетворює в цифровий сигнал для виведення через роз'єм HDMI , і передає його далі на телевізор.

Перехід до цифрового телебачення призвів до збільшення виробництва цифрових абонентських приймачів, що може мати негативний вплив на навколишнє середовище. Ці приймачі генерують слабкі електричні і магнітні поля в широкому діапазоні частот. Особливу увагу слід приділити впливу електромагнітних випромінювань, зокрема торсіонових полів, які є інформаційною компонентою цього випромінювання [45]. Наукові дослідження в Україні визначили торсіонові поля як фактор, що впливає на користувачів, особливо при використанні сучасних екранів [45]. Робоча група Всесвітньої організації охорони здоров'я виявила

•

порушення стану здоров'я при користуванні пристроями з електромагнітним випромінюванням, і ці порушення підтверджені результатами наукових досліджень [45]. Найсерйозніші:

- погіршення зору;
- порушення імунної системи;
- порушення психоемоційної сфери (стресовий синдром, агресивність)

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002». Значення ГДР напруженості електричної ($Е_{гд}$) і магнітної ($Н_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 5.2.

Таблиця 6.2

Значення ГДР напруженості електричної ($Е_{гд}$) і магнітної ($Н_{гд}$) складових

Час перебування персоналу, год	$Е_{гд}$, В/м					$Н_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

•

У результаті дії на організм людини електромагнітних випромінювань в діапазоні 30 кГц - 300 МГц (НЧ) спостерігається: загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в ділянці серця. З'являється роздратованість, втрачається увага, сповільнюються рухово-мовні реакції. Виникає ряд симптомів, які свідчать про порушення роботи окремих органів - шлунку, печінки, підшлункової залози.

Для того, щоб зменшити рівень електромагнітного випромінювання потрібно обмежити безперервний час роботи абонентського приймача [43-46].

В Україні норми електромагнітної безпеки регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання, згідно з якими допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення становлять 2,5 мкВт/см^2.

Абонентський приймач під час роботи створює шум, рівень якого становить 54 дБ. Допустимий рівень звукового тиску повинний відповідати «ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку», а саме 50 дБ.

Велика кількість звукових сигналів, що поступають до кори головного мозку, викликають переживання, страх, передчасну втому. Дія шуму на людину виражається в широкому діапазоні - від суб'єктивного роздратування до об'єктивних змін в ЦНС, органах слуху, серцево-судинних та ендокринній системах, травному акті та інших органів і систем. Першим показником шкідливої дії шуму є скарги на роздратованість, переживання, порушення сну [45].

6.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу ЕМП на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів,

•

потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають оптимальне розташування джерел електромагнітних полів (ЕМП) з метою мінімізації їх впливу на працівників. Додаткові заходи включають використання дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання та застосування засобів індивідуального захисту, таких як халати, комбінезони із металізованої тканини, з виводом на заземлюючий пристрій. Для захисту очей рекомендується використовувати захисні окуляри ЗП5-90 з напівпровідниковим оловом, яке послаблює інтенсивність електромагнітної енергії при світлопропусканні не менше 75%.

Засоби індивідуального захисту (ЗІЗ) слід використовувати тільки в тих випадках, коли інші захисні засоби неможливі або не надають достатньо ефективного захисту. Це може включати проходження через зони підвищеної інтенсивності опромінення, проведення ремо нтних і налагоджувальних робіт в аварійних ситуаціях, короткочасний контроль та зміну інтенсивності опромінення. Незважаючи на важливість, ЗІЗ можуть бути незручними в експлуатації, обмежувати можливість виконання трудових операцій та погіршувати гігієнічні умови..

Засоби індивідуального захисту, призначені для роботи в радіочастотному діапазоні, функціонують за принципом екранування, використовуючи відбиття і поглинання електромагнітного випромінювання (ЕМВ). Для захисту тіла використовується спеціальний одяг із металізованих тканин і матеріалів, які

•

поглинають радіочастоти. Металізована тканина може бути виготовлена з бавовняних ниток, які містять тонкі металеві провідці всередині, або з бавовняних чи капронових ниток, які обмотані металевим дротом. Така тканина, схожа на металеву сітку з відстанню між нитками до 0,5 мм, ефективно послаблює вплив радіочастотного випромінювання. При зшиванні деталей захисного одягу важливо забезпечити контакт ізольованих проводів, і для цього електрогерметизацію швів здійснюють за допомогою електропровідних мас або клею, які забезпечують гальванічний контакт або збільшують електричний зв'язок між ізольованими проводами..

Лікарсько-профілактичні заходи включають в себе проведення регулярних медичних оглядів працівників, які перебувають у зоні дії електромагнітного випромінювання. Заходи також передбачають обмеження часу перебування людей в області підвищеної інтенсивності електромагнітних полів, надання працюючим безкоштовного лікарсько-профілактичного харчування та організацію санітарно-оздоровчих перерв.

Захист від шуму. Для зменшення і ліквідації шуму застосовується комплекс заходів, відомий як шумозахист. Цей комплекс включає в себе використання звукопоглинаючих матеріалів, раціональне розташування будівельних об'єктів, створення земляних валів та стін різних конструкцій уздовж вулиць, а також використання шумовідбиваючих будівель, таких як магазини, склади та гаражі..

Проблема електронних відходів. Згідно з Законом України "Про відходи", для запобігання або зменшення обсягів утворення відходів, необхідно впроваджувати системи збирання та утилізації електричного та електронного обладнання [30]. З метою вирішення проблеми електронних відходів у країні, розробляється "Технічний регламент з поводження з відходами електричного та електронного обладнання", розробка якого почалася ще з 2008 року. За цим законодавчим актом, імпортери і виробники можуть утилізувати електровідходи самостійно або укладати

•

договори з уповноваженими підприємствами на організацію збирання, заготівлі та утилізації техніки.

Крім того, розглядається внесення змін до Податкового Кодексу, яким передбачається централізоване стягнення коштів з імпортерів та виробників різних товарів з метою організації ефективного збирання, заготівлі та утилізації відходів від цих товарів. Також розглядається проект Постанови Кабінету Міністрів України щодо затвердження Технічного регламенту з поводження з відходами електронного та електричного устаткування, який передбачає створення безоплатних пунктів збору відходів електронного та електричного обладнання для користувачів.

Проблему електронних відходів в Україні слід вирішувати комплексно, звертаючи увагу як на організаційно-правовий аспект (створення фондів виробників, підтримка держави для підприємств з утилізації відходів), так і на соціально-інформаційний (необхідно переконувати українців, що викидати пошкоджений електронний пристрій на звичайний смітник – неприпустимо).

ВИСНОВОК ДО РОЗДІЛУ 6

Телекомунікаційні ресурси створюють негативний вплив на навколишнє середовище. Вони є джерелами електромагнітного випромінювання та шумового забруднення. Для мінімізації ризику виникнення захворювань, ефективними є інженернотехнічні заходи, які зменшать дію шкідливих чинників. Також були розглянута проблема електронних відходів, одним зі шляхом вирішення якої є створення пунктів збору відходів електронного та електричного обладнання

•

ВИСНОВКИ

Спостерігається відновлення інтересу до багатоадресної передачі через її ефективність пропускної здатності при розповсюдженні контенту IPTV. У той час як попит на контент IPTV зростає, зростає також потреба в надійності та ефективності. Хоча ефективність такого розгортання вивчена, недостатньо розуміння того, як надійність і ефективність пов’язані між собою. Надійність є важливим фактором у будь-якій топології мережі. SRP намагається співвіднести як надійність використання кількох вхідних граничних маршрутизаторів, так і ефективність зменшення кількості фактичних каналів, необхідних для обслуговування набору приймачів. І SRP, і BRP використовують переваги кількох прикордонних маршрутизаторів. Оскільки витрати на смугу пропускання продовжують зменшувати вихідні посилання на міждоменні стають доступнішими

IPTV із вмістом HD може споживати до 19 Мбіт/с на потік. Мережа провайдера IPTV зазвичай передає сотні таких потоків. Ці постачальники також пропонують інші послуги споживачам у своїй мережі. Ці послуги включають високошвидкісний Інтернет і VOIP. SRP можна розгорнути, щоб зменшити перевантаження навколо прикордонних маршрутизаторів, а також перевантаження всередині топології під час збою з’єднання. Раптова зміна топології може спричинити надмірне надання посилань у межах внутрішньодоменної топології. Як правило, високошвидкісний Інтернет не є пріоритетною послугою для провайдера порівняно з VOIP. Отже, веб-трафік зазвичай не має пріоритету в мережі. Без SRP раптова зміна топології може вплинути на інші служби, включно з багатоадресним трафіком і веб-трафіком. SRP також обмежує один вхідний прикордонний маршрутизатор на багатоадресний потік порівняно з BRP, який може призначити кілька прикордонних маршрутизаторів для багатоадресного потоку. Якщо призначити кілька прикордонних маршрутизаторів на потік, будь-яка перевага пропускної здатності буде зменшена. На відміну від цього, SRP визначає шлях до

•

другого прикордонного маршрутизатора, але не використовує його, доки перший прикордонний маршрутизатор не стане недоступним. Це гарантує, що якщо на основному прикордонному маршрутизаторі станеться збій зв’язку, другий шлях можна швидко ініціалізувати. Цей другий шлях оптимізовано для зменшення кількості переходів від RP до другого прикордонного маршрутизатора. Налаштувавши багатоадресний потік таким чином, можна зберегти пропускну здатність між доменами. SRP також усуває перевантаження каналів навколо прикордонного маршрутизатора, зменшуючи кількість посилань на багатоадресний потік. Це досягається шляхом зміни розподілу багатоадресного потоку на RP

Збереження пропускної здатності продовжує залишатися важливою темою, оскільки споживачі вивчають більше мультимедійних програм. Мережні провайдери традиційно уникають дорогих оновлень і натомість покладаються на інші засоби, такі як Deep Level Packet Inspection, щоб контролювати пропускну здатність своїх мереж. SRP можна використовувати як інструмент, який допоможе уникнути дорогих оновлень і підвищити ефективність мережі

Майбутня робота щодо SRP може включати кілька точок входу та балансування збоїв зв’язку між кількома наборами точок входу. Це дозволить ще краще контролювати пропускну здатність під час збою з’єднання. Наслідки коливань маршруту під час інтенсивного транспортного навантаження є ще однією областю для вивчення. SRP забезпечує покращення контролю перевантаження мережі порівняно з BRP. Усі ці теми дозволять краще зрозуміти ефективність SRP, і їх слід вивчити найближчим часом.

•

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wielosz, Anna.; Islam, Kashif. "Achieving fast restoration times in IP networks for IPTV video transport"- case study. Cisco Systems, Inc.
2. Wang, N.; Pavlou, G. "Traffic engineered multicast content delivery without MPLS overlay Multimedia", IEEE Transactions on Volume 9, Issue 3, April2007 Page(s):619- 628
3. Wang, N.; Pavlou, G. "An efficient IP based approach for multicast routing optimisation in multi-homing environments. Next Generation Internet Design and Engineering", 2006. NGI apos;06. 2006 2nd Conference on Volume, Issue, 3-5 April2006 Page(s): 8 pp.
4. T.C. Bressoud et al. "Optimal Configuration for BOP Route Selection", IEEE INFOCOM, 2003.
5. T. Przygienda et al. "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems". Cisco Systems, February, 2008
6. P. Psenak et al, "Multi-Topology (MT) Routing in OSPF" Internet Draft, draft-ietf-ospf-mt-04.txt Apr. 2005
7. B. Fortz et al, "Internet Traffic Engineering by Optimising OSPF Weights", IEEE INFOCOM, 2000, pp. 519-528
8. A. Sridharan et al, "Achieving Near-Optimal Traffic Engineering Solutions for Current OSPF/IS-IS Networks", IEEE INFOCOM, pp. 1167-1177, Apr. 2003
9. Y. Wang et al, "Internet Traffic Engineering without Full Mesh Overlaying", Proc. IEEE INFOCOM, Vol. 1, pp. 565-571, 2001
10. N. Wang, G. Pavlou, "Bandwidth Constrained IP Multicast Traffic Engineering without MPLS Overlay", IEEE/IFIP MMNS, 2004
11. The GEANT network topology, available online at:

•
http://www.geant.net/upload/pdf/Topology_ Oct_2004.pdf
57
12. Wong,T.;Van Jacobson;Alaettinoglu, C. "Internet routing anomaly detection and visualization". Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on 28 June- I July 2005 Page(s):172- 181
13. Zhang, Jian; Rexford, Jennifer; Feigenbaum, Joan. "Learning-Based Anomaly Detection in BGP Updates". Proceeding of the 2005 ACM SIGCOMM workshop on Mining network data, 2005.
14. P. Rajvaidya, K. Almeroth."Multicast Routing Instabilities", IEEE Internet Computing, Vol. 8, Issue 5, 2004, pp. 42-49
15. Haakon Ringberg; Augustin Soule; Jennifer Rexford; Christophe Diot. "Sensitivity ofPCA for traffic anomaly detection". SIGMETRICS '07 Conference Proceedings, June 2007
16. Soule, Augustin; Salmatian, Kave; Taft, Nina. "Combining Filtering and Statistical Methods For Anomaly Detection". IMC '05, 2005 Internet Measurement Conference, Pp. 331-344
17. Simsarian, J .E.; Duelk, M. "IPTV Bandwidth Demands in Metropolitan Area Networks". Local & Metropolitan Area Networks, 2007. LANMAN 2007. 15th IEEE Workshop on 10-13 June 2007 Page(s):31- 36
18. Ying-Dar Lin; Nai-Bin Hsu; Chen-Ju Pan.;"Extension of RP relocation to PIM-SM multicast routing". Communications, 2001. ICC 2001. IEEE International Conference on Volume 1, 11-14 June 2001 Page(s):234- 238 vol.l