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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Метод підвищення ефективності програмно-конфігурованих мереж»

Виконавець: _____ Костянтин ЗАБЛОЦЬКИЙ
(підпис)

Керівник: _____ Роман ОДАРЧЕНКО
(підпис)

Консультанти з окремих розділів пояснювальної записки:

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

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

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

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Заблоцького Костянтина Васильовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Метод підвищення ефективності програмно-конфігурованих мереж»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: архітектура мережі ПКМ, способи передачі даних мережевих елементів, середовище моделювання програмно-конфігурованих мереж.
4. Зміст пояснювальної записки: дослідження ефективності сучасних програмно-конфігурованих мереж, удосконалена модель функціонування та надання послуг ПКМ, методи підвищення ефективності функціонування ПКМ, дослідження ефективності розроблених рішень.
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: рисунки структури мережі ПКМ, рисунки удосконалення архітектури програмно-конфігурованих мереж, рисунки архітектури МК-ПКМ, рисунки МК-ПКМ у середовищі моделювання, рисунки застосування МК-ПКМ, рисунки порівняння показників продуктивності методів.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Дослідження ефективності сучасних програмно-конфігурованих мереж	12.09.2022-24.09.2022	Виконано
4	Удосконалена модель функціонування та надання послуг ПКМ	26.09.2022-08.10.2022	Виконано
5	Методи підвищення ефективності функціонування ПКМ	10.10.2022-22.10.2022	Виконано
6	Дослідження ефективності розроблених рішень	24.10.2022-05.11.2022	Виконано
7	Охорона праці	07.11.2022-12.11.2022	Виконано
8	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Роман ОДАРЧЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Костянтин ЗАБЛОЦЬКИЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Метод підвищення ефективності програмно-конфігурованих мереж» містить 158 сторінок, 21 рисунок, 14 таблиць, 18 використаних джерел.

ПКМ, ПРОГРАМНО-КОНФІГУРОВАНА МЕРЕЖА, ДОСЛІДЖЕННЯ, УДОСКОНАЛЕННЯ, АРХІТЕКТУРА, ОНОВЛЕННЯ, МЕТОД, АЛГОРИТМ, МЕРЕЖЕВІ ЕЛЕМЕНТИ, ЕФЕКТИВНІСТЬ, ПОКАЗНИК, СТРУКТУРА, ЗАСТОСУВАННЯ, РОЗМІЩЕННЯ, КОНТРОЛЕР, КОМУТАТОР.

Об’єкт дослідження – показники ефективності програмно-конфігурованих мереж.

Предмет дослідження – метод підвищення ефективності програмно-конфігурованих мереж.

Мета кваліфікаційної роботи – розробка методу підвищення показників продуктивності мережі.

Метод дослідження – застосування кількох алгоритмів для вибору та розміщення контролерів ПКМ.

Матеріали кваліфікаційної роботи рекомендується використовувати при розробці та створенні програмно-конфігурованих мереж з великою кількістю мережевих елементів, що потребують ефективного та відмовостійкого керування. За допомогою даного методу можливо досягнути високих показників продуктивності мережі.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

2PL (two phase locking)- Двофазне блокування

API (application programming interface) - прикладний програмний інтерфейс

IETF (internet enginering task force) - Інженерна група Інтернету

IP (internet protocol) – Інтернет протокол

NFV (network functions virtualization) - віртуалізації мережевих функцій

TCP (transmission control protocol) – протокол управління передачею

UDP (user datagram protocol) – протокол користувацьких датаграм

АПГ - алгоритм пошуку гармонії

АРЧ - алгоритм рою частинок

МК-ПКМ – мультиконтролерна програмно-конфігурована мережа

МР - менеджерів ресурсів

МТ - менеджер транзакцій

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ПКМ – програмно-конфігуровані мережі

ПРЄКІНН - проблема розміщення ємного контролера з імітацією невдачі нормалізації

ПРЄКОПЗ - проблема розміщення ємного контролера з оптимізацією підв’язкової змійки

СВ - середовищ виконання

СУБД - систем управління базами даних

СЧП - середній час проходження

ЦОД - центр обробки даних

ЧС - час сеансу

ВСТУП

Актуальність теми. Програмно-конфігурована мережа (ПКМ) — це захоплююча технологія, яка забезпечує інновації в тому, як ми розробляємо мережі та керуємо ними. Хоча ця технологія, здається, з'явилася раптово, ПКМ є частиною довгої історії зусиль зробити комп'ютерні мережі більш програмованими. Я простежив інтелектуальну історію програмованих мереж, включаючи активні мережі, перші спроби відокремити площину керування та даних, а також нещодавню роботу над OpenFlow та мережевими операційними системами. Також я висвітлив ключові концепції і технологічні поштовхи та додатки, які спонукали до кожної інновації. Попутно розвінчав поширені міфи та хибні уявлення про технології та прояснив зв'язок між ПКМ і пов'язаними технологіями, такими як віртуалізація мережі.

Для керування великими комп'ютерними мережами необхідно багато видів обладнання, від маршрутизаторів і комутаторів до проміжних пристроїв, таких як брандмауери, транслятори мережевих адрес, балансувальники навантаження на сервер і системи виявлення вторгнень. Для безперебійної роботи цих систем на маршрутизаторах і комутаторах працює складне розподілене керуюче програмне забезпечення, яке зазвичай є закритим і власницьким (пропрієтарним). Програмне забезпечення реалізує мережеві протоколи, що проходять роки стандартизації та тестування на сумісність. Зазвичай мережеві адміністратори налаштовують окремі мережеві пристрої за допомогою інтерфейсів конфігурації, які відрізняються в різних постачальників і навіть у різних продуктів від одного постачальника. Хоча деякі інструменти керування мережею пропонують централізоване управління для конфігурації мережі, ці системи все ще працюють на рівні окремих протоколів, механізмів та інтерфейсів конфігурації. Такий спосіб роботи сповільнив інновації, збільшив складність, а в результаті як капітальні, так і витрати на експлуатацію мережі.

ПКМ змінює спосіб проектування та керування мережами. Програмно-конфігурована мережа має дві визначальні характеристики. По-перше, ПКМ

відокремлює площину керування (що вирішує, як обробляти трафік) від площини даних (що пересилає трафік відповідно до рішень, які приймає площина керування). По-друге, ПКМ організовує площину керування так, що одне керуюче програмне забезпечення контролює декілька елементів площини даних. Площина управління ПКМ здійснює безпосередній контроль над станом елементів площини даних мережі (тобто маршрутизатори, комутатори та інші проміжні блоки) через чітко визначений інтерфейс прикладного програмування (API).

За останні кілька років ПКМ набула значного поширення в промисловості. Багато комерційних комутаторів підтримують OpenFlow API. Початкові постачальники, які підтримували OpenFlow, включали HP, NEC і Pronto. З тих пір цей список різко розширився. З'явилося багато різних платформ контролерів. Програмісти використовували ці платформи для створення багатьох програм, таких як динамічний контроль доступу, балансування навантаження на сервер, віртуалізація мережі, енергоефективна мережа, безпроблемна міграція віртуальних машин і мобільність користувачів. Ранні комерційні успіхи, такі як глобальна система керування трафіком Google і платформа мережевої віртуалізації Nicira, привернули значну увагу галузі. Багато найбільших світових інформаційно-технологічних компаній (наприклад, хмарні провайдери, оператори, постачальники обладнання та фірми, що надають фінансові послуги) приєдналися до галузевих об'єднань ПКМ, таких як Open Networking Foundation та ініціатива Open Daylight.

Хоча хвилювання щодо програмно-конфігурованих мереж стало більш відчутним протягом останніх кількох років, багато ідей, що лежать в основі ПКМ, розвивалися протягом останніх двадцяти та навіть більше років. У певному сенсі ПКМ переглядає ідеї ранніх телефонних мереж, які використовували чіткий розподіл площини керування та даних для спрощення керування мережею та розгортання нових послуг. Проте відкриті інтерфейси, такі як OpenFlow, забезпечують більше інновацій у платформах контролерів і програмах, ніж це було можливо в закритих мережах, розроблених для вузького спектру телефонних послуг. В іншому ПКМ нагадує минулі дослідження активних мереж, які сформували бачення програмованих мереж, хоча й з наголосом на програмовані площини даних. ПКМ також стосується

попередньої роботи з розділення площини керування та даних у комп'ютерних мережах.

Зв'язок роботи з науковими програмами, планами, темами. Розробка методу виконана в рамках кваліфікаційної роботи студента-магістра.

Мета і завдання дослідження. Розробити метод підвищення показників продуктивності ПКМ, а саме: розробити ефективну методологію для оптимізації розміщення кількох контролерів адаптованим способом.

Для досягнення поставленої мети вирішуються такі наукові завдання:

1. Дослідження ефективності сучасних ПКМ.
2. Дослідження удосконаленої моделі функціонування та надання послуг програмно-конфігурованих мереж.
3. Дослідження методів підвищення ефективності функціонування ПКМ.
4. Розробка методу оптимізації розгортання кількох контролерів та дослідження ефективності розроблених рішень.

Об'єктом дослідження є показники ефективності програмно-конфігурованих мереж.

Предметом дослідження є метод підвищення ефективності програмно-конфігурованих мереж.

Методи досліджень. Для підвищення ефективності програмно-конфігурованих мереж.

Об'єкт дослідження – показники ефективності програмно-конфігурованих мереж.

Предмет дослідження – мультиконтролерний метод підвищення ефективності програмно-конфігурованих мереж.

Мета кваліфікаційної роботи – розробити метод підвищення показників продуктивності мережі. У даному методі застосовуються кілька алгоритмів для вибору та розміщення контролерів ПКМ.

Метод дослідження – використання кількох алгоритмів для вибору та розміщення контролерів для керування мережевими елементами.

Наукова новизна отриманих результатів. Розробка ефективної методології для оптимізації розміщення кількох контролерів адаптованим способом є дуже важливою та складною проблемою в такому складному середовищі, особливо через різні, пов’язані пов’язані між собою вимоги. Таким чином, оптимізація розгортання кількох контролерів у ПКМ є складною проблемою через мінливість багатьох параметрів і складних умов роботи. Надається ефективне гібридне рішення на основі метаевристики для проблем розміщення контролера в середовищі ПКМ. Це дослідження спрямоване на мінімізацію затримки між контролерами, мінімізацію затримки між комутаторами та максимізацію рівня відмовостійкості контролера.

Практичне значення отриманих результатів. Матеріали кваліфікаційної роботи рекомендується використовувати при розробці та створенні програмно-конфігурованих мереж з великою кількістю мережевих елементів, що потребують ефективного та відмовостійкого керування. За допомогою даного методу можливо досягнути високих показників продуктивності мережі.

РОЗДІЛ 1

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СУЧАСНИХ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

1.1. Аналіз концепції програмно-конфігурованих мереж

Розробка більш програмованих комп'ютерних мереж дозволяє розвиватися інноваціям в управлінні мережею та знижує бар'єр для розгортання нових послуг. У цьому розділі я розгляну перші роботи над програмованими мережами. Історію можна поділити на три етапи:

Кожен етап має свій власний внесок в історію:

1) активні мережі (з середини 1990-х до початку 2000-х), які запровадили програмовані функції в мережі та сприяли більшій інновації;

2) розділення площини керування та даних (приблизно з 2001 по 2007 рр.), що розробило відкриті інтерфейси між площиною керування та даних.

3) OpenFlow API та мережеві операційні системи (з 2007 року приблизно до 2010 року), які являли собою перший випадок широкого впровадження відкритого інтерфейсу та розроблені способи зробити розділення площини даних керування масштабованим та практичним.[1]

Віртуалізація мережі відігравала важливу роль протягом історичної еволюції програмно-конфігурованих мереж, значно передувавши даній технології, хоча це і було одним із перших значущих випадків використання ПКМ.

З початку до середини 1990-х років Інтернет почав розвиватися, його застосування та привабливість значно перевершили ранні застосування передавання файлів та електронної пошти для вчених. Більш різноманітні додатки та широке використання широким загалом привернули дослідників, що прагнули перевірити та розгорнути нові ідеї для покращення мережевих послуг. Для цього дослідники розробили та випробували нові мережеві протоколи в невеликих лабораторних умовах і змоделювали поведінку у великих мережах. Потім, якщо мотивація та

фінансування зберігалися, вони передавали ідеї Інженерній групі Інтернету (IETF) для стандартизації цих протоколів. Процес стандартизації був повільним і зрештою розчарував багатьох дослідників.

У відповідь на це деякі дослідники мережі застосували альтернативний підхід до відкриття мережевого контролю, приблизно заснований на аналогії відносної легкості перепрограмування автономного ПК. Зокрема, звичайні мережі не є «програмованими» в будь-якому значенні цього слова. Активна мережа представляла собою радикальний підхід до керування мережею, передбачаючи інтерфейс програмування (або мережевий API), який надавав ресурси (наприклад, обробку, зберігання та черги пакетів) на окремих вузлах мережі та підтримував побудову спеціальної функціональності для застосування до підмножина пакетів, що проходять через вузол. Такий підхід викликав занепокоєння багатьох в Інтернет-спільноті, які захищали таку простоту.

Програма дослідження активних мереж вивчала радикальні альтернативи послугам, що надаються традиційним стеком Інтернету через IP або за допомогою асинхронного режиму передачі (AMT), іншого домінуючого мережевого підходу початку 1990-х років.[2]

Активне мережеве співтовариство переслідувало дві моделі програмування:

• капсульна модель, де код для виконання на вузлах передається в діапазоні в пакетах даних.

• модель програмованого маршрутизатора/комутатора, де код для виконання на вузлах встановлювався за допомогою позасмугових механізмів.

Капсульна модель найбільш тісно пов’язана з активним нетворкінгом. Проте в інтелектуальному зв’язку з подальшими зусиллями обидві моделі мають деяку тривалу спадщину. Капсули передбачали встановлення нової функціональності площини даних у мережі, перенесення коду в пакетах даних (як у попередній роботі над пакетним радіозв’язком) та використання кешування для підвищення ефективності розповсюдження коду. Програмовані маршрутизатори передали рішення щодо розширюваності безпосередньо в руки оператора мережі.

«Технологічні поштовхи», які заохочували активну роботу в мережі, включали зниження вартості обчислень, що дозволило розмістити більше обробки в мережі, прогрес у мовах програмування, таких як Java, яка забезпечувала переносимість платформи та певну безпеку виконання коду, а також віртуальну машину, - технологія, яка захищала хост-машину (в даному випадку активний вузол) та інші процеси від програм, що погано поводяться. Деякі активні дослідницькі проекти мереж також скористалися прогресом у швидкій компіляції коду та формальними методами.

Важливим каталізатором активної мережевої екосистеми був інтерес фінансових агентств, зокрема програма Active Networks, створена та підтримувана Агентством передових оборонних дослідницьких проектів США (DARPA) із середини 1990-х до початку 2000-х років. Хоча не всі дослідницька робота в активних мережах фінансувалася DARPA, програма фінансування підтримувала низку проектів і, що, можливо, важливіше, заохочувала зближення термінології та набору активних мережевих компонентів, щоб проекти могли зробити внесок у ціле, яке мало бути більшим, ніж сума частин. Програма «Активні мережі» робила наголос на демонстрації та сумісності проектів із супутнім рівнем зусиль щодо розробки. Сміливий і узгоджений поштовх з боку фінансової агенції за відсутності найближчих варіантів використання, можливо, також сприяв певному скептицизму спільноти щодо активного мережевого спілкування, яке часто було здоровим, але могло межувати з ворожістю та могло затьмарити деякі інтелектуальні зв’язки між цією роботою та пізнішими зусиллями забезпечити мережеву програмованість.

«Притягнення до використання» для активної мережі, описані в літературі того часу, надзвичайно схожі на приклади, які використовуються для мотивації ПКМ сьогодні. Проблеми дня включали розчарування постачальників мережевих послуг термінами, необхідними для розробки та розгортання нових мережевих послуг (так звана окостеніння мережі), зацікавленість третіх сторін у доданій вартості, детальний контроль для динамічного задоволення потреб конкретні додатки чи умови мережі, а також бажання дослідника мати платформу, яка б підтримувала масштабні експерименти. Крім того, у багатьох ранніх статтях про активну мережу згадувалося

про поширення проміжних блоків, включаючи брандмауери, проксі та транскодери, кожен з яких мав розгортатися окремо та передбачав окрему (часто залежну від постачальника) модель програмування. Активна мережа запропонувала бачення уніфікованого контролю над цими проміжними блоками, що зрештою могло замінити спеціальні одноразові підходи до управління та контролю за цими скриньками. Цікаво, що рання література передвіщає сучасні тенденції у віртуалізації мережевих функцій (NFV), яка також спрямована на забезпечення уніфікованої системи керування для мереж, які мають складну пропускну здатність проміжних функцій.

Активні мережі запропонували інтелектуальний внесок, який стосується ПКМ. Особливо відзначу три:

• Програмовані функції в мережі, щоб знизити бар'єр для інновацій. Дослідження активних мереж започаткували поняття програмованих мереж як способу знизити перешкоди для мережевих інновацій. Думка про те, що у виробничій мережі важко впроваджувати інновації, і прохання про збільшення можливостей програмування зазвичай цитувалися в початковій мотивації для ПКМ. Значна частина раннього бачення ПКМ була зосереджена на програмованості площини керування, тоді як активні мережі більше зосереджувалися на програмованості площини даних. Тим не менш, програмованість площини даних продовжувала розвиватися паралельно з зусиллями на площині керування, і програмованість площини даних знову виходить на передній план у новій ініціативі NFV. Остання робота над ПКМ досліджує еволюцію протоколів ПКМ, таких як OpenFlow, для підтримки більш широкого діапазону функцій площини даних. Крім того, концепції ізоляції експериментального трафіку від звичайного трафіку, які сягають корінням в активну мережу, також з’являються в центрі проектних документів для OpenFlow та інших технологій ПКМ (наприклад, FlowVisor).

• Віртуалізація мережі та можливість демультиплексування програмного забезпечення на основі заголовків пакетів. Необхідність підтримувати експерименти з кількома моделями програмування призвела до роботи над віртуалізацією мережі. Активна мережа створила архітектурну структуру, яка описує компоненти такої платформи. Ключовими компонентами цієї платформи є спільна операційна система

Node (NodeOS), яка керує спільними ресурсами; набір середовищ виконання (СВ), кожна з яких визначає віртуальну машину для пакетних операцій; і набір активних додатків (АД), які працюють у певному СВ для надання наскрізної послуги. Спрямування пакетів до певного СВ залежить від швидкого зіставлення шаблонів у полях заголовка та демультиплексування до відповідного СВ. Цікаво, що ця модель була продовжена в архітектурі PlanetLab, згідно з якою різні експерименти виконуються у віртуальному середовищі виконання, а пакети демультиплексуються у відповідне середовище виконання у своїх заголовках пакетів. Демультиплексування пакетів у різні віртуальні середовища виконання також було застосовано для проектування віртуалізованих програмованих апаратних площин даних.

• Бачення уніфікованої архітектури оркестровки проміжного блоку. Незважаючи на те, що це бачення ніколи не було повністю реалізоване в активній дослідницькій програмі мереж, у перших документах проектування вказувалося на необхідність об’єднання широкого спектру функцій проміжного блоку із загальною безпечною структурою програмування. Хоча це бачення, можливо, не вплинуло безпосередньо на нещодавню роботу над NFV, різноманітні уроки з активних мережевих досліджень можуть виявитися корисними, коли ми просуваємося вперед із застосуванням керування на основі ПКМ та оркестровки проміжних блоків.

Активна мережа включала уявлення про те, що мережевий API буде доступний для кінцевих користувачів, які створюють і отримують пакети, хоча більшість у дослідницькому співтоваристві повністю визнавали, що мережеві програмісти для кінцевих користувачів були б рідкістю. Помилкове уявлення про те, що пакети обов’язково містять код Java, написаний кінцевими користувачами, дозволило відкинути активне дослідження мережі як надто далеке від реальних мереж і за своєю суттю небезпечне. Активну мережу також піддавали критиці за те, що вона не могла запропонувати практичну продуктивність і безпеку. Хоча продуктивність не була першорядним питанням спільноти активних дослідників мереж (яка зосереджена на архітектурі, моделях програмування та платформах), деякі зусилля були спрямовані на створення високопродуктивних активних маршрутизаторів. Подібним чином, у

той час як у багатьох ранніх проектах безпеці не приділялося належної уваги, проект Secure Active Network Environment Architecture був помітним винятком. [3]

Хоча активні мережі сформулювали бачення програмованих мереж, технології не отримали широкого розгортання. Багато факторів спонукають до прийняття технології (або її відсутності). Можливо, одним із найбільших каменів спотикання, з якими зіткнулися активні мережі, була відсутність одразу переконливої проблеми чи чіткого шляху до розгортання. Важливим кроком активних досліджень мереж було те, що «вбивчі» програми для площини даних важко уявити. Спільнота запропонувала різні додатки, які могли б отримати вигоду від обробки в мережі, включно з об'єднанням інформації, кешуванням і розповсюдженням вмісту, керування мережею та спеціальними додатками. У площині керування, яка не лише потребувала значного перегляду, але також (оскільки вона зазвичай реалізована в програмному забезпеченні) представляла менший бар'єр для інновацій, ніж площина даних.

1.2. Показники ефективності програмно-конфігурованих мереж

На початку 2000-х років збільшення обсягів трафіку та більший акцент на надійності, передбачуваності та продуктивності мережі спонукали мережевих операторів до пошуку кращих підходів до певних функцій керування мережею, таких як контроль над шляхами, що використовуються для доставки трафіку (практика, широко відома як проектування трафіку). Засоби для проектування трафіку з використанням звичайних протоколів маршрутизації були в кращому випадку примітивними. Розчарування операторів цими підходами було визнано невеликою спільнотою дослідників, які працювали на магістральних мережах або регулярно стикалися з ними. Ці дослідники досліджували прагматичні, короткострокові підходи, які або орієнтувалися на стандарти, або неминуче розгорталися за допомогою існуючих протоколів.

Зокрема, звичайні маршрутизатори та комутатори втілюють тісну інтеграцію між площиною керування та даних. Цей зв'язок зробив різноманітні завдання керування мережею, такі як налагодження проблем конфігурації та прогнозування чи

керування поведінкою маршрутизації, надзвичайно складним. Щоб вирішити ці проблеми, почали з'являтися різноманітні спроби розділити площину даних і керування.

Коли Інтернет процвітав у 1990-х роках, швидкість з'єднання в магістральних мережах швидко зростала, що призвело до того, що постачальники обладнання впроваджували логіку пересилання пакетів безпосередньо в апаратному забезпеченні, окремо від програмного забезпечення рівня керування. Крім того, постачальникам послуг Інтернету (ISP) було важко впоратися зі збільшенням розміру та охоплення своїх мереж, а також вимогами до більшої надійності та нових послуг (таких як віртуальні приватні мережі). Паралельно з цими двома тенденціями швидкий розвиток стандартних обчислювальних платформ означав, що сервери часто мали значно більше пам'яті та ресурсів обробки, ніж процесор площини керування маршрутизатора, розгорнутого лише один-два роки тому. Ці тенденції стали каталізатором двох інновацій:

• відкритий інтерфейс між площиною керування та даних, такий як інтерфейс ForCES (Forwarding and Control Element Separation), стандартизований Інженерною групою Інтернету (IETF), та інтерфейс Netlink для пересилання пакетів на рівні ядра функціональність в Linux.

• логічно централізоване керування мережею, як це видно в архітектурах Routing Control PlatfoMP (RCP) і Soft-Router, а також у протоколі Path Computation Element (PCE) на IETF.

Ці інновації були зумовлені потребами галузі в технологіях керування маршрутизацією в мережі провайдера. [4]

Деякі ранні пропозиції щодо розділення площин даних і керування також надходили з академічних кіл, як у мережах AMT, так і в активних мережах.

Порівняно з попередніми дослідженнями активних мереж, ці проекти були зосереджені на нагальних проблемах управління мережею, з наголосом на: інноваціях мережевих адміністраторів і для них (а не кінцевих користувачів і дослідників); програмованість у площині керування (а не площині даних); а також видимість і контроль у всій мережі (а не конфігурація на рівні пристрою).

Програми для керування мережею включали вибір кращих мережевих шляхів на основі поточного навантаження на трафік, мінімізацію тимчасових збоїв під час запланованих змін маршрутизації, надання клієнтським мережам більшого контролю над потоком трафіку та перенаправлення або відкидання трафіку ймовірних атак. Декілька додатків керування працювали в оперативних мережах провайдерів Інтернету з використанням застарілих маршрутизаторів, включаючи точку керування інтелектуальною службою маршрутизації (IRSCP), розгорнуту для надання додаткових послуг клієнтам віртуальної приватної мережі в магістральній мережі рівня 1 AT&T. Незважаючи на те, що більшість робіт у цей час була зосереджена на управлінні маршрутизацією в межах одного провайдера, деякі роботи також пропонували способи забезпечення гнучкого контролю маршрутів у кількох адміністративних доменах.

Перенесення функціональних можливостей керування з мережевого обладнання на окремі сервери мало сенс, оскільки керування мережею, за визначенням, є діяльністю всієї мережі. Логічно централізовані контролери маршрутизації стали можливими завдяки появі програмного забезпечення маршрутизації з відкритим вихідним кодом, яке знизило бар’єр для створення прототипних реалізацій. Удосконалення серверних технологій означало, що єдиний стандартний сервер міг зберігати всі дані про стан маршрутизації та обчислювати всі рішення щодо маршрутизації для великої мережі провайдера. Це, у свою чергу, створило прості стратегії первинної резервної реплікації, де резервні сервери зберігають той самий стан і виконують ті самі обчислення, що й основний сервер, для забезпечення надійності контролера.

Початкові спроби відокремити площини управління та даних були відносно прагматичними, але вони являли собою значний концептуальний відхід затруднене поступове розгортання. Замість того, щоб чекати на появу нових відкритих API, RCP використовував існуючий стандартний протокол контрольної площини (протокол межового шлюзу) для встановлення записів таблиці пересилання в застарілих маршрутизаторах, унеможливлюючи негайне розгортання. Open-Flow також зіткнувся з подібними проблемами та обмеженнями зворотної сумісності: зокрема,

початкова специфікація Open-Flow покладалася на зворотну сумісність із апаратними можливостями стандартних комутаторів. [5]

Логічно централізовані контролери маршрутів зіткнулися з проблемами, пов'язаними з розподіленим управлінням станом. Логічно централізований контролер має бути реплікований, щоб впоратися з відмовою контролера, але реплікація створює потенціал для неузгодженого стану в репліках. Дослідники розглядали ймовірні сценарії відмови та вимоги до узгодженості. Принаймні у випадку контролю маршрутизації реплікам контролерів не потрібен загальний протокол управління станом, оскільки кожна репліка зрештою обчислювала б однакові маршрути (після вивчення тієї самої топології та інформації про маршрутизацію) і тимчасові збої під час конвергенції протоколу маршрутизації були прийнятними навіть із застарілими протоколами.

Для кращої масштабованості кожен екземпляр контролера може відповідати за окрему частину топології. Потім ці екземпляри контролера можуть обмінюватися інформацією про маршрутізацію один з одним, щоб забезпечити узгоджені рішення. Проблеми побудови розподілених контролерів знову виникнуть через кілька років у контексті розподілених контролерів програмно-конфігурованих мереж. Розподілені контролери ПКМ стикаються з більш загальнішою проблемою підтримки довільних додатків контролерів, що вимагає більш складних рішень для розподіленого управління станом.

Коли були запропоновані ці нові архітектури, критики сприйняли їх зі здоровим скептицизмом, часто палко стверджуючи, що логічно централізоване керування маршрутом порушить «розподіл долі», оскільки контролер може вийти з ладу незалежно від пристроїв, відповідальних за пересилання трафіку. Багато мережевих операторів і дослідників вважали відокремлення площини керування й даних за своєю суттю поганою ідеєю, оскільки спочатку не було чіткого визначення того, як ці мережі продовжуватимуть працювати правильно, якщо контролер відмовить.

Скептики також стурбовані тим, що логічно централізоване керування відійшло від концептуально простої моделі досягнення розподіленого консенсусу маршрутизаторами, де всі вони (зрештою) мають спільний погляд на стан мережі

(наприклад, через затоплення). У логічно централізованому управлінні кожен маршрутизатор має лише локальне уявлення про результат процесу вибору маршруту.

Фактично, на той час, коли почали запроваджувати ці проекти, навіть традиційні рішення розподіленої маршрутизації вже порушували ці принципи.

Переміщення логіки пересилання пакетів в апаратне забезпечення означало, що програмне забезпечення рівня керування маршрутизатора може вийти з ладу незалежно від рівня даних. Подібним чином протоколи розподіленої маршрутизації використовують методи масштабування, такі як зони OSPF і відбивачі маршрутів BGP, де маршрутизатори в одному регіоні мережі мали обмежену видимість інформації про маршрутизацію в інших регіонах. Як я описав в наступному розділі, поділ площини керування та даних дещо парадоксальним чином дозволив дослідникам більш чітко подумати про розподілене керування станом: роз'єднання площини керування та даних уповільнило появу рівня управління станом, який підтримує послідовність перегляд стану мережі.

Домінуючі постачальники обладнання не мали стимулів приймати стандартні API площини даних, такі як ForCES, оскільки відкриті API дозволили б новим учасникам вийти на ринок. Виникла необхідність покладатися на існуючі протоколи маршрутизації для керування площиною даних, що наклало значні обмеження на діапазон додатків, які могли б підтримувати програмовані контролери.

Звичайні протоколи IP-маршрутизації обчислюють маршрути для блоків IP-адрес призначення, замість того, щоб надавати ширший спектр функцій (наприклад, відкидання, лавинну передачу або модифікацію пакетів) на основі ширшого діапазону заголовка полів (наприклад, MAC- та IP-адреси). , номера портів TCP і UDP), як це робить OpenFlow. Зрештою, хоча галузеві прототипи та спроби стандартизації досягли певного прогресу, широкого впровадження так і не вдалося досягти.

Щоб розширити уявлення про розділення рівня керування та даних, дослідники почали шукати чисті архітектури для логічно централізованого керування. Проект 4D захищав чотири основні рівні: площину даних (для обробки пакетів на основі конфігурованих правил), площину виявлення (для збору вимірювань топології та

трафіку), площину поширення (для встановлення правил обробки пакетів), і площину прийняття рішень (складається з логічно централізованих контролерів, які перетворюють цілі мережевого рівня в стан обробки пакетів).

Кілька груп приступили до проектування та створення систем, які застосували цей підхід високого рівня до нових програм інфраструктури, а також наявність окремого державного фінансування для великомасштабного «інструментального обладнання», яке раніше було зарезервовано для інших дисциплін для створення дорогої спільної інфраструктури, такої як колайдери та телескопи. Результатом цього ентузіазму стало створення Глобального середовища для мережевих інновацій (GENI) з проектним офісом GENI, що фінансується NSF, і програмою ЄС FIRE. Критики цих зусиль, зосереджених на інфраструктурі, зазначали, що ці великі інвестиції в інфраструктуру не супроводжувалися добре продуманими ідеями щодо її використання. У розпал цього група дослідників зі Стенфорда створила програму «Чистий аркуш» і зосередилася на експериментах у більш локальному та доступному масштабі: мережі кампусів.

До появи OpenFlow ідеї, що лежали в основі ПКМ, стикалися з протиріччям між баченням повністю програмованих мереж і прагматизмом, який уможливив би розгортання в реальному світі. OpenFlow встановив баланс між цими двома цілями, забезпечивши більше функцій, ніж попередні контролери маршрутів, і побудувавши існуюче апаратне забезпечення комутаторів за рахунок збільшення використання чіпсетів торгового кремнію в комутаторах загального призначення.

Незважаючи на те, що використання існуючого апаратного забезпечення комутатора дещо обмежувало гнучкість, OpenFlow майже одразу можна було розгорнути, що дозволило руху ПКМ бути прагматичним і сміливим. Після створення OpenFlow API швидко послідував дизайн платформ контролерів, таких як NOX, що дозволило створити багато нових програм керування. [6]

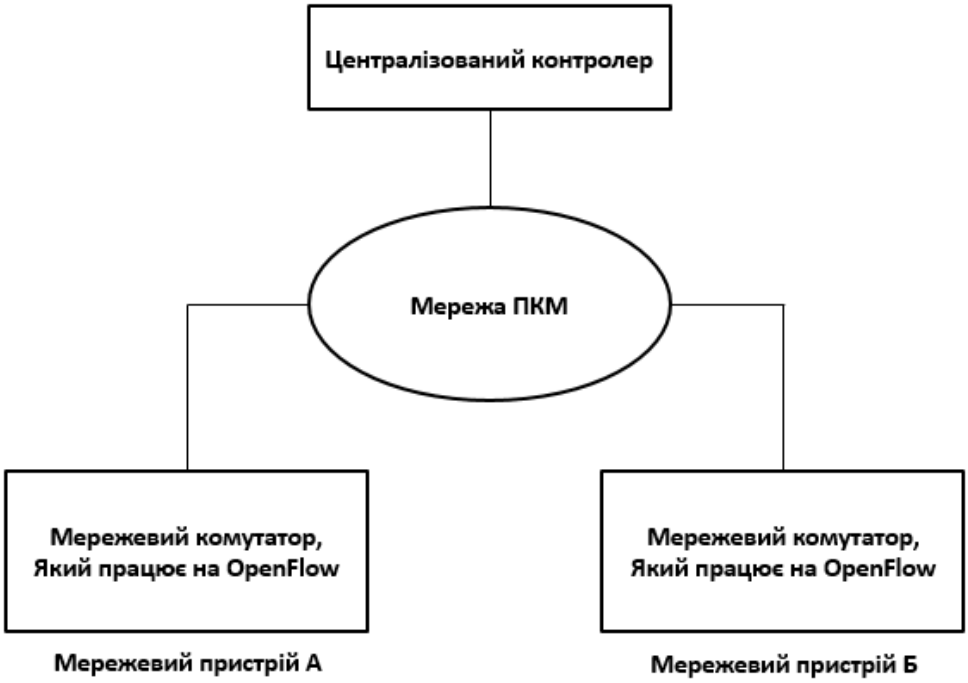

Рис. 1.1. Комутатори OpenFlow в мережі ПКМ

Комутатор OpenFlow (Рис. 1.1.) має таблицю правил обробки пакетів, де кожне правило має шаблон (який збігається з бітами в заголовку пакета), список дій (наприклад, скинути, затопити, переслати певний інтерфейс, змінити поле заголовка або надіслати пакет до контролера), набір лічильників (для відстеження кількості байтів і пакетів) і пріоритет (для усунення неоднозначності між правилами з шаблонами, що накладаються). Отримавши пакет, комутатор OpenFlow визначає правило відповідності з найвищим пріоритетом, виконує відповідні дії та збільшує лічильники. [7]

Можливо, визначальною особливістю OpenFlow є його впровадження в промисловості, особливо в порівнянні з його інтелектуальними попередниками. Цей успіх можна пояснити ідеальним вдосконаленням умов між постачальниками обладнання, розробниками чіпсетів, мережевими операторами та дослідниками мереж. До появи OpenFlow постачальники чіпсетів, наприклад Broadcom, уже почали відкривати свої API, щоб дозволити програмістам контролювати певну поведінку пересилання. Рішення відкрити чіпсет стало необхідним поштовхом для галузі, яка

вже вимагала більшого контролю над мережевими пристроями. Доступність цих наборів мікросхем також дозволила значно ширшому колу компаній створювати комутатори, не несучи значних витрат на проектування та виготовлення власного апаратного забезпечення площини даних.

Початковий протокол OpenFlow стандартизував модель площини даних і API площини керування, спираючись на технологію, яка вже підтримується. Зокрема, оскільки мережеві комутатори вже підтримували детальний контроль доступу та моніторинг потоку, увімкнути початковий набір можливостей OpenFlow на комутаторі було так само просто, як виконати оновлення мікропрограми — постачальникам не потрібно було оновлювати апаратне забезпечення, щоб зробити свої перемикає функцію OpenFlow.

Початковим цільовим сценарієм розгортання OpenFlow були кампусні мережі, що задовольняли потреби спільноти мережевих дослідників, яка активно шукала способи проведення експериментальної роботи над мережевими архітектурами «з чистого аркуша» в умовах, зручних для досліджень. Наприкінці 2000-х років група OpenFlow зі Стенфорда очолила зусилля з розгортання випробувальних стендів OpenFlow у багатьох кампусах і демонстрації можливостей протоколу як в одній мережі кампусу, так і в магістральній мережі, що охоплює кілька кампусів.

Коли реальні випадки використання ПКМ матеріалізувалися в цих кампусах, OpenFlow почав закріплюватися в інших сферах, таких як мережі центрів обробки даних, де існувала явна потреба керувати мережевим трафіком у великих масштабах. У центрах обробки даних витрати на наймання інженерів для написання складних програм керування для роботи з великою кількістю стандартних комутаторів виявилися рентабельнішими, ніж подальше придбання закритих власних комутаторів, які не могли підтримувати нові функції без значної участі з постачальниками обладнання. Коли постачальники почали конкурувати за продаж як серверів, так і комутаторів для центрів обробки даних, багато менших гравців на ринку мережевого обладнання скористалися можливістю конкурувати з відомими постачальниками маршрутизаторів і комутаторів, підтримуючи нові можливості, такі як OpenFlow.

Незважаючи на те, що OpenFlow втілив багато принципів із попередніх робіт із розділення рівня керування та даних, розвиток OpenFlow запропонував кілька додаткових інтелектуальних внесків:

• Узагальнення мережевих пристроїв і функцій. Попередня робота з управління маршрутами зосереджена в основному на зіставленні трафіку за IP-префіксом призначення. Навпаки, правила OpenFlow можуть визначати поведінку пересилання в потоках трафіку на основі будь-якого набору з 13 різних заголовків пакетів. Таким чином, OpenFlow концептуально об'єднав багато різних типів мережевих пристроїв, які відрізняються лише тим, яким полям заголовків вони відповідають і які дії вони виконують. Маршрутизатор збігається за префіксом IP-адреси призначення та пересилає посилання, тоді як комутатор збігається з MAC-адресою джерела (для вивчення MAC-адреси) та MAC-адресою призначення (для пересилання) і або передає, або пересилає одне посилання. Транслятори мережевих адрес і брандмауери збігаються з п'ятьма кортежами (IP-адреси джерела та призначення, номери портів і транспортний протокол) і або переписують поля адреси та порту, або відкидають небажаний трафік. OpenFlow також узагальнив правило- методи інсталяції, які дозволяють будь-що, починаючи від проактивної інсталяції грубих правил (тобто з «підстановними знаками» для багатьох полів заголовків) до реактивної інсталяції тонких правил, залежно від програми. Проте OpenFlow не пропонує підтримку площини даних для глибокої перевірки пакетів або повторної збірки з'єднання; як такий, OpenFlow сам по собі не може ефективно забезпечити складну функціональність проміжного блоку.

• Бачення мережевої операційної системи. На відміну від попередніх досліджень активних мереж, які пропонували операційну систему вузла, робота над OpenFlow привела до поняття мережевої операційної системи. Мережна операційна система — це програмне забезпечення, яке абстрагує установку стану в мережевих комутаторах від логіки та програм, які керують поведінкою мережі.

• Методи управління розподіленим станом. Розділення площини управління та даних створює нові виклики щодо управління мережею. Запуск кількох контролерів має вирішальне значення для масштабованості, надійності та продуктивності, але ці

репліки повинні працювати разом, щоб діяти як єдиний логічно централізований контролер. Попередня робота над контролерами розподіленого маршруту розглядала ці проблеми лише у вузькому контексті обчислення маршруту.

Для підтримки довільних додатків контролерів у роботі над контролером Onix була введена ідея інформаційної бази мережі — представлення топології мережі та іншого стану керування, спільного для всіх копій контролера. Onix також включив минулу роботу в розподілені системи, щоб задовольнити вимоги щодо узгодженості стану та довговічності. Наприклад, Onix має транзакційну постійну базу даних, що підтримується реплікованим кінцевим автоматом для повільної зміни стану мережі, а також розподілену хеш-таблицю в пам’яті для швидкої зміни стану з меншими вимогами до узгодженості. Зовсім недавно система ONOS пропонує контролер з відкритим вихідним кодом з аналогічною функціональністю, використовуючи існуюче програмне забезпечення з відкритим кодом для підтримки узгодженості в розподіленому стані та надання бази даних топології мережі додаткам контролера.

Один з міфів щодо програмно-конфігурованих мереж полягає в тому, що перший пакет кожного потоку трафіку має надходити до контролера для обробки. Дійсно, деякі ранні системи, такі як Ethane, працювали таким чином, оскільки вони були розроблені для підтримки дрібнозернистих політик у невеликих мережах. Насправді ПКМ загалом і OpenFlow зокрема не накладають жодних припущень щодо деталізації правил чи обробляє контролер будь-який трафік даних. Деякі програми ПКМ реагують лише на зміни топології та грубу статистику трафіку та рідко оновлюють правила у відповідь на збої зв’язку чи перевантаження мережі. Інші додатки можуть надсилати перший пакет деякого більшого сукупного трафіку до контролера, але не пакет із кожного з’єднання TCP або UDP.

Другий міф навколо ПКМ полягає в тому, що контролер має бути фізично централізованим. Фактично, Onix і ONOS демонструють, що контролери програмно-конфігурованих мереж можна — і потрібно — поширювати. Глобальне розгортання ПКМ, як і в приватній магістралі Google, має багато контролерів, розкиданих по всій мережі.

Нарешті, поширена помилкова думка полягає в тому, що ПКМ і OpenFlow еквівалентні; насправді OpenFlow є лише одним (широко популярним) екземпляром принципів ПКМ. Різні API можуть бути використані для керування пересиланням у всій мережі; попередню роботу, яка була зосереджена на маршрутизації (з використанням BGP як API), можна вважати, наприклад, одним екземпляром ПКМ, а архітектури від різних постачальників (наприклад, Cisco ONE та JunOS SDK) представляють інші екземпляри ПКМ, які відрізняються від OpenFlow.

Незважаючи на початкове хвилювання навколо програмно-конфігурованих мереж, варто визнати, що ПКМ — це лише інструмент, який забезпечує інновації в управлінні мережею. ПКМ не диктує, як цей контроль має бути розроблений, і не вирішує жодної конкретної проблеми. Навпаки, дослідники та мережеві оператори тепер мають у своєму розпорядженні платформу, яка допоможе вирішити давні проблеми в управлінні їхніми мережами та розгортанні нових послуг.

Зрештою, успіх і впровадження ПКМ залежить від того, чи можна його використовувати для вирішення нагальних проблем у мережі, які було важко або неможливо вирішити за допомогою попередніх протоколів. Програмно-конфігурована мережа вже виявилася корисним для вирішення проблем, пов’язаних з віртуалізацією мережі, як ми описуємо в наступному розділі.

1.3. Аналіз ефективності сучасних програмно-конфігурованих мереж

У цьому розділі я розглядаю віртуалізацію мережі та видатний ранній «випадок використання» ПКМ. Віртуалізація мережі представляє собою абстракцію мережі, яка відокремлена від основного фізичного обладнання. Віртуалізація мережі дозволяє працювати декільком віртуальним мережам через спільну інфраструктуру, і кожна віртуальна мережа може мати набагато простішу (більш абстрактну) топологію, ніж базова фізична мережа. Наприклад, віртуальна локальна мережа (VLAN) створює ілюзію єдиної локальної мережі, що охоплює кілька фізичних підмереж, і кілька VLAN можуть працювати через ту саму колекцію комутаторів і маршрутизаторів.

Хоча віртуалізація мережі концептуально не залежить від ПКМ, останніми роками зв’язок між цими двома технологіями став набагато тіснішим.

При обговоренні віртуалізації мережі існує три застереження. По-перше, повна історія мережі віртуалізація потребує окремого опитування; я зосереджуюсь на розробках мережевої віртуалізації, які безпосередньо стосуються інновацій у програмованих мережах. По-друге, хоча віртуалізація мережі набула популярності як приклад використання програмно-конфігурованих мереж, ця концепція передує сучасній ПКМ і фактично розвивалася паралельно з програмованими мережами. Ці дві технології фактично тісно пов’язані: програмовані мережі часто передбачають механізми спільного використання інфраструктури (між кількома орендарями в центрі обробки даних, адміністративними групами в кампусі або експериментами в об’єкті) і підтримують логічні топології мережі, які відрізняються від фізичних мереж, обидві з яких є центральними принципами віртуалізації мережі. Нарешті, зазначається, що точне визначення «віртуалізації мережі» є невловимим, і експерти, природно, не погоджуються щодо деяких з механізмів, які ми обговорюємо (наприклад, нарізка), представляють форми віртуалізації мережі. У цьому розділі я визначаю сферу віртуалізації мережі, яка включає будь-яку технологію, яка полегшує розміщення віртуальної мережі на базовій фізичній мережевій інфраструктурі.

Протягом багатьох років мережеве обладнання підтримувало створення віртуальних мереж у формі VLAN і віртуальних приватних мереж. Однак лише мережеві адміністратори могли створювати ці віртуальні мережі, і ці віртуальні мережі були обмежені запуском існуючих мережевих протоколів. Таким чином, поступове впровадження нових технологій виявилося складним. Замість цього дослідники та практики вдалися до накладених мереж, де невеликий набір оновлених вузлів використовує тунелі для формування власної топології поверх застарілої мережі. У накладеній мережі оновлені вузли запускають власний протокол рівня керування та спрямовують трафік даних (і повідомлення рівня керування) один до одного шляхом інкапсуляції пакетів, надсилання їх через застарілу мережу та декапсуляції на іншому кінці, де Mbone (для багатоадресної передачі), 6bone (для IPv6) і X-Bone були яскравими ранніми прикладами. [8]

Ці перші накладні мережі складалися з виділених вузлів, які керували спеціальними протоколами, в надії стимулювати впровадження запропонованих удосконалень мережевої інфраструктури. Невдовзі поняття накладених мереж розширилося й охопило будь-який кінцевий комп'ютер, який встановлює та запускає спеціальну програму, завдяки успіху ранніх однорангових програм для обміну файлами (наприклад, Napster і Gnutella). На додаток до значних досліджень однорангових протоколів, дослідницьке співтовариство мереж відновило дослідження використання накладених мереж як способу покращення мережевої інфраструктури, наприклад, робота над Resilient Overlay Networks, де невелика колекція - хости, що спілкуються, утворюють оверлей, який швидко реагує на збої мережі та проблеми з продуктивністю.

На відміну від активних мереж, накладені мережі не потребують спеціальної підтримки з боку мережевого обладнання чи співпраці з боку постачальників послуг Інтернету.Їх набагато легше розгортати. Щоб зменшити бар'єр для експериментів із накладеними мережами, дослідники почали будувати віртуалізовані експериментальні інфраструктури, такі як PlanetLab, які дозволили кільком дослідникам запускати власні накладені мережі на спільній та розподіленій колекції хостів. Цікаво, що сама PlanetLab була формою активної мережі «програмованого маршрутизатора/комутатора», але використовувала набір серверів, а не мережевих вузлів, і пропонувала програмістам звичайну операційну систему (тобто Linux). Ці конструктивні рішення підштовхнули до прийняття спільнотою дослідників розподілених систем, що призвело до значного підвищення ролі експериментів із прототипами систем у цій спільноті.

Завдяки успіху спільних експериментальних платформ у сприянні дослідженню експериментальних систем дослідники почали виступати за створення спільних експериментальних платформ, які сприяли підтримці віртуальних топологій, які можуть запускати спеціальні протоколи в базовій мережі, щоб реалістичні експерименти проводилися паралельно з робочим трафіком. У цій моделі саме мережеве обладнання «розміщує» віртуальну топологію, повертаючись до ранньої архітектури Tempest, де кілька віртуальних мереж АМТ могли співіснувати на одному

наборі фізичних комутаторів. Архітектура Tempest навіть дозволяла визначати поведінку переадресації комутаторів за допомогою програмних контролерів, передвіщаючи роботу над керуванням і розділенням площини даних.

Ініціатива GENI підняла ідею віртуалізованої та програмованої мережевої інфраструктури до набагато більшого масштабу, побудувавши національну експериментальну інфраструктуру для досліджень мережевих і розподілених систем. Виходячи за межі експериментальної інфраструктури, деякі дослідники стверджували, що віртуалізація мережі може стати основою майбутнього Інтернету, який дозволить одночасно існувати кільком мережевим архітектурам (кожна оптимізована для різних додатків чи вимог, або керовані різними бізнес-об'єктами), і розвиваються з часом, щоб задовольнити мінливі потреби.

Віртуалізація мережі (абстракція фізичної мережі в термінах логічної мережі) явно не потребує програмно-конфігурованих мереж. Подібним чином ПКМ (відокремлення логічно централізованої площини керування від базової площини даних) не передбачає віртуалізації мережі. Цікаво, що виник симбіоз між мережевою віртуалізацією та ПКМ, який почав каталізувати кілька нових напрямків досліджень. ПКМ і віртуалізація мережі пов'язані трьома основними способами:

• ПКМ як сприятлива технологія для віртуалізації мережі. Хмарні обчислення зробили мережеву віртуалізацію помітною, оскільки хмарним провайдерам потрібен спосіб дозволити кільком клієнтам (або «орендарям») спільно використовувати одну мережеву інфраструктуру. Платформа мережевої віртуалізації Nicira (NVP) пропонує цю абстракцію без потреби будь-якої підтримки з боку основного мережевого обладнання. Рішення полягає у використанні перекритої мережі, щоб надати кожному орендарю абстракцію єдиного комутатора, який з'єднує всі його віртуальні машини. Проте, на відміну від попередньої роботи над накладеними мережами, кожен накладений вузол фактично є розширенням фізичної мережі — програмним комутатором (як Open vSwitch), який інкапсулює трафік, призначений віртуальним машинам, що працюють на інших серверах. Логічно централізований контролер встановлює правила в ці віртуальні комутатори, щоб керувати інкапсуляцією пакетів, і оновлює ці правила, коли віртуальні машини переміщуються в нові місця.

• Віртуалізація мережі для оцінки та тестування програмно-конфігурованих мереж. Можливість відокремити контрольну програму ПКМ від базової площини даних дає змогу тестувати та оцінювати контрольні програми ПКМ у віртуальному середовищі до того, як програму буде розгорнуто в робочій мережі. Mininet використовує віртуалізацію на основі процесів для запуску кількох віртуальних комутаторів OpenFlow, кінцевих хостів і контролерів ПКМ — кожен як один процес на одній фізичній (або віртуальній) машині. Використання віртуалізації на основі процесів дозволяє Mininet імітувати мережу з сотнями хостів і комутаторів на одній машині. У такому середовищі дослідник або оператор мережі може розробити логіку керування та легко перевірити її на повномасштабній емуляції площини виробничих даних; після того, як рівень керування оцінено, протестовано та налагоджено, його можна розгорнути в реальній виробничій мережі.

• Віртуалізація (нарізка) програмно-конфігурованих мереж. У звичайних мережах віртуалізація маршрутизатора або комутатора є складною, оскільки кожен віртуальний компонент повинен запускати власний екземпляр програмного забезпечення рівня керування. Навпаки, віртуалізація «тупого» комутатора ПКМ набагато простіше. Система FlowVisor дозволяє кампусу підтримувати випробувальний стенд для мережевих досліджень поверх того самого фізичного обладнання, яке переносить виробничий трафік. Основна ідея полягає в тому, щоб розділити простір потоку трафіку на «зрізи» (концепція, введена в попередній роботі над PlanetLab, де кожен зріз має частку мережевих ресурсів і керується іншим контролером ПКМ. FlowVisor працює як гіпервізор, спілкуючись з OpenFlow і з кожним із контролерів ПКМ і базовими комутаторами.

Люди часто посилаються на передбачувані «переваги ПКМ», наприклад, амортизацію вартості фізичних ресурсів або динамічну зміну конфігурації мереж у багатокористувацьких середовищах, які фактично походять від віртуалізації мережі. Незважаючи на те, що ПКМ полегшує мережеву віртуалізацію і, таким чином, може полегшити реалізацію деяких із цих функцій, важливо визнати, що можливості, які пропонує ПКМ (тобто розділення площини даних і керування, абстракції для стану розподіленої мережі), безпосередньо не надавати ці переваги.

Незважаючи на те, що Програмно-конфігурована мережа досягла певних практичних успіхів і, безсумнівно, пропонує такі необхідні технології для підтримки конкретного варіанту використання мережевої віртуалізації, потрібна додаткова робота як для вдосконалення існуючої інфраструктури, так і для вивчення потенціалу ПКМ для вирішення проблем для набагато ширшого кола проблем у випадках використання. Хоча перші розгортання ПКМ були зосереджені на університетських кампусах, центрах обробки даних і приватних магістралях, я досліджую програми та розширення ПКМ для більш широкого діапазону мережевих параметрів, включаючи домашні мережі, корпоративні мережі. мережі, точки обміну Інтернетом, базові мережі стільникового зв'язку, мережі радіодоступу стільникового зв'язку та WiFi, а також спільне керування додатками кінцевого хоста та мережею. Кожне з цих умов відкриває багато нових можливостей і викликів, які спільнота досліджуватиме в наступні роки.

1.4. Дослідження методів підвищення ефективності сучасних ПКМ

Загальна структура мережі є складною структурою, яку слід розглядати як єдину гетерогенну мережу, що складається з кількох різних типів ресурсів і, таким чином, керувати як єдину сутність замість того, щоб розглядати рівні окремо та індивідуально. З цією метою слід визначити ефективні механізми для вирішення складних цілей HetNets з точки зору фізичних, функціональних аспектів і аспектів безпеки.

Необхідність визначення та впровадження інновацій призначено архітектуру для вирішення поточних обмежень мережевих інфраструктур. Це буде досягнуто шляхом конвергенції сучасних широкосмугових бездротових рішень з оптичною технологією в доменах доступу та метро/основному. Оптичні мережі в доменах доступу та метро забезпечують високу пропускну здатність і надійну підтримку послуг; однак вони вимагають масового розгортання волоконно-оптичної інфраструктури для підключення кількох абонентів у будинках або на підприємствах (наприклад, парадигма Fiber To The Home – FTTH). Таким чином, впровадження

оптичної технології, загалом, збільшує необхідні інвестиції та відповідні капітальні витрати. З іншого боку, технології бездротового доступу вимагають менше розгортання інфраструктури, хоча вони здатні забезпечити гнучке та повсюдне підключення. Однак через обмежену пропускну здатність рішення автономного бездротового доступу є «проблематичним» щодо підтримки додатків, які потребують пропускної здатності. Використання взаємодоповнюючих переваг обох технологій може забезпечити гнучке та життєздатне рішення доступу, розгорнувши гібридну бездротову оптичну мережу доступу. Конвергентна архітектура буде розширена технологією ПКМ для контролю базових мережевих компонентів і об'єктів. Будуть визначені та конкретизовані елементи гібридної оптико-бездротової мережі. Крім того, вони будуть перетворені на «обчислювальні еквівалентні» елементи з метою моделей і контролерів програмно-конфігурованих мереж.

Крім специфікації конвергентної гібридної оптико-бездротової архітектури, яка необхідна для рівномірного управління всіма ресурсами, необхідно сприяти тому, що базові компоненти мережі стануть програмованим, гнучким і динамічним «обчислювальним еквівалентом». З самого початку, протягом життєвого циклу розгортання HetNets, апаратні абстракції та моделі повинні бути використані, щоб увімкнути програмований інтерфейс для конфігурації стану апаратного забезпечення, включаючи рівні представлення обладнання (HPL) і рівні апаратного інтерфейсу (HIL). Оптичні та бездротові компоненти та елементи будуть вдосконалені до когнітивних програмованих пристроїв, де їхні характеристики та конфігурація будуть оптимізовані з точки зору розподілу ресурсів, представлення інтерфейсу та функціональності. Фізичні характеристики як оптичних, так і бездротових мережевих пристроїв будуть доступні для оптимізації залежно від динаміки мережі (користувачі, трафік, доступність спектру, споживання енергії та характеристики користувача). З цією метою ефективне використання комутаторів, маршрутизаторів, базових станцій і пристроїв M2M дозволить реалізувати мережі нового покоління з підтримкою 5G високої пропускної здатності в реальних сценаріях.

Основні можливості технології ПКМ слід використовувати в контексті HetNets, шляхом проектування та впровадження передових моделей і контролерів ПКМ для

інноваційних архітектур. Контролери вирішуватимуть дві основні проблеми програмного забезпечення мережі 5G:

а) ефективний і оперативний контроль потоку неоднорідних ресурсів і послуг,

б) уніфікований контроль і управління в хмарі, включаючи потребу в ефективній обробці збоїв і відновленнях у ПКМ через архітектуру 5G.

Розділення площини управління та даних забезпечить безперебійну роботу гібридних оптико-бездротових пристроїв. Інтелектуальні шлюзи з оптичним і бездротовим інтерфейсами будуть розгорнуті та ефективно використані для обробки потоків трафіку 5G від мобільних користувачів до оптичного зворотного зв'язку. Крім того, функціональні можливості на основі ПКМ будуть розроблені на рівні маршрутизації, враховуючи оптичну транспортну мережу високої пропускної здатності на основі ПКМ. Вони дозволять повністю маніпулювати фізичними фотонними характеристиками, забезпечуючи гнучку та динамічну оптичну передачу. Крім того, будуть застосовані механізми відновлення в частині багаторазових компонентів, що дозволить швидко та ефективно відновлювати наявні збої. Відбудеться визначення метрик і запитів для фіксації та обробки змінних у часі подій. Крім того, гібридна архітектура повинна продемонструвати потенціал парадигми ПКМ, щоб зробити 5G придатним для всіх типів трафіку даних, включаючи M2M і потоки трафіку «людина-машина» (H2M). Докладніше слід уточнити, як система стільникового радіодоступу (RAN) і мережа збору даних машинного типу (MTC) можуть бути динамічно інтегровані в 5G RAN на основі програмно-конфігурованих мереж з MTC і зв'язком людського типу (HTC). [9]

Необхідно розробити та встановити методологію проектування, впровадження та підтримки програмних компонентів, бібліотек та API для ефективного управління контролерами ПКМ. Розроблені бібліотеки забезпечуватимуть взаємозв'язок між 5G та оптичними рівнями, підтримуючи співіснування кількох мережевих доменів. Вони також підтримуватимуть когнітивну інженерію трафіку в компонентах мережі M2C. Програмні модулі підтримуватимуть динамічне оновлення мережевих/сервісних архітектур, а також оптимізацію витрат і процесів, забезпечуючи програмне забезпечення мережі, кероване додатками. Вони також нададуть прозорий рівень

інструментів програмування, який підтримуватиме визначення абстракцій високого рівня та розробку однорівневих модулів програмування, що забезпечить уніфікований протокол оркестровки керування для будь-якого фону мережі (наприклад, одна процедура керування буде застосована в бездротових і оптичні мережі з точки зору адміністраторів/розробників). Під час цього процесу необхідно спиратися на загальновизнані принципи традиційної розробки програмного забезпечення, такі як відстеження вимог, специфікація дизайну та модульна реалізація. Зокрема, слід полегшити повторне використання шляхом відокремлення апаратно-специфічних частин від апаратно-незалежних і забезпечення чітко визначених інтерфейсів між мережевими рівнями.

Включення уніфікованого управління із застосуванням сучасних схем і абстракцій розподілу для надання віртуальних ресурсів, послуг, функцій, апаратного забезпечення, з особливим фокусом і інтересом до контролю та оркестровки, зокрема у федеративних доменах (наприклад, кілька операторів, клієнтські мережі та центри обробки даних). Питання сумісності будуть вирішені шляхом координації кількох доменів керування ПКМ з акцентом на нові стандартизовані оркестратори. Інтеграція мережевих можливостей у гетерогенних середовищах, моніторинг фізичних і віртуальних мережевих ресурсів у режимі реального часу та автоматизоване високомасштабне забезпечення безпеки — це деякі ключові риси розширеної оркестровки віртуалізації. Необхідно розвинути проактивне та реактивне прийняття рішень у площині управління. Передові методи віртуалізації будуть розроблені та впроваджені, щоб зробити життєздатним використання мережевих ресурсів декількома орендарями. Слід приділяти особливу увагу розробці передових методів розподілу для оптичних доменів і доменів 5G, що дозволяє одночасно використовувати обидва типи мережевих ресурсів в цілому. Орендарям, кінцевим користувачам, провайдерам і зацікавленим сторонам буде доступна відкрита та захищена платформа для функціонування та реалізації сегментів мережі в режимі реального часу, дотримуючись, таким чином, концепції «нульової затримки» при створенні нових мережевих послуг або програм.

Існує важлива вимога розробити адаптивні механізми обробки та стратегії інженерного трафіку для підтримки операцій управління та контролю з високою пропускною спроможністю, низькою затримкою та оптимізацією спектру в базовій архітектурі мережі. Механізми моніторингу в реальному часі будуть розроблені та розподілені по гібридній архітектурі. Ці механізми відстежуватимуть усі потоки трафіку, сервіси, додатки та гарантії QoS від інтерфейсів з'єднання 5G (міні-базові станції, LTE-сумісний SDR та Evolved Node B – eNodeB). Будуть розроблені нові схеми та алгоритми розподілу пропускної здатності для полегшення розподілу пропускної здатності в архітектурі доступу 5G, приділяючи наголос справедливому та ефективному розподілу пропускної здатності у віртуалізованій мережі. У домені metro/core необхідно зосередитися на використанні функцій еластичності, пропонуючи визначення вужчої довжини хвилі. Методи балансування навантаження та пересилання трафіку будуть розроблені на рівні маршрутизації шляхом ефективного контролю фізичних характеристик пристроїв оптичної передачі. Необхідно вивчити та проаналізувати вдосконалені методи доступу OFDM (OFDMA). З огляду на те, що бездротові мережі 5G характеризуються неоднорідністю, гібридна архітектура і використовуватиме більш складні технології для використання спектру, мультидоступу, обробки сигналів і безпеки для підтримки взаємозв'язку ще більш різноманітного користувацького обладнання та пристроїв. Адаптивні механізми керування спектром будуть розроблені для забезпечення повної реконфігурації характеристик доступу до спектру базових станцій. Для підтримки прямого та непрямого доступу до шлюзів H2C і M2C або/або базових станцій слід вивчити розширені стратегії контролю фізичного доступу та доступу до середовища (MAC), щоб забезпечити надання високого рівня спектру в зв'язку M2M.

Енергоефективне управління контролюватиметься когнітивними бібліотеками ПКМ з урахуванням енергії, які дозволять повністю маніпулювати оптичною та бездротовою мережею сутності на основі умов руху. Відповідні бібліотеки підтримуватимуть оптимізовану генерацію коду, пропонуючи енергоефективні альтернативи для уникнення відходів. Механізми для вимірювання та оцінки споживання енергії, методи моделювання енергетичної поведінки гібридних

мережевих систем 5G і моделі для виявлення «запаху» поганої енергії є одними з цілей передових енергетичних схем. Механізми сплячого режиму та перемикання в сплячий режим будуть застосовані для всіх вузлів, щоб заощаджувати енергію, коли наявний трафік низький або навіть відсутній. Гібридна архітектура 5G забезпечить ефективні енергозберігаючі механізми для конвергентних оптичних терміналів 5G, дозволяючи перебувати в режимі сну та сну, коли трафік, що надходить із країв 5G, низький або зовсім відсутній. Необхідно розробити аналітичні моделі мінімізації потужності для підтримки низького енергоспоживання в оптичних і бездротових областях.

У контексті розробленої архітектури важливо розробляти, інтегрувати та впроваджувати інноваційні прототипи та платформи, щоб відповідати високим вимогам викликів 5G. Щоб забезпечити гібридну оптико-бездротову мережу доступу з високою пропускною здатністю, потрібне впровадження прототипу 5G гібридної оптично-бездротової оптичної мережі (ONU). Традиційні пристрої ONU просуваються до гібридних оптико-бездротових шлюзів на основі ПКМ, здатних обробляти потоки трафіку 5G і оптичні сигнали одночасно гладко та ефективно. Цей прототип підвищить продуктивність мережі в мережі доступу за рахунок збільшення пропускної здатності мережі, гнучкості функцій високого рівня та можливостей переднього оптичного бездротового пристрою/шлюзу. Крім того, дуже важливо створити платформу еластичної оптичної програмованої конфігурації для вирішення проблеми статичної модуляції довжини хвилі в поточних оптичних транспортних мережах. Зосереджуючись на метро/основному домені, відповідні зусилля розширять можливості оптичних мереж маршрутизації шляхом ефективного управління фотонними характеристиками на фізичному рівні. Сучасні мережі оптичної маршрутизації не здатні динамічно маніпулювати своїми фізичними характеристиками, наприклад, модуляції або швидкості передачі. Гібридна архітектура 5G закриє цю прогалину, інтегрувавши нову програмовану платформу в оптичний рівень для контролю та управління, використовуючи потужні бібліотеки програмного забезпечення та API, параметри передачі, функції контролю фізичного доступу та доступу до середовища (MAC), а також можливості комутації базових

транспондерів, маршрутизатори та пристрої додавання/виведення та вибору довжини хвилі. Нарешті, необхідно запровадити інноваційну інфраструктуру радіодоступу; Cloud-based RAN (C-RAN) із підтримкою МТС. Завдяки ефективному з'єднанню доменів МТС із стільниковими мережами C-RAN із підтримкою МТС використовуватиме динамічні хмарні контролери ПКМ для керування радіоінтерфейсом найсучасніших технологій 3GPP (LTE та LTE-A), щоб адекватно обробляти потоки трафіку, що походять від центрів обробки даних і доменів даних M2M або/або H2M.

1.5. Постановка задач дослідження

Вимоги безпеки ПКМ можуть відрізнятися від вимог класичної мережі через властиві їм характеристики та варіанти реалізації. Залежно від його фізичної реалізації, централізоване керування може надати зловмисникам окремий цінний актив, на відміну від більшої кількості автономних активів у розподіленому домені керування. Оскільки логічно централізовані контролери, імовірно будуть реалізовані розподіленим способом, вони можуть мати додаткові вразливості, пов'язані з реалізацією, які не видно у архітектурі програмно-конфігурованих мереж. Тобто архітектура моделює контролер ПКМ як єдину сутність, передбачаючи єдиний захищений сеанс між контролером і об'єктами площини даних або додатків, а фактична реалізація може вимагати кількох сеансів зв'язку через фізичний розподіл, кожен з яких вимагає надійної безпеки . Операторам необхідно усунути деякі загрози логічно централізованому контролеру шляхом розгортання контролерів ПКМ у своїх безпечних обчислювальних середовищах.

Виникає новий клас загроз, тому що програмно-конфігурована мережа пропонує програмний доступ до клієнтської площини контролера або об'єктів додатків. Ці клієнти, як правило, є окремими організаційними чи одиницями. Ця нова бізнес-модель пред'являє вимоги, яких немає в закритих адміністративних доменах, щодо захисту цілісності системи та сторонніх даних для забезпечення повної ізоляції

управління бізнесом і інформації про контроль в реальному часі одного об’єкта від усіх інших.

З іншого боку, функція програмування також надає можливості для підвищення рівня безпеки мереж. Наприклад, може бути можливим використання методів ПКМ для створення рішення безпеки рівня даних, яке здатне координувати як мережу, так і пристрої безпеки для виявлення та реагування на атаки більш гнучким способом. Однак реалізація нових функціональних можливостей безпеки площини даних не повинна досягатися за рахунок загальної цілісності та безпеки системи.

Ізоляція трафіку між орендарями є актуальною темою безпеки. У контексті ПКМ більше компонентів, які можуть впливати на ізоляцію, взаємодіючи більш динамічно, ніж у мережах без ПКМ. Як стандарти, так і операційна практика повинні гарантувати, що ізоляція не буде порушена.

Враховуючи взаємозв’язок різних компаній і організацій, який заохочує ПКМ, архітектура сильно керується поняттями доменів довіри з чітко визначеними межами. Уніфікована модель інтерфейсу допомагає цілісно думати про проблеми безпеки, тоді як жорсткі межі допомагають захистити решту мережі від довірених доменів із порушеною безпекою. Однак такі довірчі домени не можуть блокувати загрози, створені зловмисниками, які отримують доступ до довіреного домену ПКМ (в межах довірчої межі оператора), або які використовують слабкі місця в програмах або міждоменних інтерфейсах. Тому архітектура вимагає надійної автентифікації та надійної безпеки на всіх інтерфейсах. Не унікальним для ПКМ є той факт, що інсайдери становлять значну загрозу безпеці, а помилка оператора загрожує цілісності системи. Щоб вирішити цю проблему, архітектура повинна включати надійні функції керування ідентифікацією та обліковими даними, які захищають усі об’єкти та їхній пов’язаний стан.

Ці та інші фактори вказують на важливість аудитів для забезпечення роботи процесів належним чином. Може знадобитися моніторинг у реальному часі довіреною третьою стороною. Аудити в режимі реального часу можуть бути корисними, а журнали аудиту можуть знадобитися у маубутньому. Таким чином, важливо, щоб процес аудиту та самі журнали були захищені від підробки та

пошкодження. Реалізації повинні обмежувати доступ оператора та процесу до мінімальних авторизованих рівнів привілеїв, а також розподіляти вплив порушень, які можуть бути спричинені довіреними суб'єктами.

На основі власних критеріїв оператори можуть зменшити обмеження безпеки на певних інтерфейсах, наприклад, на фізично захищених портах керування на серверах. Важливо розуміти наслідки безпеки, пов'язані з таким вибором реалізації. Загалом безпека покращується, коли функціями безпеки та адміністрування можна керувати в масштабі з мінімальним втручанням людини протягом усього життєвого циклу.

Досвід показує складність модернізації можливостей безпеки в існуючі технології (DNS і BGP є яскравими прикладами). Однак інтерфейси та протоколи ПКМ розробляються у загальновизнаному контексті ескалації використання технічних і технологічних недоліків із дедалі серйознішими наслідками. Таким чином, критично важливо, щоб слабкі сторони, які раніше були усунені в архітектурах, не пов'язаних із ПКМ, не повторювалися під час створення структури ПКМ шляхом забезпечення безпеки мережевої архітектури за допомогою цілісного підходу до розробки протоколів та інтерфейсів. [10]

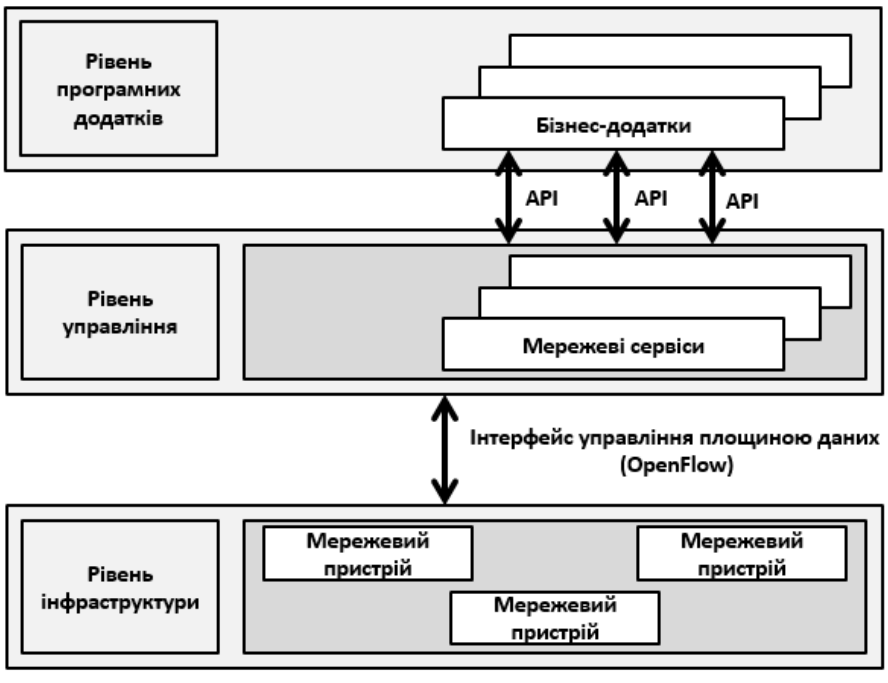

Рис. 1.2. Відокремлення рівнів мережі

Відокремлення рівнів керування та даних, що зображено на Рис. 1.2., заохочує еволюцію мережевої інфраструктури до масивів подібних блоків, кожен із передбачуваними, якщо не ідентичними, функціями, з усіма спеціалізованими функціями, що надаються або за межами домену ПКМ, або, за допомогою віртуальних мережевих функцій. Залишається побачити, наскільки цього можуть досягти навіть окремі оператори, а тим більше спільнота в цілому. У доступному для огляду майбутньому неоднорідність є фактом життя в мережі, який ПКМ повинен вирішити.

Таким чином, в сферу дії ПКМ може входити широкий спектр мережевих елементів. Теоретично можливо спонтанно встановити довільний мережевий елемент (МЕ) в межах довільного контролера ПКМ, ризикуючи несумісними можливостями, методами або протоколами. Насправді, мережеве планування апріорі гарантує, що на додаток до загальних протоколів МЕ і контролерів ПКМ спільно мають необхідний набір функцій і можливості керування.

Різні можливості МЕ також створюють проблеми для віртуалізації мережі, але це проблема планування обслуговування, а не проблема під час виконання. Під час виконання можуть виникати винятки між контролером та інфраструктурою через збої або обмеження продуктивності ресурсів або ємності, але винятки непідтримуваних можливостей ніколи не повинні виникати.

Необхідно, щоб базові МЕ надавали свої можливості контролеру ПКМ, принаймні для цілей аудиту та перевірки. Коли погляд клієнта є абстрактним МЕ або невиродженим у підмережі, вона може мати унікальні можливості та обмеження підключення, які повинні бути відображені контролером сервера. Наприклад, навіть на фізичному МЕ деякі порти можуть адаптувати трафік між двома заданими типами характеристичної інформації, а інші – ні.

Іншим прикладом є те, що деякі з’єднання внутрішньої підмережі можуть бути захищені або можливо захистити, тоді як інші з’єднання можуть бути не захищеними. Подібні фактори стосуються A-CPI, ускладненого широким колом можливих клієнтів і програм, а також очікуванням швидкого надання послуг. Провайдери можуть публікувати каталоги, які визначають їхні зобов’язання щодо підтримки конкретних

об’єктних моделей (можливо, у формі API). Якщо достатньо запису в каталозі, клієнт може отримати послугу майже негайно, особливо якщо контролер ПКМ постачальника підтримує встановлення пакетів функцій за вимогою та робить їх доступними для агента клієнта. Спеціальні функції та інтерфейси все ще можуть вимагати зусиль щодо розробки як від імені постачальника, так і від імені клієнта. Очікується, що з часом каталог буде розширюватися, поки більшість клієнтів не будуть задоволені пропозиціями каталогу. Суть цього пункту полягає в тому, щоб застерегти від ідеї, що довільна інфраструктура, контролери та програми можуть бути об’єднані без ретельного планування та перевірки.

У цьому розділі не розглядаються деталі розподілених контролерів або розподіленого стану, що передбачає опис добре відомих проблем впровадження розподілених систем. Суттєві аспекти передбачають забезпечення прозорості розповсюдження ключів, що приховує різні аспекти основного розповсюдження від користувача. Прозорості, включають доступ, розташування, паралельність, реплікацію, помилку та міграцію.

• Прозорість доступу: немає очевидної різниці між методами локального та віддаленого доступу (синтаксична та семантична узгодженість)

• Прозорість розташування: можливість отримати доступ до будь-якого компонента системи без необхідності знати його місцезнаходження (подробиці топології не стосуються користувача)

• Прозорість паралелізму: можливість, для різних програм отримувати доступ до спільних даних/об’єктів без створення перешкод між ними

• Прозорість реплікації: здатність групи компонентів надавати єдиний інтерфейс для інших (якщо система забезпечує реплікацію з причин доступності або продуктивності, це не повинно стосуватися користувача)

• Прозорість відмов: можливість приховати відмову компонента від інших, чого можна досягти за допомогою прозорості реплікації (група системних компонентів, що надає єдиний інтерфейс для інших, може бути поінформована про відмову одного члена та координувати між собою самі, щоб переконатися, що інші цього не знають)

• Прозорість міграції: підтримка приховування міграції або реконфігурації компонентів системи, наприклад, для забезпечення кращої продуктивності, надійності тощо (користувача не повинно хвилювати)

Контролер ПКМ може використовувати площину даних ПКМ для деяких або всіх своїх внутрішніх або зовнішніх інтерфейсів, доки контролер ПКМ не покладається на підключення до працездатності площини даних, якою він керує; інакше контролер ПКМ може опинитися на мілині або безповоротно фрагментованим.

Це необхідно враховувати під час планування розгортання контролерів ПКМ щодо їхніх контрольованих підмереж, особливо якщо контролери ПКМ розподілені, деякі чи всі компоненти розташовані в хмарах і підлягають міграції.

Багато сценаріїв ПКМ оптимізують мережеві ресурси, але припускають послуги, орієнтовані на підключення, у яких програма встановлює маршрут, ємність і QoS перед початком передачі даних. Реагування контролера в режимі реального часу на запити встановлення з'єднання зазвичай не є фактором у цих випадках. Інші випадки використання ПКМ передбачають аналіз у реальному часі потоків трафіку та навантаження на мережу, які можуть бути принаймні частково хаотичними з оптимізацією в замкнутому циклі зворотного зв'язку. Необхідно мати на увазі, що, крім часу вимірювання та часу спрацьовування, на мінімальну постійну часу такої петлі зворотного зв'язку впливає затримка зв'язку між мережевою інфраструктурою та контролером ПКМ. Додаткова затримка виникла б, якщо контролер ПКМ був розподіленим і якщо керування зворотним зв'язком вимагало зв'язку між розподіленими компонентами контролера.

Об'єднавши вже існуючі мережі під егідою принципів ПКМ, постачальник може запропонувати своїм клієнтам середовище ПКМ. Тобто клієнт може бачити ПКМ за A-CPI, тоді як провайдер реалізує ПКМ у частково або повністю не ПКМ мережі. Постачальник може зробити це за допомогою адаптаційного проміжного програмного забезпечення, існуючих систем управління чи контролю, субпідряду з постачальниками нижчого рівня або будь-якої комбінації цього.

Вже існують протоколи керування, які спілкуються з ресурсами рівня даних, навіть інтерфейси командного рядка. Ці протоколи придатні для налаштування та моніторингу квазістатичних ресурсів на мережевих елементах, що не належать до ПКМ, інформація з яких потім може бути доступною для контролерів ПКМ або доступною для додатків клієнтів. Ці протоколи та інформаційні потоки існують у поточних розгорнутих елементах мережі та в інфраструктурі OSS постачальників. За відсутності чіткого ділового обґрунтування для їх заміни вони залишаться на місці на невизначений термін. Тому важливо якомога більше використовувати принципи ПКМ у змішаному середовищі, визнаючи, що повне середовище ПКМ є довгостроковою метою. Важливими принципами, які слід застосовувати, є уніфікований контроль і глобальний огляд.

Уніфікований контроль означає, що МЕ ніколи не потрібно займатися суперечливими вимогами до своїх ресурсів. Є принаймні два способи, якими це можна реалізувати.

1. Контролер ПКМ може підключитися до МЕ за допомогою функції посередника, наприклад, існуючої EMS, для перекладу своїх інструкцій на терміни, зрозумілі МЕ. Не потрібно буде вносити зміни до МЕ; платформу посередника потрібно буде оновити для виконання функцій агента та віртуалізатора.

2. МЕ можна оновити для підтримки архітектури, але деякі ресурси можуть залишатися поза межами. Ці ресурси будуть контролюватися через протоколи, відмінні від ПКМ, тоді як контролерам ПКМ буде надано контроль над строго окремими ресурсами.

В обох випадках концептуально монолітний контролер ПКМ залишатиметься відповідальним за підтримку загального, самоузгодженого уявлення про інформацію та стан ресурсів під його контролем.

Принцип глобального перегляду означає, що контролер ПКМ має повну інформацію про свій домен, де значення повних знань може змінюватися залежно від потреби. Для цілей цього пункту питання полягає в тому, як контролер ПКМ отримує ці знання та підтримує їх в актуальному стані. Запити, опитування чи сповіщення з самої мережі, є важливим джерелом інформації. Системи керування можуть

створювати або оновлювати інформацію в контролері ПКМ, наприклад про інвентаризацію. Раніше зазначалося, що контролер ПКМ може запускати протоколи маршрутизації або сигналізації для зв'язку за межами своєї власної технології або адміністративного домену.

Взаємозв'язані домени ПКМ і домени, що не належать до ПКМ, імовірно, існуватимуть ще деякий час. Для контролерів ПКМ або пов'язаних з ними бек-офісних мереж і систем планування послуг буде доцільно зрозуміти, як створювати служби, які продовжуватимуть використовувати існуючу потужність МЕ, одночасно використовуючи гнучкість ПКМ, де це може додати цінності. Це передбачає інтелектуальне планування мережі та послуг для розподілу функціональних можливостей між різними вузлами у віртуальній мережі.

Мережеві елементи й надалі потребуватимуть усіх існуючих функцій керування, таких як встановлення обладнання та інвентаризація та оновлення програмного забезпечення. Протоколи продовжуватимуть використовуватися необмежений час у МЕ-ПКМ. Деякі з них, наприклад METCONF, також є кандидатами на використання в середовищах ПКМ.

Функції управління включають:

• Обслуговування інфраструктури: аналіз несправностей, діагностика, кореляція тривог і управління.

• Підписка на сповіщення про перевищення порогу РМ, моніторинг кількості РМ. Моніторинг SLA з коригуванням платіжних записів щодо порушень SLA.

• Ведення журналів, особливо журналів безпеки. Зберігання, завантаження та збереження журналів.

• Постійність конфігурації та служби, резервне копіювання, відновлення, аудит.

• Аналіз трафіку, проектування мережі та обладнання, монтаж, інвентаризація.

• Розповсюдження та оновлення програмного забезпечення. Централізоване глобальне подання, доступне для контролера ПКМ, може полегшити тимчасову маршрутизацію трафіку навколо МЕ, для яких заплановано оновлення програмного забезпечення або значні зміни обладнання, таким чином зменшуючи або, можливо, уникаючи перебоїв у обслуговуванні, які можуть виникнути в існуючій мережі.

У крайньому випадку принцип логічно централізованого керування припускає, що єдиний контролер ПКМ має всесвітню сферу дії. Однак реальний контролер ПКМ, ймовірно, не охоплює всіх кінцевих точок, які цікавлять його клієнтів. Обслуговування клієнтів часто поширюється на інші технічні чи адміністративні сфери. Ці домени можуть включати мережі, що не належать до ПКМ.

Зокрема, під час взаємодії з мережами, що не контролюються ПКМ, які вже існують і працюють, може бути доречним, щоб контролер ПКМ запускав різноманітні існуючі протоколи, наприклад BGP або GMPLS. При безпосередньому спілкуванні з іншим контролером ПКМ відповідний інтерфейс є питанням для подальшого вивчення, але цілком може бути розширенням цих або інших існуючих протоколів, наприклад протоколу зв'язку елемента обчислення шляху, PCEP.

Дотримуючись принципу ощадливості, нові протоколи слід розробляти лише за наявності переконливих доказів того, що жоден існуючий протокол не може бути належним чином використаний або адаптований.

Подання служби ПКМ може сильно відрізнятися від подання основного ресурсу. Використовується модель оптового продавця-посередника, щоб стверджувати, що перегляд та інтерфейс на кожному рівні ієрархії можуть бути однаковими. З іншої точки зору вигляд та інтерфейс можуть бути зовсім іншими. Це відбувається, коли контролер ПКМ пропонує своїм клієнтам щось відмінне від просто подальшої абстракції тих самих ресурсів. Інформація, необхідна для цього, може бути налаштована, доступна з інших джерел або може бути наявною властивістю основних ресурсів.

• A-CPI має підтримувати здатність забезпечувати цілісність транзакцій для додатків, які цього вимагають. Загалом програми працюють у власних доменах довіри, окремо від домену довіри контролера ПКМ. Для A-CPI настійно рекомендується використовувати той самий інтерфейс агентської політики, визначений для інших CPI.

• A-CPI має підтримувати надійні функції безпеки, коли він перетинає межі довірчого домену. ПКМ має на меті запропонувати своїм клієнтам широкий спектр функцій. Навіть якщо ігнорувати наскрізну модель, ця різноманітність ускладнює

визначення єдиного універсального A-CPI. Програми можуть підтримувати інтерфейси до інших програм або контролерів ПКМ у ролі клієнтів, серверів або однорангових пристроїв і, можливо, у різних ролях у різний час.

Мережі мають обмежений набір функціональних можливостей, які програми так чи інакше захочуть використати. Не кожна програма вимагатиме всіх цих функцій, і не кожна реалізація контролера ПКМ обов'язково потребуватиме підтримки всіх із них. Пакети функцій, які можна завантажити, допомагають зберегти програми ПКМ відкритими.

Специфікація A-CPI повинна дозволяти такі можливості. Залежно від конкретного призначення екземпляр A-CPI може необов'язково підтримувати всі можливості.

• Відкриття повного перегляду ресурсів, включаючи топологію віртуальної мережі.

• Для прямого виявлення інформаційної моделі низького рівня.

• Виявляти абстрактні погляди на свої ресурси. Це має бути зроблено за допомогою спеціалізації тієї ж інформаційної моделі, яка розкриває всі деталі.

Багато з наведених нижче функцій ілюструють клієнтські можливості, які, якби контролер ПКМ запропонував своїм програмам, потребували б підтримки.

• Дозволити ПЗ встановлювати та запитувати будь-який атрибут або стан у межах її контролю.

• Дозволити ПЗ контролювати пересилання трафіку: вибирати трафік відповідно до набору критеріїв, змінювати або адаптувати трафік, якщо необхідно, пересилати його до заданого набору точок виходу. Критерії відбору можуть бути такими простими, як вхідний порт, або такими складними, як вектор, який включає поля відповідності до рівня 7 включно, потенційно охоплюючи кілька пакетів потоку.

• Дозволити додатку пропонувати конструкцію пересилання трафіку, яка потребує використання нових або існуючих ресурсів відповідно до визначених показників ефективності, і отримувати одну або більше пропозицій від контролера. Клієнт може запропонувати та прийняти в одному запиті або може переглянути пропозиції та прийняти жодну або одну з них.

• Дозволити програмі викликати та контролювати стандартизовані функції, такі як STP, навчання MAC, ICMP, BFD/802.1ag, 802.1X тощо.

• Дозволити ПЗ підписуватися на сповіщення про несправності, зміни значень атрибутів, зміни стану та попередження про перевищення порогу (TCA).

• Дозволити ПЗ налаштовувати точки збору моніторингу продуктивності (PM) із пороговими значеннями та отримувати поточні та останні результати.

• Дозволити ПЗ викликати та контролювати функції обробки трафіку шляхом обміну непрозорими блоками даних.

Окремою роботою в ONF є оцінка варіантів використання A-CPI, що може розширити або вдосконалити ці критерії.

Поведінка ME (агента), який втрачає зв'язок зі своїм контролером ПКМ, регулюється політикою. Пакетно-орієнтовані ME можуть продовжувати працювати, як і раніше, з тайм-аутом входу пересилання або без нього, або можуть негайно припинити пересилання пакетів. Як правило, очікується, що ME з комутацією каналів продовжуватимуть передавати трафік, як і раніше. Такі функції OAM, як захисне перемикання та оголошення тривоги, зазвичай продовжують працювати. Оператори можуть мати особливі вимоги до такої поведінки, а розробники можуть дозволити забезпечення керування такими аспектами.

З цими вимогами пов'язані питання стійкості, скільки даних слід зберігати на ME, як їх резервно копіювати та відновлювати, а також скільки функціональних можливостей ME має мати на увазі під час повторної ініціалізації локально, перш ніж встановити з'єднання з контролером. Чи має це бути визначено архітектурою, для подальшого вивчення.

Якщо керований ПКМ ME продовжує функціонувати або перезавантажується з певним обсягом функціональних можливостей, відновленим з локальної постійної пам'яті, необхідно буде, щоб контролер перевірив і узгодив ME з деякою конфігурацією та базою даних служби. Зберігання, резервне копіювання та відновлення такої бази даних наразі не визначено.

Ці вимоги передбачають значну складність. Може бути прийнятним для деяких типів керованих ПКМ ME не підтримувати постійних даних і ініціалізуватись у

нульовому стані. Цей варіант означатиме більший час, перш ніж послуга буде доступна. Погіршення доступності або якості послуг може бути вирішено.

В ієрархічній структурі керування можливо, що збій або повторна ініціалізація може вплинути лише на один або кілька необхідних рівнів між програмою та обладнанням. У деяких випадках можливе відновлення через захист або перенаправлення. У будь-якому випадку, слід попередньо обговорити, як кожен рівень буде поводитися у разі втрати та відновлення сусіднього рівня. Фактори для розгляду включають:

• Рівень стійкості стану та поведінки одного рівня під час відсутності сусіда.

• Гарантія того, що локальна або мережева ініціалізація або відновлення не призводять до втрати ресурсів.

• Чи може або повинен сусід зберігати деякий корисний стан під час повторної ініціалізації.

• Як сусідні контролери взаємодіють, коли вони знову підключаються.

Вплив МЕ або повторної ініціалізації підмережі на зовнішні програми не визначається архітектурою, але може залежати від зобов’язань щодо доступності служби. У будь-якому випадку очікується, що буде підтримуватися ручне відновлення уражених програм.

Кілька заходів, пов’язаних із ПКМ, проводяться в усій спільноті. У якості постійних зусиль бажано, щоб ця архітектура розуміла та інтегрувала додану цінність кожної з цих дій. Запрошуються внески щодо всіх наступних тем, а також додаткових пунктів списку.

Моделі захисту та відновлення рівня даних добре запроваджені для мереж на всіх стандартизованих рівнях. Запровадження ПКМ явно не передбачає змін цих стандартів. Швидке перемикання захисту означає, що пов’язані протоколи та кінцеві автомати продовжують розміщуватись на самих мережевих елементах, при цьому контролер ПКМ відповідає за ресурси відновлення до обчислення, ініціалізацію поведінки відновлення та підписку на сповіщення.

На вищих рівнях контролер ПКМ може відповідати за відновлення трафіку, можливо, шляхом повторного обчислення шляхів і перенаправлення трафіку,

можливо, шляхом повторної оптимізації розподілу ресурсів на глобальній основі та, можливо, шляхом запуску міграції віртуальних машин на інші фізичні розташування в хмарі.

Якщо основними ресурсами користуються більше ніж один клієнт, необхідно планувати використання резервування, щоб задовольнити потреби всіх таких клієнтів. Це можна зробити будь-якою комбінацією кількох способів:

1. Групуйте клієнтів у пули ресурсів відповідно до вимог загальної доступності та часу відновлення.

2. Захистіть базові ресурси відповідно до найсуворіших вимог будь-якого з клієнтів, і дозвольте іншим їздити вільно.

3. Запропонуйте рівень захисту спільних ресурсів за умовчанням і вимагайте від клієнтів із більш суворими потребами підписатися на виділені ресурси.

4. Інше.

ВИСНОВКИ ДО РОЗДІЛУ 1

У даному розділі я представив інтелектуальну історію програмованих мереж. Ідея програмованої мережі спочатку оформилася як активна мережа, яка підтримувала багато тих самих бачень, що й ПКМ, але не мала ні чіткого сценарію використання, ні шляху поступового розгортання. Після ери активних дослідницьких проектів мереж дослідження перекинулося від бачення до прагматизму у формі розділення площини даних і управління, щоб полегшити керування мережею. Ця робота була зосереджена головним чином на кращих способах маршрутизації мережевого трафіку — набагато вужче бачення, ніж попередня робота з активної мережі.

Зрештою, робота над OpenFlow і мережевими операційними системами знайшла правильний баланс між баченням і прагматизмом. Ця робота пропагувала мережевий контроль для широкого спектру програм, але покладалася лише на існуючі можливості комутаційних чіпсетів. Зворотна сумісність із існуючим апаратним забезпеченням комутатора привернула увагу багатьох постачальників обладнання,

які прагнули конкурувати на зростаючому ринку мереж центрів обробки даних. Баланс широкого, чіткого бачення з прагматичною стратегією широкого впровадження набув популярності, коли ПКМ знайшов переконливий варіант використання у віртуалізації мережі.

Оскільки Програмно-конфігурована мережа продовжує розвиватися, я вірю, що історія може винести важливі уроки. По-перше, технології ПКМ будуть жити або помруть на основі «використання залучення». Хоча ПКМ часто проголошують вирішенням усіх мережевих проблем, варто пам’ятати, що ПКМ — це лише інструмент для більш легкого вирішення проблем керування мережею. Лише ПКМ передає в наші руки владу для розробки нових програм і рішень давніх проблем. У цьому плані наша робота тільки починається. Якщо минуле свідчить про те, що розробка цих нових технологій вимагатиме інновацій у різних часових масштабах, від довгострокових сміливих бачень (таких як активна мережа) до найближчого творчого вирішення проблем (таких як операційно-орієнтована робота з розділення контролю і площини даних).

По-друге, необхідно зазначити, що баланс між баченням і прагматизмом залишається слабким. Сміливе бачення ПКМ підтримує широкий спектр додатків керування; однак контроль OpenFlow над площиною даних обмежується примітивними операціями зіставлення з полями заголовків пакетів. Нам слід пам’ятати, що початковий дизайн OpenFlow був зумовлений бажанням швидкого впровадження, а не першочерговими принципами. Підтримка широкого спектру мережевих послуг вимагала б набагато складніших способів аналізу та маніпулювання трафіком (наприклад, глибока перевірка пакетів, а також стиснення, шифрування та перекодування пакетів), використовуючи стандартні сервери (наприклад, машини x86). або програмоване обладнання (наприклад, FPGA, мережеві процесори та графічні процесори), або те й інше. Цікаво, що відродження інтересу до більш складної функціональності площини даних, такої як віртуалізація мережевих функцій, повертається до попередніх робіт з активної мережі, завершуючи нашу історію.

Збереження сміливого бачення програмно-конфігурованих мереж вимагає від нас продовжувати думати «нестандартно» про найкращі способи програмування мережі, не обмежуючись обмеженнями сучасних технологій. Замість того, щоб просто розробляти програми ПКМ з урахуванням поточних протоколів OpenFlow, ми повинні подумати про те, який контроль ми хочемо мати над площиною даних, і збалансувати це бачення з прагматичною стратегією розгортання.

РОЗДІЛ 2
УДОСКОНАЛЕНА МОДЕЛЬ ФУНКЦІОНУВАННЯ ТА НАДАННЯ ПОСЛУГ ПКМ

2.1. Аналіз робочого процесу обробки трафіку програмно-конфігурованих мереж

Площина керування та передня площина мають керувати усією мережею безперервно та одночасно. Основною функцією комп'ютерної мережі є обчислення шляхів маршрутизації потоків трафіку, які прибувають, щоб передавати їх до місць призначення. Деякі служби контролера мають високі постійні вимоги, які сильно впливають на продуктивність контролера ПКМ через його багато обов'язків і можуть спричинити затримку в обробці іншого контролера. Хоча контролер ПКМ має обмежені можливості, його архітектура покладається на єдиний централізований контролер для керування всіма мережевими операціями, такими як обробка пакетів, що надходять, обчислення шляхів маршрутизації, встановлення записів потоку в комутаторах, доставка мережевої інформації до програм, моніторинг поведінки мережі. , взаємодія з іншими контролерами тощо.

Традиційна архітектура ПКМ не розроблена для підтримки високого рівня масштабованості та великого трафіку. Різні дослідження запропонували різні дизайни розподілених контролерів для мереж на основі ПКМ, які значно підвищили масштабованість площини керування. Однак схема управління розподіленими контролерами вимагає значних зусиль щодо синхронізації між контролерами.

Контролер ПКМ містить деякі важливі функції, які вимагають значного обсягу інформації та обробки в різних масштабах часу. Наприклад, програми маршрутизації вимагають величезної кількості інформації про поточний стан потоків трафіку в усіх каналах, одночасно знаходячи ефективні маршрути для кожного потоку до місця призначення в мережі. Ці завдання вимагають застосування різних додатків маршрутизації з глобального погляду з урахуванням деяких важливих питань трафіку

щодо топології мережі, включаючи поточний стан трафіку, інформацію про пропускну здатність, надійність, взаємодію інженерного трафіку тощо. Таке завдання можна обробляти окремо у зовнішніх блоках відповідно до будь-яких правил або політик, встановлених контролером. Запуск зовнішнього блоку для покращення масштабованості площини керування потребує додаткового вартість архітектури мережі; однак це ефективно зменшить навантаження на контролер ПКМ, узурпувавши одне з його основних завдань.

ПКМ — це архітектура комп'ютерних мереж, яка швидко розвивається та розширюється, перетворюючи комп'ютерні мережі на організації, керовані програмним забезпеченням. Він має на меті відокремити площину керування від мережевих пристроїв. Таким чином, управління мережею та вихідні дані організації покладаються на один віддалений інтелектуальний пристрій керування, тоді як пряма площина стає простим пристроєм пересилання пакетів. Важливою перевагою ПКМ є те, що він робить роботу та керування мережею більш гнучкими, що може покращити продуктивність мережі. Архітектура ПКМ складається з трьох різних рівнів: рівня інфраструктури, рівня керування та рівня додатків.

Рівень інфраструктури складається з набору мережевих пристроїв, таких як комутатори ПКМ, які представляють передову площину. Основним завданням цих мережевих пристроїв є прийом і пересилання потоків трафіку через фізичні інтерфейси відповідно до інструкцій, наданих керуючим рівнем. На якість взаємодії між мережевими пристроями суттєво впливає якість площини керування.

Рівень керування містить віддалений централізований контролер, який представляє площину керування. Основні завдання контролера ПКМ включають моніторинг, обчислення та керування додатками для інших компонентів мережі. Він також надає бізнес-додаткам статистичну інформацію про мережеві пристрої.

Прикладний рівень містить кілька бізнес-додатків, які забезпечують додаткове керування мережею та послуги, такі як інженерний трафік, балансування навантаження, контроль доступу та застосування політики, які працюють у мережі.

OpenFlow — це перший комунікаційний протокол, який дозволяє розгортати ПКМ. Він призначений для підтримки зв'язку між контролером ПКМ і мережевими

пристроями шляхом забезпечення безпечного каналу зв’язку для надсилання повідомлень від контролера та мережевих пристроїв і до них. До основних компонентів мережі на основі OpenFlow належать:

• Центральний контролер OpenFlow виконує всі складні операції, включаючи обчислення маршрутів, керування політикою та контроль безпеки, щоб контролювати поведінку всієї мережі.

• Мережеві пристрої, такі як комутатори пакетів, керуються контролером OpenFlow. Вони є основними елементами, які отримують інформацію про маршрутизацію від контролера OpenFlow для перенаправлення вхідного трафіку на відповідний порт на основі інструкцій, продиктованих контролером.

• Безпечний канал зв’язку визначає стандартизований протокол для обробки повідомлень через південні канали зв’язку, які знаходяться між контролером OpenFlow і мережевими пристроями.

На Рис. 2.1. показано, як звичайна обробка маршруту виконується за допомогою типової мережі на основі ПКМ і як ці компоненти взаємодіють один з одним, щоб обробляти запити маршрутизації щодо щойно прибулого трафіку. Як показано, головний контролер несе повну відповідальність за обробку цих запитів, незалежно від обсягу трафіку та можливостей контролера.

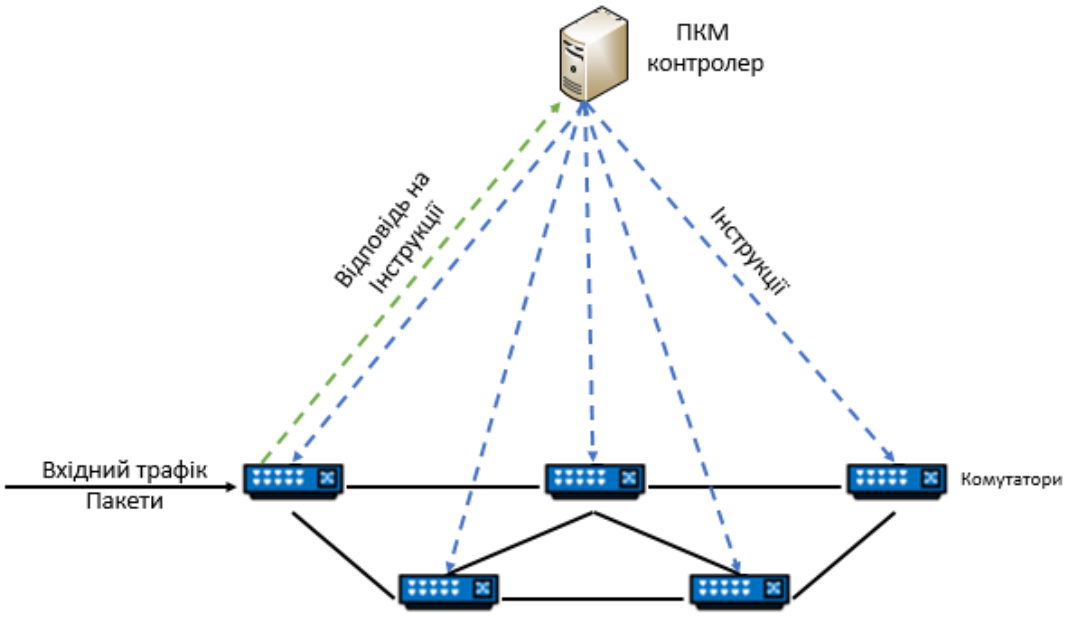

Рис. 2.1. Традиційний робочий процес обробки трафіку

У традиційних мережах на основі ПКМ усі обов’язки з контролю покладаються на один контролер, що означає, що така конструкція може легко спричинити збої контролера. Як правило, Блок резервного копіювання (БРК) можна додати навколо контролера ПКМ, щоб забезпечити здатність керування витримувати екстремальні умови. Крім того, контролер може обробляти кілька різних завдань паралельно, запускаючи кілька БРК, і кожен БРК може незалежно обробляти конкретне контрольне завдання з урахуванням усіх правил і політик, створених контролером.

Цей підхід не позбавляє основного контролера можливості взаємодії з передньою площиною. Контролер ПКМ все ще має доступ до передньої площини для застосування будь-яких служб керування, якщо це необхідно. Крім того, контролер має виділений прямий доступ до БРК для встановлення будь-яких додаткових правил або політик. БРК розгорнуто поблизу контролера ПКМ, тому він може отримати прямий доступ до основної пам’яті контролера ПКМ, щоб уникнути більш трудомісткого читання даних.

Контролер ПКМ залишається основним блоком, який відповідає за виконання всіх контрольних завдань; однак, якщо деякі завдання споживають занадто багато контрольної потужності, контролер передасть ці завдання потрібним БРК. Ця модель додає додаткові завдання та обов’язки контролеру, вимагаючи каналу зв’язку та пов’язаних програм для надсилання та отримання повідомлень від БРК. Однак це вдосконалення дозволяє контролеру запускати більше одного БРК одночасно, що дає змогу одночасно обробляти більш складні завдання.

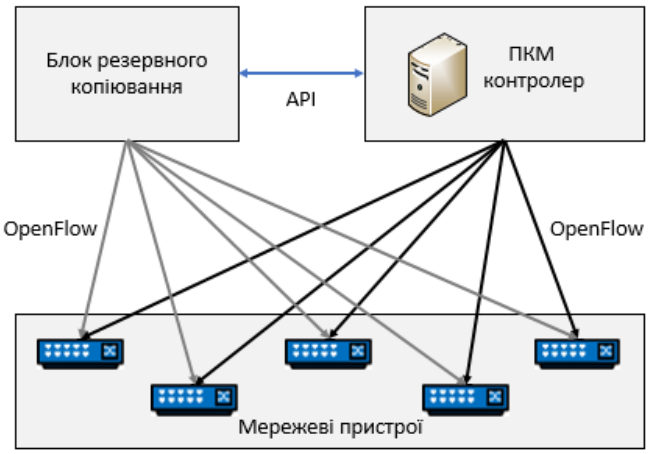

Рис. 2.2. Архітектура ПКМ після додавання БРК

Контролер виконує обробку маршруту, використовуючи окремий резервний блок, призначений лише для операцій обчислення маршруту. Він має два канали зв'язку: перший канал призначений для отримання інструкцій від контролера ПКМ, а другий канал призначений для надсилання інструкцій маршруту до мережевих пристроїв.

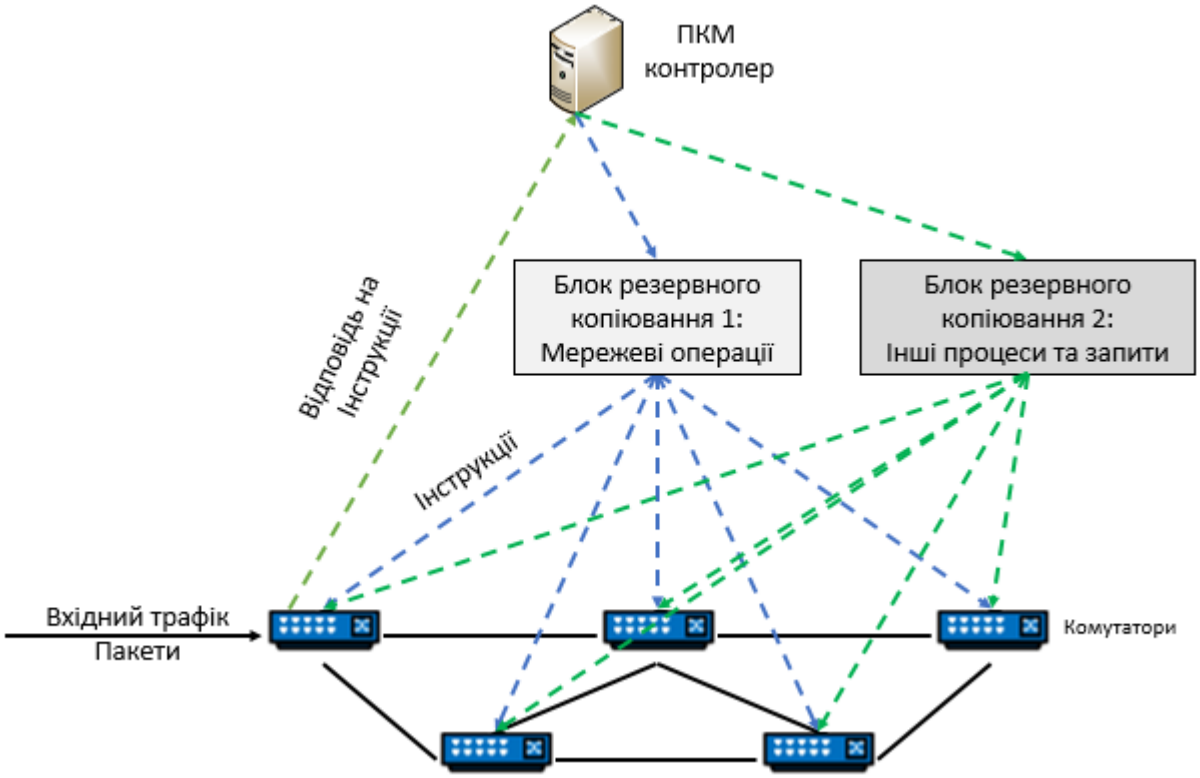

Рис. 2.3. Робочий процес обробки трафіку після додавання БРК

У порівнянні з традиційним випадком, контролер тут може використовувати існуючі БРК для обробки додаткових завдань, якщо він отримує занадто багато запитів на обробку. Це допомагає контролеру працювати в умовах високого навантаження на додаток до виконання паралельних і одночасних операцій з меншими зусиллями за допомогою кількох БРК.

2.2. Алгоритми підвищення ефективності функціонування ПКМ

Алгоритм пошуку гармонії (АПГ) — це метаевристичний алгоритм, натхненний музикантами, мета яких — покращити музику шляхом налаштування

параметрів музичного інструменту для кращого стану гармонії. АПГ підтримує широкий спектр задач оптимізації, які працюють краще, ніж попередні алгоритми оптимізації з точки зору математичного аналізу. Алгоритм АПГ вирішує широкий спектр інженерних задач оптимізації в різних областях, таких як вирішення головоломок, проблеми маршрутизації та проблеми розподіленої мережі. Типовий АПГ складається з трьох кроків, а саме ініціалізації, імпровізації та оновлення, які можна сформулювати як:

$$H_i^{New} = \begin{cases} H_i(l) \in H_i(1), H_i(2), \dots, H_i(l) & R_1 > hmcr \\ H_i(l) \in H_i^1, H_i^2, \dots H_i^{HMS} & R_1 \leq hmcr \\ H_i(l) + R_3 * BW & R_2 \leq par \end{cases}, \quad (2.1)$$

де H_i^{New} - нова гармонія, R1, R2 і R3 - випадкові числа між [0, 1], hmcr - швидкість розгляду пам’яті гармонії, par - налаштування висоти швидкості, BW позначає пропускну здатність, а HHMS позначає рішення гармонійної пам'яті гармонійних.

Алгоритми АПГ здебільшого обмежені високою швидкістю збіжності, що впливає на точність. Таким чином, деякі з модифікацій вводяться в алгоритм АПГ, а саме:

• Динамічна адаптація параметрів АПГ для підвищення швидкості конвергенції;

• Покращено роботу з точки зору точності шляхом поєднання з іншими алгоритмами оптимізації (наприклад, гібридними рішеннями);

• Набір попередньо визначених правил для нової гармонії (тобто гібридної гармонії).

Алгоритм рою частинок (АРЧ) – це алгоритм стохастичної оптимізації, який базується на популяції (тобто поведінці) кількох тварин, таких як зграї птахів, зграї риб тощо. Різні алгоритми АРЧ здебільшого пов’язані з двома основними методами дослідження, такими як еволюційні алгоритми та штучні алгоритми. Цей алгоритм забезпечує кращі результати оптимізації порівняно з алгоритмами генетичної оптимізації. Він виконується на основі розміру рою вектора положення кожної

частинки кінцевого розміру з вектором швидкості. Оптимальні позиції кожної особини відчуває рій і оновлює оптимальну позицію особин з початкового стану. Ми оновлюємо оптимальне положення кожної особини, використовуючи рій, враховуючи положення та швидкість. Формула оновлення позиції виражається наступним чином: [12]

$$P_{ij}(R+1) = P_{ij}(R) + v_{ij}(R+1), \tag{2.2}$$

де Pij(R) позначає положення частинок, vij(R + 1) позначає швидкість частинок, і позначає частинку, а R позначає ітерацію. Крім того, оновлення швидкості виконується шляхом врахування ваги інерції для формули оновлення швидкості, яка виражається наступним чином:

$$v_{ij}(R+1) = W(R)v_{ij}(R) + A_1R_1\left(P_{Best} - P_{ij}(R)\right) + A_2R_2(G_{Best} - P_{ij}(R)), \tag{2.3}$$

де $v_{ij}(R)$ представляє швидкість частинки під час ітерації, W(R) представляє значення ваги, A1, A2 представляють константи прискорення, R1, R2 позначає випадкові значення між [0, 1], а P_{Best} і G_{Best} представляють локальні і глобальне положення частинок.

Він долає обмеження алгоритму АПГ. Цей алгоритм забезпечує високу обчислювальна ефективність з ефективними контрольними параметрами в порівнянні з кількома евристичними алгоритмами оптимізації.

Нове рішення для проблеми розміщення контролера в програмно визначених мережах. У цій роботі використовуються натхненні природою алгоритми, такі як оптимізація пошуку їжі для скатів мант і алгоритм зграї salp для вирішення проблем із розміщенням контролера. Щоб покращити продуктивність окремих алгоритмів, дискретизація виконується потрійними операторами. Дискретизовані алгоритми використовуються гібридним способом для розміщення контролера. У цій роботі вирішено проблему розміщення контролера шляхом забезпечення затримки в мережі.

Однак для оптимального розміщення контролера враховуються інші обмеження (наприклад, вимоги до комутатора, відмовостійкість тощо).

Ефективний метод для задачі розміщення контролера з використанням евристичних алгоритмів. Спочатку аналізується затримка між комутаторами та контролерами та створюється модель з урахуванням затримки. Модель з урахуванням затримки оцінюється трьома алгоритмами оптимізації, а саме алгоритмом оптимізації кажана, алгоритмом світлячка та алгоритмом оптимізації на основі VARNA. Усі три параметри алгоритму оптимізації оптимізовано за допомогою оптимізації рою частинок для підвищення продуктивності. У цій роботі використовувалися лише обмежені показники мережі, що вплинуло на її оптимальність у вирішенні проблеми розміщення контролера.

Алгоритм оптимізації для розміщення контролера в програмно визначених мережах. У цій роботі використовуються два алгоритми для розміщення контролера, а саме генетичний алгоритм і алгоритм АРЧ. Алгоритм оптимізації роя частинок спочатку вибирає найкращий контролер на основі значень придатності, враховуючи його обмеження затримки. Генетичний алгоритм використовується для оновлення положення та швидкості контролери. У цій роботі використовується генетичний алгоритм і алгоритм оптимізації рою частинок для розміщення контролера; однак генетичний алгоритм обмежений великими витратами часу на обчислення. [13]

Оптимізований підхід для CPP. У цій роботі використано алгоритм оптимізації на основі VARNA, який зменшує загальні витрати часу під час розміщення контролера. Ця робота перевершує алгоритм Teacher Learning Based Optimization і алгоритм Jaya з точки зору витрат часу. У цій роботі розглядається лише затримка як обмеження розміщення проблеми контролера. Однак для кращого розміщення слід також враховувати інші обмеження.

Розміщення контролера за допомогою алгоритму оптимізації в мережі ПКМ. Тут для кожного кластера було розміщено контролер, щоб зменшити затримку між перемиканням на контролер. Запропонований метод розраховує максимальну відстань для зменшення затримки між комутатором і контролером. Запропонований метод досягає меншої затримки для різних типів і кількості розміщення контролера.

Експериментальні результати демонструють, що запропонована робота досягла кращих показників у відмовостійкості порівняно з існуючими роботами.

Нова структура розміщення контролерів була запропонована з використанням багатокритеріального методу кластеризації. Основною метою цього дослідження було зменшення затримки зв’язку та наскрізної затримки. Запропонована топологія ПКМ побудована у вигляді графа. Тут контролер і перемикачі розташовані за допомогою запропонованого підходу кластеризації. Після цього визначається шлях між контролером і комутатором. Для цього була запропонована оптимізація полум'я молі. Нарешті, результати моделювання демонструють, що запропонована робота досягла кращої продуктивності порівняно з деякими іншими існуючими підходами.

Задачу розміщення контролера вирішували за допомогою алгоритму оптимізації VARNA в середовищі ПКМ. Спочатку популяції ініціалізуються та класифікуються на два типи варн на основі переваги частинок. Varna optimization обчислює значення придатності частинок для двох класів. На основі значень придатності було виконано розміщення контролера. Експериментальні результати показують, що запропонована робота досягла кращої продуктивності порівняно з іншими алгоритмами оптимізації.

Підхід до розміщення контролера в програмно-конфігурованих мережах для зменшення збоїв зв’язку. Спочатку було проведено дослідження зв’язку, щоб проаналізувати та впорядкувати рівень відмов зв’язку. Покращений евристичний алгоритм на основі NSGA-II був розроблений для зменшення кількості контролерів, щоб забезпечити ефективне рішення для багатоканальних збоїв CPP-MLF. Генетичний алгоритм недомінованого сортування-II (NSGA-II) вдосконалено зокрема з точки зору відстані скупчення та недомінованого набору з використанням оператора на основі рівномірного розподілу та адаптивної техніки змагання для досягнення оптимальних рішень Парето для вирішення CPP-MLF. Нарешті, дисперсія навантаження контролерів була оцінена для досягнення ефективних рішень щодо ефективного розміщення контролерів. Експериментальний аналіз проводився шляхом порівняння розробленого евристичного підходу з кількома попередніми

алгоритмами. Однак такий підхід не підходить для великих мереж, оскільки призводить до збільшення навантаження на мережу.

Підхід до ефективного розміщення кількох контролерів у програмно-конфігурованих мережах. Спочатку дерево Штайнера було реалізовано для оптимального обчислення міжконтролерів шляхом об'єднання кінцевих точок невдалих з'єднань за найкоротшим шляхом з урахуванням кількості контролерів, потужності контролера та відображення контролера комутатора. Переспрямування потоків за певною функцією називається швидким відновленням після відмови в групових таблицях OpenFlow. Нарешті, розміщення спільного контролера оптимально виконується з урахуванням вагового параметра дерева Штайнера до і після відмови, щоб зменшити збій зв'язку. Оцінка ефективності цього методу була виконана з точки зору вартості синхронізації мережі та реконфігурації мережі, що виникла з ладу, тощо.

Підхід до оптимального розміщення контролера з оптимальним вибором контролерів за допомогою динамічного алгоритму оптимізації роя chaotic-SALP (SSOA) у мережі ПКМ. Спочатку алгоритм SSOA був представлений з хаотичними картами для підвищення продуктивності оптимізатора. Було проведено оцінку оптимальної кількості контролерів і з'єднань між контролерами та комутаторами, у яких оптимальні розподіли та кількість контролерів виконувалися хаотичними алгоритмами на основі SSA, щоб зменшити вартість під час розгортання та затримку мережі. Вилучення випадкових параметрів за допомогою розподіленої реалізації цього методу за Гауссом виконується за допомогою Internet topology zoo та оцінки цієї роботи шляхом розгляду кількох параметрів.

Підхід до оптимального розміщення контролерів у середовищі програмно-конфігурованих мереж. Спочатку формалізація комплексного математичного підходу для CPP вибирає розташування контролерів, зменшує кількість контролерів і призначення вузлів для кожного контролера, враховуючи затримку під час розповсюдження, пропускну здатність контролерів і балансування навантаження з використанням евристичного підходу як NP-hard. У евристичному підході формування кластерів здійснювалося між вузлами для керування мережею та

призначення контролерів для кожного кластера шляхом вибору оптимального вузла на основі компромісного методу. Нарешті, враховуючи діаметр мережі, було обрано найкоротший шлях. Експериментальний аналіз порівнювався з кількома найсучаснішими роботами, щоб підтвердити ефективність цієї роботи.

Підхід до розміщення мультиконтролерів у ПКМ шляхом поширення спорідненості. Спочатку мережа була розділена шляхом реалізації алгоритму на основі модифікованого розповсюдження спорідненості, який є алгоритмом кластеризації, який автоматично обчислює кількість кластерів та ідентифікацію зразків-кандидатів для розміщення контролерів ПКМ, враховуючи подібність кількох параметрів, таких як посилання пропускна здатність і евклідова відстань. Нарешті, було виконано моделювання шляхом побудови топології мережі з використанням топології Інтернет-зоопарку для оцінки запропонованої роботи з точки зору затримки між контролерами, факторів дисбалансу, найгіршого та середнього випадку. Таблиця 2.1. підсумовує переваги та недоліки пов’язаних робіт, розглянутих у цьому огляді:

Таблиця 2.1.

Переваги та недоліки відповідного обстеження робіт.

Переваги	**Недоліки**
Вирішено КПП гібридним методом. Забезпечення затримки в мережі.	Обмеження (наприклад, вимоги до комутації, відмовостійкість) для оптимального розміщення контролера.
Надає модель з урахуванням затримки за допомогою bat оптимізації, алгоритму firefly, і VARNA.	Використовує лише обмежені мережеві індикатори.

Продовження таблиці 2.1.

Генетичний алгоритм і алгоритм АРЧ використовувалися для вибору найкращого контролера на основі значень придатності, враховуючи їх обмеження затримки.	Генетичний алгоритм обмежує високу витрату часу на обчислення
Він використовує алгоритм оптимізації VBO на основі VARNA, який зменшує загальне споживання часу в режимі консолі. Кращий, ніж алгоритм оптимізації, заснований на навчанні вчителів, і алгоритм Jaya з точки зору витрат часу.	Ця робота лише із затримкою вважається обмеженням CPP та іншими обмеженнями кращої ситуації.
Для кожної групи було налаштовано контролер, щоб зменшити затримку між S2C методом «$». Запропонований метод досягає меншої затримки для різних типів підрахунків режимів контролера. Результати показують, що запропонована робота показала кращий рівень відмовостійкості.	Є лише одна несправність мережевого контролера № 5 в плані надійності шляху
Вони використовували неконтрольований тип-оптимізатор локуса з контрольованим полум'ям для трьох показників, кількості стрибків, затримки розповсюдження та використання каналу допризначити S2C. Вони відрізняються надійністю шляху і найкращим розташуванням консолей.	Це було зосереджено на методі кластеризації, і існують інші обмеження «k» кількох контролерів і не вказує кількість збоїв на шляху до запропонованої структури.
Вони використовували алгоритм VBO в середовищі ПКМ для вирішення CPP і зменшення середньої затримки ПКМ, щоб VBO забезпечував найкращу динамічну продуктивність.	Він заснований на кластеризації.

Продовження таблиці 2.1.

Розроблено вдосконалений евристичний алгоритм на основі NSGA-II, щоб покращити продуктивність CPP у ПКМ і зменшити кількість збоїв зв'язку контролерів. Було визначено, що дистанція нагромадження та недомінуюча групова адаптивна конкуренція прийшли до оптимальних рішень Парето для рішення CPP-MLF Multi-Link Failures.	Такий підхід не підходить для глобальних мереж, що призводить до збільшення навантаження на мережу.
Дерево Штейнера було реалізовано для розрахунку оптимального внутрішнього контролера з точки зору вагового параметра для досягнення невдалих зв'язків через найкоротший шлях. Кількість і потужність контролерів враховуються та відображаються в комутаторі. Швидке відновлення після відмови в групових таблицях OpenFlow.	У разі збою мережевої синхронізації та переналаштування мережі стягується оплата.
Алгоритм динамічної оптимізації salp swaMP ПКМ (SSOA) використовувався для отримання найкращої продуктивності для оптимального розміщення контролера з хаотичним відображенням. Оптимальна кількість контролерів і з'єднання між контролерами та комутаторами були оцінені з точки зору створення оптимальної кількості призначень контролерів, щоб зменшити витрати під час розгортання та затримки мережі.	Він заснований на вилученні випадкових параметрів.

Закінчення таблиці 2.1.

Використовує комплексний математичний підхід до рішення CPP, який знаходить і мінімізує контролери, вибираючи оптимальний вузол на основі методу обміну та призначаючи вузол кожному контролеру, враховуючи затримку розповсюдження, пропускну здатність контролерів і балансування навантаження за допомогою евристичного підходу, такого як НП-твердий. Найкоротший шлях був обраний з урахуванням діаметра сітки.	Затримка розповсюдження між вузлами до контролерів знаходиться в кінцевих межах у разі розподілу між контролерами.
Алгоритм на основі розділення використовувався для функції кластеризації, де він автоматично підраховує кількість кластери та вибирає варіанти розміщення кількох контролерів у ПКМ, враховуючи подібність кількох параметрів, таких як смуга пропускання кореляції та евклідова відстань, і таким чином обчислює затримку між контролером і факторами дисбалансу.	Не всі контролери вказуються для розділення та ємності мережі.

2.3. Застосування та напрямки досліджень

У цьому розділі я представив програми програмно-конфігурованих мереж і останні дослідження, включаючи програмно визначені ICN, мультимедіа, мережеве керування, мережеву віртуалізацію, хмару та центр обробки даних, безпеку, бездротові та мобільні мережі.

В останні роки багато дослідників стверджували, що поточна архітектура Інтернету не в змозі відповісти на нові та майбутні потреби користувачів. На основі цього твердження були представлені нові архітектури. Інформаційно-центрована

мережа є однією з таких архітектур. В ICN ім’я інформації є унікальним і не залежить від місць розташування, програм, сховищ і розподілу, а мережеві примітиви створюються на основі імен. Для отримання іменованої інформації вводяться різні методи передачі, включаючи маршрутизацію на основі імен, розв’язку на основі імен тощо. Щоб підтримувати ці методи та використовувати переваги ICN, необхідні значні зміни в мережевих пристроях, розгорнутих у поточному Інтернеті, які призводить до проблеми з впровадженням ICN. Ряд проектів пропонували впровадження ICN через ПКМ. Це призводить до зниження витрат на впровадження. Це також забезпечує інновації та оптимізацію мережевих ресурсів і функцій.

Інтеграція ICN і ПКМ може допомогти новим технологіям ефективно розвиватися та легко протистояти викликам сучасних мереж. Підтримка мобільності та хмарних обчислень є двома суперечливими темами в сучасних мережах через невідповідність протоколу IP. ПКМ можна використовувати для прийняття найкращих та оптимізованих рішень щодо міграції віртуальної машини на основі погляду контролерів на мережу та автоматичного оновлення конфігурацій мережевих пристроїв після міграції.

Однією з переваг впровадження ICN над ПКМ є покращення функціональних можливостей ICN. Було запропоновано протокол маршрутизації, який підтримує мобільність за допомогою контролера. Це можна легко реалізувати за допомогою програмно визначеного ICN. Також обговорювалася роль віртуалізації в NDN (архітектура, заснована на ICN) і окреслили оптимізацію трафіку, розробку трафіку та керування перехопленням у мережі як переваги реалізації NDN перед ПКМ, особливо для мультимедійного трафіку.

Сучасна архітектура Інтернету базується на наскрізному контролі зв’язку, що забезпечує найкращі послуги. Це важливо для передачі даних, але не для мультимедійного трафіку. Мультимедійні програми, такі як потокове відео, відео на вимогу, відеоконференції, WebTV тощо, потребують стабільних мережевих ресурсів і допускають особливу кількість затримок, тремтіння та частоти помилок. Забезпечення цих вимог ЯП потребує вибору оптимального шляху серед усіх шляхів, доступних у мережі. Для цієї мети пропонуються такі архітектури QOS, як IntServ і

DiffServ , які мають труднощі. Їм бракує централізованого перегляду мережі, і вони обирають шлях поетапно, що може бути не оптимальним шляхом. Вони також потребують спеціалізованих вимог до програмного та апаратного забезпечення для впровадження. Програмно визначені мережі дають змогу вибирати різні шляхи для різних потоків трафіку за допомогою різних протоколів маршрутизації (виконуючи пріоритетність маршрутизації) на основі вимог потоку та централізованого перегляду мережі. Крім того, OF має деякі особливості QOS. У OF 1.0 пакети потоків можна поставити в чергу у вихідних портах. Цей механізм черги можна налаштувати за допомогою таких протоколів, як SNMP, CLI і NetConf. За допомогою допоміжного протоколу конфігурації під назвою OF-Config можна налаштувати максимальну та мінімальну швидкість передачі черг. У OF 1.1 додано підтримку перезапису бітів ECN (явне сповіщення про перевантаження). Найважливішою функцією є табличні вимірювачі, які підтримуються з OF 1.3. Ця функція дозволяє обмежити швидкість. Багато проектів пропонували методи вдосконалення або оптимізації для мультимедійного QOS через ПКМ.

ПКМ створює абстрактну картину мережі для спрощеного застосування політики та керування мережею, тому керування мережею застосовується з однієї логічної точки. Архітектура OF, як частина архітектури ПКМ, зробила управління мережею більш гнучким, контроль на рівнях деталізації пакетів або потоків. Керування в програмно визначеній мережі з централізованої логічної точки на таблиці потоків на контролерах і використання цих таблиць потоків, розподілених у мережі (комутатори), забезпечує гнучке керування мережею. Ось деякі зусилля, досягнуті в галузі управління мережею.

Конфігурація мережі через специфікації політик високого рівня в режимі розподіленої конфігурації низького рівня (з використанням CLI) і змінний стан мережі є складним. Також вирішувалися три проблеми керування мережею ПКМ: часті зміни, що відбуваються в мережі, використання мови високого рівня для конфігурації мережі, розпізнавання несправностей і помилок та усунення несправностей. Проектувалося це за допомогою Procera, керованої подіями системи управління, заснованої на парадигмі ПКМ, яка заснована на функціональному

реактивному програмуванні (FRP) і OF 1.0.0. Політики високого рівня можна перетворити на набір правил, і оператори можуть контролювати чотири домени: час, використання даних, статус автентифікації та потік трафіку. Іншою системою управління є інтегрована система управління та контролю мережі (I-NMCS) виявлення та виявлення несправностей. Ініціалізація та керування об'єднані разом і є модульними, мають слабкий зв'язок, мають низькі витрати та можливість розширення. I-NMCS використовується в гібридному режимі, що означає, що контролери оброблятимуть лише вибрані потоки, а решта потоків – мережеві протоколи. Це пояснюється думкою авторів, що традиційне керування мережею та ПКМ у майбутніх мережах співіснуватимуть одне з одним. Управління безпекою є ще одним аспектом управління мережею. Деякі програми, реалізовані в контролерах, забезпечують складну обробку більше, ніж безпеку. Представлялися також алгоритми системи управління інформаційною безпекою в поєднанні з нечіткою логікою та прототип системи виявлення вторгнень (IDS). Використання нечіткої логіки в цьому документі зменшує кількість рядків коду на 20-30%. Для підходу мережевого керування на основі подій пропонується система Lithium, а для мінімальної видимості продуктивності та контролю пропонується підхід до програмованої вимірювальної платформи, результатом якого є BISmark. Також представлялася проблема управління онлайн-конфігурацією, яка використовує OF і включає гнучкість, точність, надійність і масштабованість. Ця структура складається з двох частин: сегмент виявлення та фільтрації подій катастрофи та сегмент кореляції катастроф і керування детекторами. Більше зусиль докладається в сферах управління мережею від продуктивності до безпеки.

Віртуалізація мережі є однією з важливих областей досліджень сучасної мережі, яка дозволяє користувачам спільно використовувати ресурси та інфраструктуру. ПКМ завдяки центральному контролеру розглядається як рішення для управління віртуальними мережами. Переваги використання мережевої віртуалізації на основі префіксів рівня 2 (L2PNV) для віртуалізації мережі складаються з простоти конфігурації та гнучкості полів заголовка, що дозволяє користувачам створювати різні фрагменти та іншу віртуальну мережу. Міжрівневий

підхід для ізоляції мережі на основі OF для оптимізації віртуалізації мережі без втручання між різними зрізами, щоб користувачі могли змінювати поведінку власної віртуальної мережі. Запропоноване рішення базувалося на FlowVisor і SCML. Рівень контролю та управління фрагментами (SCML) використовується для управління та моніторингу операцій інфраструктури сегментів.

FITS, тестовий стенд для повністю ізольованої віртуальної мережі з різним QoS. FITS надав можливість дослідникам вибрати Xen, гіпервізор для віртуалізації з найкращою продуктивністю та високою здатністю керувати ресурсами, або OF для тестування та проведення своїх експериментів. Інструменти вимірювання FITS відстежують стан фізичної та віртуальної мережі, що допомагає адміністратору оптимально керувати ресурсами та розподіляти їх.

ВИСНОВКИ ДО РОЗДІЛУ 2

Використання мобільних пристроїв, нових технологій, таких як хмарні обчислення та віртуалізація, призвело до зміни моделей трафіку. Зростання великих даних у центрах обробки даних викликає потребу у високій пропускній здатності мережі та її масштабуванні. Щоб забезпечити ці потреби, мережеві пристрої стають складнішими. Крім того, для адміністраторів було б важко та довго налаштовувати окремі пристрої через навіть незначні зміни в мережі, такі як додавання або виключення пристрою. Вони повинні змінити конфігурацію багатьох комутаторів і маршрутизаторів, ACL, що може спричинити неузгодженість і помилки.

Ідея програмованих мереж була введена для вирішення цих проблем і сприяння розвитку мережі. Як наслідок, програмно-конфігурована мережа є новою парадигмою, яка революціонізувала традиційну мережеву архітектуру. ПКМ фактично відокремлює площину керування від площини даних і переміщує її на централізований сервер під назвою контролер. Він переміщує складність керування мережею в програмний контролер і забезпечує абстракцію базової інфраструктури. Це дозволяє простим пристроям даних і мережевим пристроям створювати площину керування прямо програмованою та керованою централізовано.

Архітектура ПКМ забезпечує програмованість, гнучкість і надійність у мережі. Оператори мереж можуть запроваджувати власні протоколи, правила та політики за допомогою загальних мов програмування. Вони можуть досягти гнучкого контролю над мережевими службами, такими як маршрутизація, інженерний трафік, QOS і безпека. Мережа може адаптуватися залежно від вимог користувачів. Керування мережею та конфігурації має можливість автоматизації за допомогою централізованого контролера та стандартного відкритого API, що полегшує масштабування мережі. Використовуючи ПКМ, адміністратори можуть додавати функції в площину керування без зміни площини даних або вдосконалювати пристрої в площині даних без зміни площини керування. Відокремлення площини управління від інфраструктури також є важливим, оскільки це зменшує витрати та незручності тестування нових ідей і стратегій у мережі або розгортання нових архітектур. У даному розділі я представив впровадження та тестування мереж, програми ПКМ і відкриті дослідницькі області та описав існуючі проблеми ПКМ.

Програмно-конфігуровані мережі можна застосовувати в бездротовій сенсорній мережі. Загалом використання ПКМ у мережах WSN забезпечило такі переваги, як гнучкість, спрощене керування, оптимізоване використання ресурсів тощо. Контролери мережі мають повноваження встановлювати політики для підтримки кількох додатків, використовуючи бездротову мережу, визначену програмним забезпеченням на основі датчиків. Крім того, цей підхід дозволить використовувати ті самі сенсорні вузли для кількох програм. OF можна використовувати для застосування гнучкого керування в бездротових сітчастих мережах. Цей підхід має переваги як у мережах Mesh, так і в OF, які включають самоналаштування та гнучку переадресацію відповідно. Щоб застосувати концепцію абстракції до бездротової спеціальної мережі смартфона, було розроблено програмно визначену мережу в спеціальних мережах. Ця гібридна платформа була реалізована на операційній системі Android. Цільова платформа є більш модульною та легшою для модифікації та розширення її компонентів. Інші випадки використання та про переваги ПКМ, такі як управління перешкодами між сотами та керування мобільним трафіком. OF може забезпечувати безперебійну передачу, динамічне управління ресурсами для

бездротового транспортного зв’язку, оптимізацію енергоспоживання в мережі мобільного транспортного зв’язку, безпеку та оптимізацію зворотного зв’язку тощо.

Безпека програмно-конфігурованих мереж має бути всюди:

A) архітектура та її контролер, програми, пристрої, канали (TLS з відкритим текстом) і таблиця потоків,

B) служби (для захисту доступності),

C) підключені ресурси

D) інформація.

Крім того, надійна структура політики для перевірки та балансування контролерів, політики відновлення, звітності та розгортання безпеки все ще дуже потрібні. Рішення мають бути простими в розгортанні та обслуговуванні, економічно ефективними та надійно безпечними. Нова категорія під назвою програмно-визначена безпека (SDSec), яка є прикладом віртуалізації мережевих функцій (NFV), забезпечує примусове забезпечення безпеки мережі, відокремлюючи площину контролю безпеки від площин обробки та пересилання.

Окрім безпеки, доступність (існування контролерів), гнучкість, контролери та сумісність програм, надійність зв’язку та контролера є значними проблемами. Централізований контролер може відновити себе в деяких процесах, використовуючи потоки резервного копіювання не так швидко, як очікувалося.

Крім цих проблем, існують деякі проблеми з реалізацією, наприклад наявність відповідних полів у потоці, кількох таблиць і їх великої кількості записів потоку, інструкцій і дій, програмування рівня потоку та власне програмування контролерів, які слід враховувати. Також відсутність стандартних API у разі перекривання домену серед контролерів, необхідність API шифрування для пакетів площини даних, API ін’єкції для пакетів і миттєвих API для таких служб, як IDS і брандмауер на комутаторі, відсутність операцій у разі відсутності контролера, існування інших форматів пакетів також розглядаються.

РОЗДІЛ 3
МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ПКМ

3.1. Оновлення мережевих структур програмно-конфігурованих мереж

Щоб побачити потребу в транзакційних оновленнях у програмно-конфігурованих мережах, розглянемо приклад мережі з Рис. 3.1. Вона має вісім комутаторів (від Комутатор 1 до Комутатор 8) і чотири вузли користувача (від користувача 1 до користувача 4). Ним керує один контролер із двома додатками ПКМ, Зелений Додаток і Блакитний Додаток, які змагаються за певний ресурс. Це може бути пропускна здатність посилання або навіть таблиця потоків комутатора. Припустімо перше, аби експозиція була конкретною. Зауважте також, що в останньому випадку це можуть бути буквально будь-які програми. Отже, нехай бюджет пропускної здатності всіх посилань у мережі становить 1,5 Мбіт/с, тоді як програми збираються зарезервувати шляхи по 1 Мбіт/с кожна. Якщо резервування є одночасним, може статися такий результат: одна програма зарезервувала посилання Комутатор 2 - Комутатор 5, а інша утримує посилання Комутатор 5 - Комутатор 7. Таким чином, жодна з них не зможе продовжити, обидва повинні будуть відмовитися від своїх бронювання.

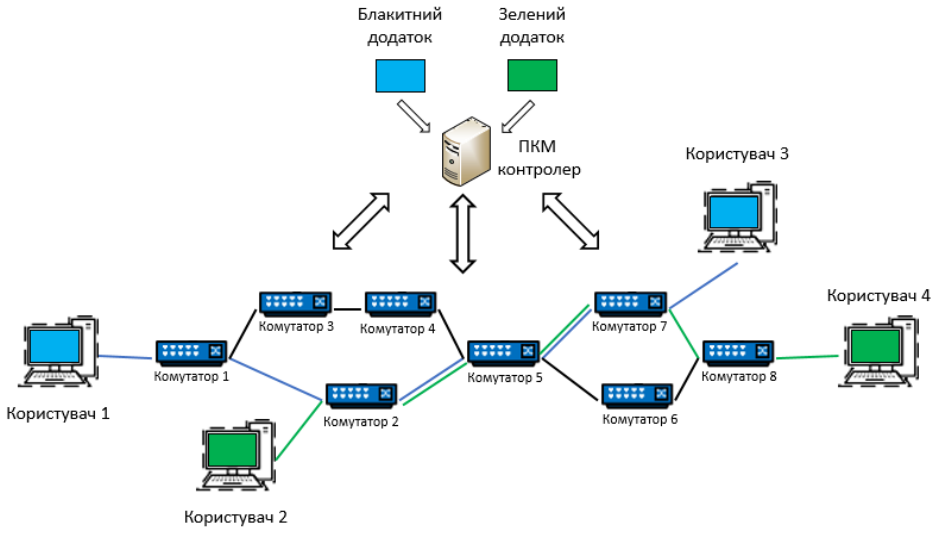

Рис. 3.1. Приклад мережі для ілюстрації неатомних і неузгоджених оновлень.

Ця проблема є артефактом паралелізму, який властивий будь-якому розгортанню ПКМ, централізованому чи розподіленому, з одним чи кількома контролерами. Якщо говорити конкретно, то ми маємо справу з випадком так званого «непослідовного читання». Нехай x і y позначають доступну пропускну здатність каналів Комутатор 2 - Комутатор 5 і Комутатор 5 - Комутатор 7 відповідно. Тоді наведений вище опис еквівалентний наступному шаблону чергування операцій читання та запису: [14]

$$r_1(x)r_2(y)w_1(x)r_1(y)w_2(y)w_1(y)w_2(x), \tag{3.1}$$

де нижні індекси позначають дві програми. Я стверджую, що цей розклад не підлягає конфліктній серіалізації, тобто він не може бути еквівалентним будь-якому послідовному розкладу. Таким чином, це має бути усунено за допомогою відповідних механізмів керування паралелізмом. Після огляду доступних механізмів і їх придатності для ПКМ, у даній роботі буде запропоновано повне вирішення цієї проблеми.

Ідея транзакційних оновлень була розроблена в області систем управління базами даних (СУБД). У транзакційних СУБД менеджер транзакцій (МТ) координує транзакції, які охоплюють кілька менеджерів ресурсів (МР). МР реалізують механізм керування паралелізмом для підтримки одночасних запитів на зміни до локального ресурсу в більш-менш суворому режимі. Залежно від цієї суворості, керування паралелізмом може бути песимістичним або оптимістичним і дає різні рівні ізоляції, поступово приймаючи можливі конфлікти на користь більшого паралелізму і, отже, кращої продуктивності. На жаль, як показують наші приклади, конфлікти можуть бути справжньою проблемою для деяких програм ПКМ; отже, далі я зосереджуюсь на планувальниках, які відповідають високим вимогам ізоляції.

Двофазне блокування (2PL) – песимістичний механізм. МР використовує 2PL, щоб надати блокування даних для однієї транзакції, змушуючи інші транзакції чекати, якщо вони хочуть отримати доступ до тих самих даних. У своїй базовій формі 2PL гарантує можливість серіалізації. Два додаткових варіанти 2PL: S2PL (суворий

2PL) і SS2PL (сильний 2PL) забезпечують відновлюваність і безкаскадність відповідно. Планувальники впорядкування зобов'язань (ПВЗ) налаштовані оптимістично. Вони серіалізують виконання транзакцій шляхом побудови та аналізу графіка черговості транзакцій. Зазвичай це дає кращу продуктивність, ніж песимістичні планувальники, але вимагає додаткових витрат, складності алгоритмів, які має запускати МР.

Коли транзакції охоплюють кілька МР, може знадобитися забезпечити глобальну серіалізацію для МР. Якщо всі МР синхронізовані та мають спільну інформацію, напр. мітки часу, це можна зробити за допомогою протоколу впорядкування міток часу. Як альтернатива, а МТ, який використовує протоколи атомарної фіксації (ПАФ), такі як 2PC, і координує МР, які забезпечують механізм контролю паралельного виконання, такий як SS2PL, цілком підійде. Пакет групує пов'язані зміни стану на комутаторі та виконує їх атомарним та ізольованим способом. Пакети можуть бути попередньо перевірені на комутаторах і зафіксовані контролером. Однак специфікація OpenFlow вказує на те, що виконання пакета може виникнути збій під час фіксації. Таким чином, пакети не можуть забезпечити ізоляцію та атомарність усієї мережі, коли одночасні оновлення всієї мережі впливають на кілька комутаторів.

Нещодавно було запропоновано фреймворк синхронізації для координації розподілених оновлень, у якому кілька контролерів одночасно оновлюють комутатор. Вони ставлять перемикач із встановленим ідентифікатором політики та додають примітиви для читання та оновлення значення штампа. Програма ПКМ може встановити політику, лише якщо їй відоме поточне значення штампа - це гарантує, що стан комутатора тим часом не було змінено іншим контролером. Оновлення працює таким чином: програма створює пакет із примітивом оновлення штампу на початку, а потім командами оновлення. Використання комплекту для встановлення разом із штампуванням забезпечує можливість серіалізації та відновлення, але лише якщо такі оновлення впливають на один комутатор. Залишається незрозумілим, як поширити це на оновлення всієї мережі.

Керуючись мотивацією, подібною до нашої, було представлено концепцію запланованих пакетів (тим часом включену в OpenFlow v1.5). Це дозволяє виконувати команди в групі в заздалегідь визначений час. Таким чином, ця робота є найближчою до нашої, оскільки вона може серіалізувати виконання одночасних оновлень і, отже, створювати послідовну історію. Однак обраний підхід обходиться ціною ідеальної синхронізації часу між елементами мережі і будь-яка неправильна синхронізація може призвести до неправильних розкладів. Крім того, оскільки час оновлення комутатора залежить від апаратних можливостей, навантаження на керування та характеру оновлень, час завершення фіксації пакетів може не синхронізуватися, навіть якщо час початку фіксації пакетів є, що робить пакети на льоту під час оновлення обробляється проміжним станом. Нарешті, для виконання таких запланованих пакетів потрібен центральний орган для планування всіх оновлень, що призводить до вузьких місць і єдиної точки збою. У розподіленій площині керування примірникам контролера потрібен протокол і накладні витрати, щоб узгодити час виконання їхніх оновлень.

Було запропоноване транзакційне проміжне програмне забезпечення для семантичної композиції розподілених оновлень. Він перехоплює оновлення, серіалізує їх і за потреби змінює, щоб запобігти заміні існуючої конфігурації мережі. Оскільки проміжне програмне забезпечення обробляє оновлення послідовно, воно має бути однопотоковим, що перешкоджає використанню переваг розповсюдження рівня керування. Крім того, пропозиція не містить технічних деталей реалізації або аналіз складності дизайну проміжного ПЗ.

Ряд робіт розглядає впорядкування часу виконання команд в рамках одного мережевого оновлення та пропонує механізми, які забезпечують різні властивості оновлення. Було розроблено двофазний протокол оновлення для досягнення узгодженості кожного пакета, який гарантує, що кожен пакет, що проходить мережею, ніколи не оброблятиметься сумішшю двох конфігурацій. Як варіант, запропоновано Dionysus, механізм для оновлень мережі без перевантажень. Це вимагає оновлення правила, яке приносить новий потік до посилання, яке має відбуватися після оновлення, яке видаляє існуючий потік, якщо посилання не може

підтримувати обидва потоки одночасно. Однак ці пропозиції не вирішують проблеми паралельності в ПКМ.

Я коротко оглянув доступні рішення щодо атомарності та ізоляції та проаналізував їх придатність для ПКМ. Щоб застосувати транзакційну архітектуру СУБД до програмно-конфігурованих мереж, цікаво знати, де мають працювати МТ і МР? Хоча цілком зрозуміло, що МТ має бути модулем у контролері ПКМ, існує кілька варіантів для МР.

По-перше, можна розмістити всі МР локально в контролері ПКМ, де вони діятимуть як зображення комутаторів. Завдяки цьому ми можемо вибирати будь-який контроль паралельності в МР, оптимістичні однаково хороші, як і песимістичні, навіть якщо вони складніші. Однак виникає проблема, якщо ми виходимо за рамки розгортання одного контролера: важко підтримувати образи комутаторів у кількох контролерах, які одночасно оновлюють мережу.

З іншого боку, можна включити МР у комутатор. Це найменше обмеження щодо цільового розгортання. Недоліком є те, що нам потрібно подовжити комутатор. Оскільки планувальники ПВЗ повинні підтримувати графік пріоритетів, буферизувати отримані запити транзакцій і змінювати порядок відповідних комітів, реалізувати оптимістичний механізм у комутаторі може бути нелегко. Навпаки, песимістичні видаються здійсненними, оскільки МР повинні запускати лише планувальник 2PL і реалізовувати когортну сторону 2PC2. По-третє, ми можемо розмістити МР у проміжному програмному забезпеченні, намагаючись усунути недоліки двох вищезгаданих крайнощів. Але потім нам потрібен новий протокол, який МР могли б використовувати для координації оновлень їх контрольовані домени.

У даній кваліфікаційній роботі я інтегрую МР у комутатор. Я вважаємо це розумним першим кроком до інтеграції оновлень транзакцій із ПКМ. Інші варіанти можуть досліджуватися в майбутніх роботах.

Тепер я коротко розглянув можливості інтеграції запропонованої архітектури з деякими з існуючих механізмів узгодженості. В архітектурах на основі проксі, напр. VeriFlow або NetPlumber, МТ працюватиме як основна служба в проксі. Коли

VeriFlow або NetPlumber перевірять оновлення, вони надсилають його в мережу за допомогою виклику API МТ. Те саме стосується інтеграції з механізмом(ами) забезпечення узгодженості, інтегрованим у контролер, напр. SE - Прожектор. Я не розглядаю інтеграцію з такими механізмами, як Dionysus і Cupid, оскільки вони передбачають конкретні типи додатків і стани мережі, що суперечить власним припущенням і вимогам для досягнення механізму агностику додатків ПКМ.

На Рис. 3.2. показано нашу архітектуру високого рівня. Доповнення до стандартних моделей програмно-конфігурованих мереж показано червоним кольором. До них належать менеджер транзакцій (МТ), який працює в контролері ПКМ, менеджер ресурсів (МР), що працює в комутаторі, і транзакційний Південний інтерфейс (ТПІ), розширення південного інтерфейсу для зв'язку МТ - МР. МТ отримує запити на оновлення від програм ПКМ і спілкується з необхідними МР від їх імені, тобто обробляє транзакції. Наш МР по суті перетворює комутатор програмно-конфігурованих мереж на середовище, що підтримує транзакції, із чітко визначеними станами, до яких можна отримати доступ і змінити лише відповідно до семантики транзакцій (наприклад, невдалі транзакції можна скасувати).

Архітектура, очевидно, застосовується до розгортання ПКМ з одним контролером. Крім того, це стосується розгортань із кількома контролерами, у яких кожен контролер, тобто кожен МТ, пов'язаний з усіма комутаторами мережі.

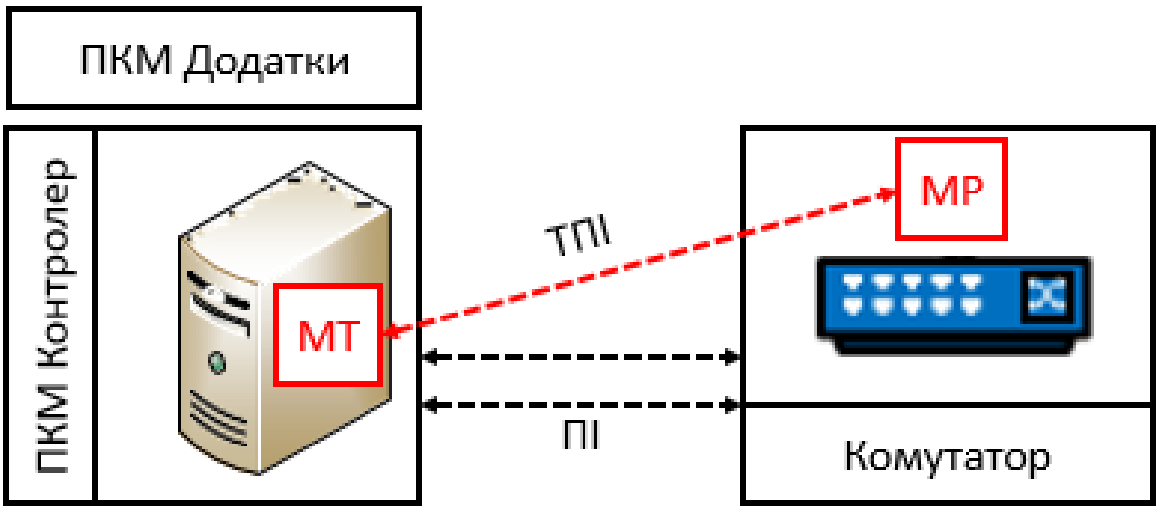

Рис. 3.2. Транзакційна архітектура ПКМ.

Розглянемо типову послідовність кроків у циклі оновлення транзакційної мережі:

1) Після отримання запиту на оновлення мережі від програми ПКМ, МТ надсилає так зване повідомлення Vote до МР, що беруть участь в оновленні. Ресурс (комутатор) інтерпретує це повідомлення як ініціацію транзакції та голосування ACP.

2) Після отримання Vote, відповідно до SS2PL, кожен МР локально блокує ресурс, тому він стає недоступним для інших запитів (наприклад, від іншої МТ або програми) до подальшого сповіщення від ініціального МТ. Кожен МР намагається застосувати всі запитані зміни до відповідної робочої області. Якщо це вдається, МР надсилає повідомлення підтвердження назад до МТ. В іншому випадку МР надсилає Reject і негайно розблоковує ресурс.

3) Якщо МТ отримав підтвердження від усіх МР у поточному оновленні, він починає фазу фіксації, надсилаючи їм повідомлення про фіксацію. Якщо принаймні один МР відхилив запит (наприклад, він уже заблокований) або не відповів протягом очікуваного часу, МТ перериває оновлення, надсилаючи Відкат до МР, які відповіли ConfiMP. Таким чином, навіть якщо МТ отримує підтвердження від усіх комутаторів, крім одного, він зніме отримані блокування та почне заново. Це можлива область покращення, яка буде досліджена в майбутній роботі.

Під час фіксації МР активують свої проміжні області, тоді як під час відкату вони скидають їх. В обох випадках вони відправляють Finished назад до МТ і знімають блокування.

Щоб забезпечити довговічність, ми забороняємо чіткі правила самозакінчення в ресурсах; натомість ми використовуємо скоординовану комбінацію методів, наведених вище, щоб досягти правильного ефекту всієї мережі.

Зверніть увагу, що я об’єдную ініціацію транзакції та початок протоколу атомарної фіксації, що може обмежити діапазон підтримуваних транзакцій лише записом оновлень, тобто ми виключаємо запити на читання. Я вважаю, що таких оновлень достатньо через обмеження OpenFlow: справді, згідно з OpenFlow v1.4 і пізнішими версіями, повідомлення Read-State можуть отримувати лише дуже обмежену інформацію з комутатора (наприклад, значення лічильників), більшість з

яких керується площиною даних; ці дані недоступні для керування транзакціями, тобто транзакції, які в них записуються, не контролюються OpenFlow. Оскільки ми не прагнемо запобігати ситуаціям, коли програми ПКМ можуть зчитувати мережеву інформацію, яка стає застарілою лише через мить через зміни площини даних, і радше зосереджуємося на вирішенні потенційних конфліктів з інших одночасних оновлень, ми ігноруємо «читання перед записом». . Об'єднання замків і голосів ACP дозволяє скоротити час блокування перемикача, який є параметром, пов’язаним з продуктивністю, наслідки якого я аналізую та показуємо в наступному розділі.

3.2. Впровадження та тестування ПКМ

Багато комутаторів і контролерів доступні для реалізації програмно визначеної мережі. Але є також способи тестування ідей у програмно-конфігурованих мереж, наприклад використання симуляторів, емуляторів і випробувальних стендів. NetFPGA можна використовувати для побудови вузла ПКМ. Налагоджувачі також доступні для тестування контролерів. У цьому розділі я описую та порівнюю доступні симулятори та емулятори ПКМ, такі як Mininet, NS-3 і Estinet.

Mininet, платформа емулятора, що використовує протокол OF, запускає набір кінцевих хостів, комутаторів, маршрутизаторів і посилань на одному ядрі Linux за допомогою легкої віртуалізації. Компоненти Mininet діють як компоненти реальної мережі. Цей емулятор має багато інструментів для перевірки можливої пропускної здатності, зв’язку між вузлами та найглибшими вузлами, а також швидкості потоків. Ці інструменти називаються Ipref, Ping, PingAll, PingPair, CBench, а також Wireshark для перегляду мережевого трафіку. Mininet використовується розробниками, викладачами та дослідниками, і це завдяки легкій взаємодії з мережею за допомогою CLI та API, функціям налаштування та обміну, а також функції розробки на реальному обладнанні. Слід зазначити, що Mininet активно розвивається і підтримується. Даний емулятор широко використовується завдяки швидкому запуску простої мережі, підтримці користувацьких топологій і пересилання пакетів, запуску реальних програм, доступних у Linux, роботі на ноутбуках, серверах, віртуальних

машинах, можливості спільного використання та реплікації, простоті використання, знаходженню в відкритий вихідний код і стан активної розробки. На відміну від цих переваг, Mininet також має деякі недоліки: відсутність можливості передачі величезної кількості даних в одній системі, відсутність підтримки довільних контролерів OF, підтримка лише однієї платформи (ядра Linux), використання NAT із коробки, спільне використання файлова система хоста та простір PID та відсутність поняття віртуального часу.

NS-3 - це симулятор мережі дискретних подій, який підходить для дослідників і викладачів. Бібліотека NS-3 поділена на багато модулів, організованих на вкладці модулів. Один із цих модулів OF сумісний із ПКМ. NS-3 має об'єкт OpenFlowSwitchNetDevice, який поводиться як комутатор і є OF сумісним. Цей об'єкт реалізує таблицю потоків для всіх отриманих пакетів, а також підключення до контролера, як і архітектура ПКМ. Два контролери доступні в оригінальному пакеті, DropController і LearningController (на основі алгоритму перемикання навчання). Цей симулятор має такі переваги: додавання нових протоколів, невелика відстань між реальною мережею та змодельованою мережею, наявність інтеграції та можливість налаштування без переробки ядра симулятора. Недоліками NS-3 є: втрата доступних моделей, відсутність візуального інтерфейсу для створення топології та видимих можливостей на експериментальному рівні.

Симулятор і емулятор EstiNet підтримує багато комутаторів OF 1.3.2 і 1.0.0. Окрім цієї переваги, у режимі моделювання EstiNet; Контролери POX, NOX, Floodlight і Ryu виконуватимуть роль площини контролера ПКМ. У режимі емуляції EstiNet ці контролери можуть працювати на зовнішній машині, яка відрізняється від машини, яка імітує комутатори. Також у цьому режимі можлива реалізація контролера як спеціального апаратного пристрою за допомогою кабелю Ethernet, що забезпечує дистанційне керування. Інші переваги використання цього симулятора/емулятора: точність, швидкість, повторення та масштабованість. EstiNet має унікальну можливість, яка називається «методологією симуляції повторного введення ядра». Використовуючи це, тестування нової прикладної програми контролера дослідником OF є простим і ефективним.

NetFPGA - це програмно-апаратна платформа, призначена для дослідників і використовується для навчання. Зараз він доступний на 2 платформах: NetFPGA-1G (1G) і NetFPGA-10G (10G). Завдяки програмному забезпеченню з відкритим вихідним кодом і недорогому апаратному забезпеченню його враховують багато студентів. NetFPGA складається з PCI з чотирма портами Ethernet, Xilinx Virtex II pro, статичної оперативної пам'яті та подвійної швидкості дати (DDR2) SDRAM. Завдяки згаданим перевагам і гнучкості платформи NetFPGA вона призначена як одне з рішень для реалізації ПКМ. Програмована вентильна матриця (FPGA) дозволяє програмувати обробку ядра за допомогою визначеної користувачем логіки, а вбудоване ядро дозволяє програмувати функції керування.

Випробувальні стенди OF – це експериментальні середовища, які в основному розроблені для тестування нових програм із використанням OF. В даний час існує кілька відкритих випробувальних стендів, які можна використовувати для академічних досліджень. У продовженні представлені та описані деякі з найважливіших тестових стендів OF.

GENI означає Глобальне середовище для мережевих інновацій, яке підтримується Національним науковим фондом. Це широкий набір інфраструктури, розроблений для підтримки експериментальних досліджень у мережах шляхом створення величезного випробувального стенду. Щоб досягти своєї мети, GENI об'єднав деякі платформи, такі як PlanetLab, Internet2, Emulab, тощо. На високому рівні він має перспективу експериментального тестового стенду, в якому всі компоненти будуть програмованими, об'єднаними та віртуалізованими, отже, це найкращий кандидат при масштабному розгортанні. На сьогоднішній день проект GENI у поєднанні з Internet2 створює мережу на основі ПКМ, готову до розгортання нової архітектури для нових мережевих послуг і майбутнього Інтернету.

OFELIA: фінансується Сьомою рамковою програмою (FP7) Європейського Союзу. Ідея, що лежить в основі OFELIA, — це тестовий стенд, у якому дослідники можуть динамічно контролювати та розширювати мережу через OF. Інфраструктура OFELIA утворена набором взаємопов'язаних островів, кожний з яких управляється незалежно. Застосування віртуалізації дозволяє кожному експериментатору отримати

зріз мережі. Кожен фрагмент формується віртуальними машинами для запуску клієнтів і сервера, віртуальна машина, яка відповідає типовому контролеру OF і віртуальній мережі OF. OFELIA Control Framework (OCF) — це загальна система контролю для проведення експерименту. OCF надає інструменти для верифікації користувача та доступу, виділення зрізу, налаштування мережі.

FIBRE: Головною метою FIBER є створення спільного простору між Бразилією та Європою для майбутніх архітектур Інтернету. Ключова ідея цього проекту полягає в тому, щоб побудувати об'єднаний тестовий стенд шляхом поєднання бездротових мереж і глобальної мережі. Бездротова мережа та глобальна мережа керуються за допомогою OF.

Як згадувалося раніше, контролер ПКМ є програмованим, і ця функція збільшує ймовірність випадкових помилок. Загалом пошук помилок є складним і трудомістким, тому відладчики стали одним із важливих компонентів OF/ПКМ. Налагоджувачі — це інструменти, які використовуються для тестування та діагностики програм і дозволяють програмістам взаємодіяти з програмою під час її виконання на комп'ютері. Налагоджувачі OF дозволяють нам відстежувати поведінку потоку пакетів, щоб перевірити, чи мережа працює належним чином.

VeriFlow містить рівень між контролером і хостами, який аналізує та перевіряє конфігурацію мережі, щоб знайти помилки, не маючи негативного впливу на продуктивність мережі. Вони стверджували, що реалізація VeriFlow сумісна з контролером NOX, і продемонструвала, що вона здатна перевіряти правила плану контролю в реальному часі та запобігати помилкам, які впливають на належне функціонування мережі.

FlowChecker — це інструмент аналізу конфігурації. Використання цієї системи забезпечує можливість перевірки правильності конфігурації плану передачі даних і перевірки узгодженості різних пристроїв у мережі OF шляхом інтерпретації внутрішньої/міжкомутаторної таблиці потоків за допомогою бінарних діаграм рішень. Аналіз конфігурації можна проводити під час роботи мережі. Ця функція корисна для визначення QoS. Підхід для збору параметрів мережі та використав ці дані для моніторингу, аналізу та налагодження ПКМ. Основна інформація для

налагодження збирається з таблиці потоків, різної статистики трафіку та повідомлень контролера. Деякі різні інструменти використовувалися для налагодження та перевірки трафіку між контролером і комутаторами за допомогою інтеграції Wireshark, яка була заявлена як найефективніший підхід.

3.3. Хмарні служби та центр обробки даних програмно-конфігурованих мереж

Однією з областей, до якої ПКМ приділяли велику увагу, є хмарні служби та центр обробки даних. Однією з основних характеристик хмари є те, що користувачі отримують адекватні ресурси на основі потреб у режимі реального часу. Управління хмарою є найважливішою проблемою, яка завжди була, і для цього було запропоновано багато рішень. ПКМ високо оцінюється як одне з найновіших рішень, яке дозволяє легко налаштовувати та керувати хмарою та центром обробки даних. Впровадження хмарних центрів обробки даних за допомогою OF виявило, що реалізація на основі програмно-конфігурованих мереж є швидшою та легшою для налаштування через централізований контролер ПКМ та план управління абстракціями. Іншою проблемою хмарної системи є витрати на підтримку, оскільки ПКМ завдяки централізованому управлінню розташуванням добре вирішує цю проблему.

Oracle ПКМ є прикладом системи, яка віртуалізує центр обробки даних за допомогою підключення визначень у програмному забезпеченні. Ця система з’єднує віртуальну машину з іншими віртуальними машинами та мережевими серверами за допомогою на 70 відсотків простішої інфраструктури. Використовувати конфігурацію інтерфейсу Oracle Fabric Manager і моніторинг віртуальної мережі можна з будь-якого місця. Стверджується, що вартість системи Oracle ПКМ порівняно із застарілою мережею на 50 відсотків менша, оскільки ви отримуєте перевагу пропускної здатності до 80 ГБ/с між серверами.

Raghavendra та інші в представляють NetGraph, програмну архітектуру для керування хмарними системами на основі ПКМ. Ця система є спільною бібліотекою

графів і надає модуль із набором API для моніторингу та діагностики хмарної системи.

Hedera, який представлений Al-Fares et al., визначає динамічне планування потоку для мереж центрів обробки даних з використанням OF. Центральний планувальник дає змогу балансувати навантаження на основі стану активного потоку в усій системі.

Також пропонується міжшарова архітектура відмовостійкості для з'єднання центрів обробки даних із підтримкою OF. Розгортання віртуальних машин на сервері використовується на основі типу служби. Для обслуговування ресурсів використовуються керуючі ресурси, ступінь їх зайнятості та резервні механізми. Ця система розроблена для оптичних мереж Flexi-Grid. Хуей Янг та інші стверджували, що система має покращену наскрізну реакцію та оптимізоване використання ресурсів.

Завдяки централізованій архітектурі ПКМ він використовувався для виявлення проблеми безпеки. Нагляд програмно-конфігурованих мереж за всім мережевим потоком і моніторинг поведінки користувачів дозволяють ПКМ швидко виявляти атаку та запобігати подальшій шкоді. Багато дослідників запровадили механізми для виявлення атак Dos і DDos через їх поведінку, засновану на затопленнях. Приклад такої системи наведено Junho Suh et.al, яка реалізована на платформі NetFPGA-OF. Представлена система, яка використовує перемикач OF на межі, щоб пропускати лише безпечний трафік, який визначено в таблиці потоків, і LISP (протокол розділення локатора/ідентифікатора) для розпізнавання надійного користувача. Були досліджені рішення для атаки на основі сканування. Представлена система OF Random Host Mutation (OFRHM), яка змінює реальну IP-адресу кожного хоста на випадкову віртуальну IP-адресу. За допомогою цього механізму фальшиву IP-адресу можна легко виявити, а система запобігає великому відсотку атак, таких як приховане сканування, розповсюдження хробаків тощо. Відповідальність часто призначається віртуальній IP-адресі хосту.

Розгляд безпеки на основі політики є ще одним рішенням безпеки. Представлена багаторівнева система безпеки, яка запобігає інформації певного рівня, зібраній хостом того ж або нижчого рівня. При розробці системи використовується

OF, який використовується для моніторингу пакетів і перевірки вмісту, щоб фільтрувати пакети з проблемою безпеки. Основна ідея полягає в тому, щоб динамічно ізолювати мережевий пристрій від атаки всередині локальної мережі за допомогою OF. У запропонованій архітектурі компонент IDS відповідає за виявлення атак і розпізнавання незахищених пристроїв і інформує контролера OF. Стверджується, що результати показали, що ця архітектура достатньо ефективна в реальній локальній мережі.

Однією з проблем виявлення аномалій підходу ПКМ є те, що коли мережевий трафік високий, збір повних даних із таблиці потоків є неефективним, тому існує рішення для оптимальної системи виявлення в реальному часі. Об'єднано з sFlow і OF, що використовує вибірку замість повної інформації про потік і використовував алгоритм на основі ентропії для виявлення та пом'якшення аномалії. В умовах низького трафіку продуктивність системи порівнянна з рідною архітектурою OF.

ВИСНОВКИ ДО РОЗДІЛУ 3

У сучасних програмно-визначених мережах мережеві оновлення не є ні атомарними, ні ізольованими. Таким чином, якщо вони виконуються одночасно, вони можуть призвести до неузгодженості, наприклад двох конфліктуючих політик, встановлених у різних частинах мережі. У даному розділі пропонуються транзакційні (тобто атомарні та ізольовані) мережеві оновлення, втілені в простій і зрозумілій архітектурі, яка є паралельною системі керування базами даних і включає в себе менеджер транзакцій (МТ), що працює на контролері, і менеджер ресурсів (МР), який працює на перемикач. Я впроваджую їх як розширення до сучасного контролера (Floodlight) і комутатора ПКМ (OVS). Реалізація не тільки демонструє здійсненність дизайну, але й показує легкість його реалізації. Я також оцінюю наш дизайн, вимірюючи, скільки часу потрібно для надсилання транзакційних оновлень і з якою пропускною здатністю за різних показників надходження оновлень, для різних типів оновлень і основних топологій. Таким чином, ми дізнаємося, що, наприклад, з маленьким кроком надлишковості, ми можемо налаштувати майже всі потоки, які

надходять зі швидкістю до 1000 $с^{-1}$, надаючи кожному затримку в межах лише кількох мілісекунд.

Хоча програмно-конфігурована мережа прокладає шлях до програмних мережевих оновлень на основі подій, вони не дуже корисні для розробників у поточній формі. Дійсно, у поточному ПКМ немає гарантії, що стан мережі не буде змінено, тоді як керуюча програма намагається застосувати деякі зміни. Події потоку надходять до контролера нескоординованим способом і, відправлені в керуючі додатки, можуть призвести до взаємно суперечливих або суперечливих заяв. Це може мати нешвидкий загальний ефект, що призведе до часткової, конфліктної або просто неправильної сукупної політики, активованої в комутаторах. Проводячи паралель із добре відомими властивостями ACID транзакцій бази даних, ПКМ отримає прибуток від оновлень мережі, які:

• Атомарне, що означає, що оновлення всієї мережі, що виходять за межі одного комутатора, або повністю успішні, або не виконуються взагалі.

• Послідовність, що означає, що загальномережні інваріанти та політики повинні зберігатися в міру розвитку стану мережі, тобто обмеження, накладені цією політикою, ніколи не порушуються.

• Ізольовано, що означає, що дві операції, що збігаються, виконуються одночасно та спрямовані на ті самі перемикачі, не можуть призвести до неочікуваних наслідків. По суті, ізоляція усуває невідповідності, які є результатом паралелізму як такого, а не семантики окремих операцій. Наприклад, якщо одна програма блокує тип потоку, а якась інша програма одночасно дозволяє цей самий тип потоку, тоді в ізоляції виграє той, хто прийде останнім, тобто тип потоку не можна заблокувати на наборі комутаторів і дозволити на іншому.

• Тривалість, що означає, що ефект транзакції зберігається необмежений час, якщо він не змінений іншою транзакцією.

На мою думку, програмно-конфігурована мережа має налагодити підтримку цих сервісів замість того, щоб перекладати тягар на розробника або просто нехтувати ними, як це відбувається зараз. З чотирьох наведених вище властивостей лише узгодженості наразі приділено достатню увагу. Я вважаю, що атомарність, ізоляція та

довговічність однаково важливі. Це справедливо не лише для «розподіленої площини керування», у якій кілька додатків керування, які знаходяться на потенційно різних контролерах, одночасно оновлюють мережу, але також і для найбільш типового розгортання програмно-конфігурованих мереж, а саме для одного контролера ПКМ, який запускає набір незалежних програм керування.

Я аналізую семантику конфліктів, які можуть виникнути, коли кілька керуючих додатків одночасно оновлюють мережу, і дійшли висновку, що так звані конфліктні серіалізовані графіки оновлення можуть їх усунути. Говорячи мовою бази даних, ми дозволяємо лише розклади оновлення з класу еквівалентності історій, які можна серіалізувати (CSR). Серед багатьох можливих алгоритмів планування (планувальників), які надають історію CSR, я вважаю, що краще - двофазний блокування (SS2PL) як правильний вибір. Основна причина полягає в тому, що SS2PL легко реалізувати в комутаторі ПКМ, як показує моє підтвердження реалізації концепції, що дає можливість підтримувати оновлення транзакцій у ПКМ за допомогою простої та зрозумілої архітектури, яка є паралельною системі керування базами даних і передбачає:

• менеджер транзакцій (МТ), що працює на контролері,

• менеджер ресурсів (МР), який працює на комутаторі.

Наша МТ також координує МР за допомогою протоколу атомарної фіксації (АФ) (наприклад, двофазної фіксації, 2PC), щоб досягти глобальної атомарності. Таким чином, наші МТ і МР також досягають глобальної серіалізації.

При такій архітектурі мережеве оновлення блокує необхідні комутатори, які стають фактично недоступними для інших під час оновлення. Моя оцінка зосереджується саме на розумінні того, чи є це обмеженням і в якій мірі. Таким чином, ми перевіряємо архітектуру для різних типів оновлення, швидкості оновлення та основних топологій і з’ясовуємо, що, наприклад, за допомогою невеликої надлишковості шляху є можливість налаштувати майже всі потоки, які надходять із швидкістю до 1000 $с^{-1}$, надаючи кожному затримка всього в кілька мілісекунд.

РОЗДІЛ 4
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ РІШЕНЬ

4.1 Методології дослідження програмно-конфігурованих мереж

Проблема розміщення контролера є однією з життєво важливих проблем у мережах ПКМ. Розміщення контролера в точному місці підвищить продуктивність мережі. Під час розміщення контролера виникає кілька проблем, таких як висока затримка під час зв’язку між контролерами, затримка розповсюдження між комутаторами та контролерами, відмовостійкість контролера та задоволення вимог до комутаторів.

Затримка між контролерами є складною проблемою під час розміщення контролерів. Нехай контролери (C1) і (C2), C∈C1 і C2 хочуть спілкуватися один з одним. Неточне розташування між цими контролерами під час розміщення контролерів збільшить затримку між контролерами, яку можна сформулювати як:

$$Lat_{C_1 \leftrightarrow C_2} = \frac{1}{C} \sum_C max_{C \in C_1, C_2} Lat, \tag{4.1}$$

де $Lat_{C_1 \leftrightarrow C_2}$ позначає затримку між контролером C1 і C2 і $max_{C \in C_1, C_2}$ позначає високу затримку під час зв'язку через неточне розташування контролерів.

Затримка розповсюдження між комутаторами та контролерами вплине на надійність зв’язку між ними. Нехай комутатори в мережі є s ∈ S, а контролери c ∈ C, тоді затримку поширення (PD) між ними можна сформулювати як:

$$PD_{S \leftrightarrow C} = \sum_N max_{S \leftrightarrow C} PD, \tag{4.2}$$

де $max_{S \leftrightarrow C} PD$ позначає збільшення поширення між контролерами та комутаторами та N позначає мережу ПКМ. Вибір високовідмовостійкого контролера також є важливим під час розміщення контролера. Для вищезазначених проблем під

час розміщення контролера запропонована робота має на меті забезпечити точне рішення для CPP з наступними цілями. Цілі такі: [15]

$$Minimize \rightarrow Lat_{C_1 \leftrightarrow C_2}, \tag{4.3}$$

$$Minimize \rightarrow PD_{S \leftrightarrow C}, \tag{4.4}$$

$$Maximize \rightarrow Controller\ fault\ tolerence. \tag{4.5}$$

Існуючі методи намагаються вирішити проблеми з розміщенням контролера. однак, ефективного рішення, яке б вирішило вищезазначені проблеми, ще не надано. Оптимальне розміщення контролера з урахуванням затримки в точному місці з урахуванням збоїв зв'язку уже було представлено. Оптимізоване рішення щодо розміщення контролерів для CPP з урахуванням пропускної здатності контролерів уже було представлено. Метод балансування навантаження для пом'якшення проблем під час розміщення контролера шляхом врахування затримки та стабільності контролера уже був представлений. Евристичний підхід для пом'якшення проблеми розміщення контролера з урахуванням часу обчислення уже була представлена. Загальні загальні проблеми, які використовуються в наведених вище документах:

• Існуючі роботи враховують лише затримку між контролерами та комутаторами. Однак для досягнення точного рішення для CPP необхідно враховувати зв'язок між контролерами після розміщення, що збільшує затримку зв'язку між контролерами та впливає на продуктивність мережі ПКМ;

• Вибір обмежень під час розміщення контролера – це затримка між комутаторами та контролерами, затримка розповсюдження та збій зв'язку. Однак рівень відмовостійкості контролера не враховувався, що також призводить до погіршення під час розміщення контролера;

• В існуючих роботах використовувалися евристичні алгоритми для задач розміщення контролера. Однак вони досягають меншої продуктивності з точки зору затримки та затримки поширення, оскільки параметри існуючих алгоритмів не були налаштовані ефективно. Крім того, розгляд окремих алгоритмів оптимізації обмежує їх неточним розміщенням контролера.

Щоб подолати недоліки, з якими стикаються існуючі роботи, запропонований метод спочатку будує мережу як графову структуру для покращення масштабованості мережі ПКМ. Після цього виконується вибір контролера для покращення продуктивності розміщення контролера. Вибір контролера здійснюється за допомогою алгоритму оптимізації (FA) Firefly, який враховує особливості контролера. Використання цього алгоритму оптимізації firefly полягає у виборі оптимального контролера з високою відмовостійкістю та потужністю. Після вибору оптимальних контролерів розміщують контролери в оптимальному місці з урахуванням відстані. Вибір оптимального місця для розміщення контролера використовується гібридним алгоритмом, який називається алгоритмом гармонійного пошуку (АПГ) і оптимізацією роєм частинок (АРЧ). АРЧ використовується для ініціалізації параметрів АПГ, що також покращує продуктивність розміщення контролера. Проблема розміщення контролера мінімізує затримку між контролерами та затримку розповсюдження між комутаторами та контролерами. Запропонована робота досягає покращеної пропускної здатності та продуктивності мережі за допомогою вищевказаних процесів. Запропоновану модель МК-ПКМ можна вважати застосовною до загальних характеристик мережі ПКМ і її можна використовувати ефективним, гнучким, масштабованим і надійним способом.

У цьому розділі описані методології дослідження запропонованого підходу МК-ПКМ. Пропонована робота забезпечує масштабованість, надійність і підвищує загальну продуктивність мережі за допомогою трьох процесів, які пояснюються наступним чином. На Рис 4.1. представлена загальна модель системи запропонованої архітектури МК-ПКМ з механізмом розподілу та вибором контролерів за алгоритмом FA.

Мережа розглядає кілька контролерів, комутаторів і пристроїв. Топологія мережі будується на основі неорієнтованої графової структури, яка визначається як:

$$G = (V, E, U), \tag{4.6}$$

де G представляє графік, U представляє кількість контролерів, E представляє межі, а V представляє з'єднання між комутаторами та контролерами. Ця топологія зменшує затримку між комутаторами та контролерами. Тут контролери та вузли є елементами пересилання, тому ми припускаємо розташування контролера як розташування вузла в середовищі ПКМ. Отже, нам потрібно обчислити значення k, яке представляє кількість контролерів, щоб знайти відношення відображення U → V, через яке обчислюється цільова функція. Припустимо, що C = (C1, C2, . . . Cn) є кількістю контролерів, розгорнутих в мережі. S = (S1, S2, . . . Sn), що представляють кількість перемикачів, так що V = C ∪ S. n = V представляє кількість вузлів, а k = U представляє кількість контролерів. Pc = {pc1, pc2, . . .,pcm} представляє можливості розміщення контролера.

Де m представляє n варіантів елементів, взятих із групи. Розрахунок m визначається наступним чином:

$$m = \frac{n!}{k!(n-k)!}. \tag{4.7}$$

У запропонованій мережі контролер вибирається на основі найкоротшої відстані d (s,c) між комутатором і контролером від вузлів s ∈ V і c ∈ V.

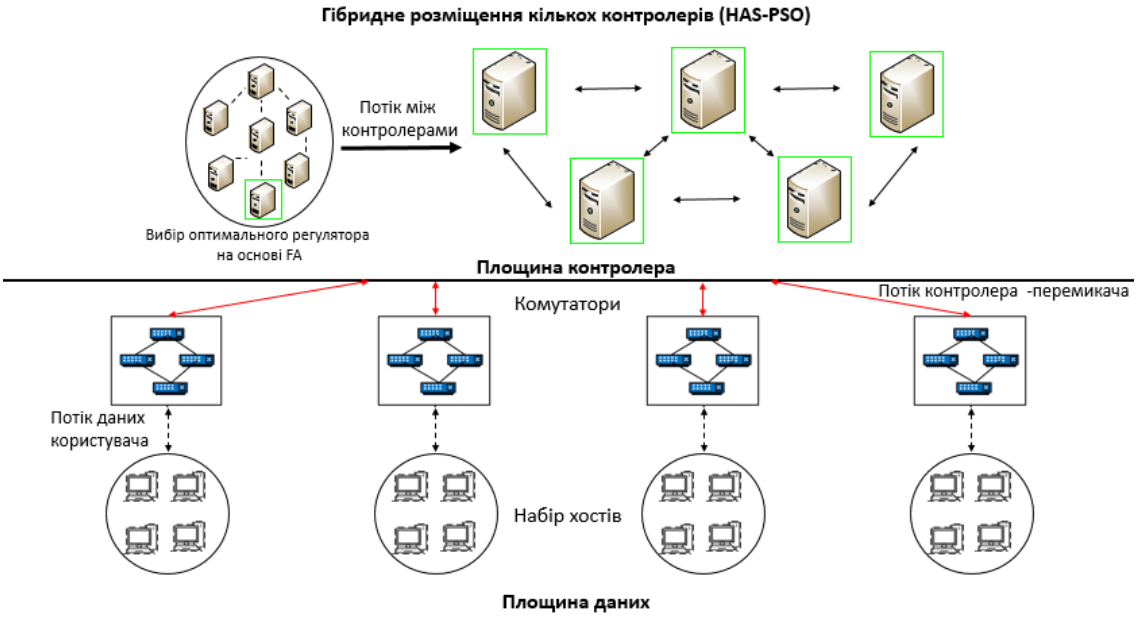

Рис. 4.1. Пропонована архітектура МК-ПКМ.

Контролер є основним компонентом у мережі ПКМ, який керує мережею в цілому. Тому для управління мережею в цілому необхідно вибрати оптимальний вибір контролерів. Оптимальний вибір контролерів базується на характеристиках контролера.

Запропонований метод вибору регулятора включає два етапи, а саме якісний та кількісний підходи за алгоритмом оптимізації. У запропонованій роботі використовується алгоритм FA. FA — це природний алгоритм, натхненний жуками, які випромінюють привабливі вогники з черевної частини. Наведено роботу вибору контролера на основі FA. Спочатку ініціалізуються функції контролерів у мережі, що можна сформулювати як:

$$F_{Cn} = \{F_{c1}, F_{c2}, F_{c3}, F_{c4}, F_{c5}, F_{c6}, F_{c7}, \dots, F_{cn}\}. \quad (4.8)$$

Спочатку обчислюються функції, які дуже відповідають за вибір контролера. Для кожного контролера в мережі їх відповідні ефективні характеристики обчислюються шляхом обчислення відстані між ними на основі вищої інтенсивності освітлення. Високоефективним функціям (тобто функціям контролера з високою відмовостійкістю) надається велике значення. Відстань між ознаками формулюється як:

$$FT(D) = \frac{F_C}{D_C}, \quad (4.9)$$

де FT(D) — функція високої відмовостійкості на основі відстані між контролерами Dc, а FC позначає функції контролера. Вибір високовідмовостійких функцій обчислюється, щоб розмістити контролер в оптимальному положенні. Цільова функція функції високої відмовостійкості може бути сформульована як

$$FT_{F_C} = f(F_C)\ . \quad (4.10)$$

З наведеного вище FTFC ми вибираємо функції контролера, які є високоефективними (тобто високостійкими до відмов), що базується на коефіцієнті притягання контролера, який є відносно високим коефіцієнтом поглинання світла, який можна сформулювати як:

$$\aleph(D) = \aleph_0 e^{-\gamma D^2}, \tag{4.11}$$

де ℵ(D) – коефіцієнт поглинання контролера, який використовується для залучення найкращих контролерів на основі алгоритму FA, ℵ0 = найкраща висока інтенсивність світла для firefly, а γ – коефіцієнт поглинання для поглинання контролера з високою відмовостійкістю. На основі привабливого значення регулятора ℵ оптимальний регулятор – це вибір, який можна сформулювати як

$$\aleph\left(\mathrm{F}T_{F_C}\right) = \{\aleph\left(\mathrm{F}T_{F_{C1}}\right), \aleph\left(\mathrm{F}T_{F_{C2}}\right), \ldots, \aleph\left(\mathrm{F}T_{F_{C7}}\right)\}. \tag{4.12}$$

Псевдокод вибору контролера на основі FA наведено порівнянням лише двох контролерів як приклад. На основі прикладу FA оптимально вибирає найкращий контролер серед семи контролерів, а на Рис. 4.2. представлено псевдокод оптимального вибору контролера ПКМ за допомогою FA, залежно від вищої інтенсивності освітлення, яке випромінюється (Рис. 4.3.). [16]

Initialize F_C
Formulate objective function using (13)
Formulate controller absorption coefficient using (14)
Initialize absorption coefficient using (15)
While all F_C **do**
Compute controller feature distance using (12)
For F_{C1} = 1 to n (all n controllers)
For F_{C2} = 1 to n (all n controllers)
If ($D_{F_{C2}} > D_{F_{C1}}$), select F_{C2} over F_{C1}
End if
Update the $\aleph(D)$
End for F_{C2}
End for F_{C1}
Rank the controller and find the current best controller
End while

Рис. 4.2. Псевдокод ФА для вибору оптимального регулятора

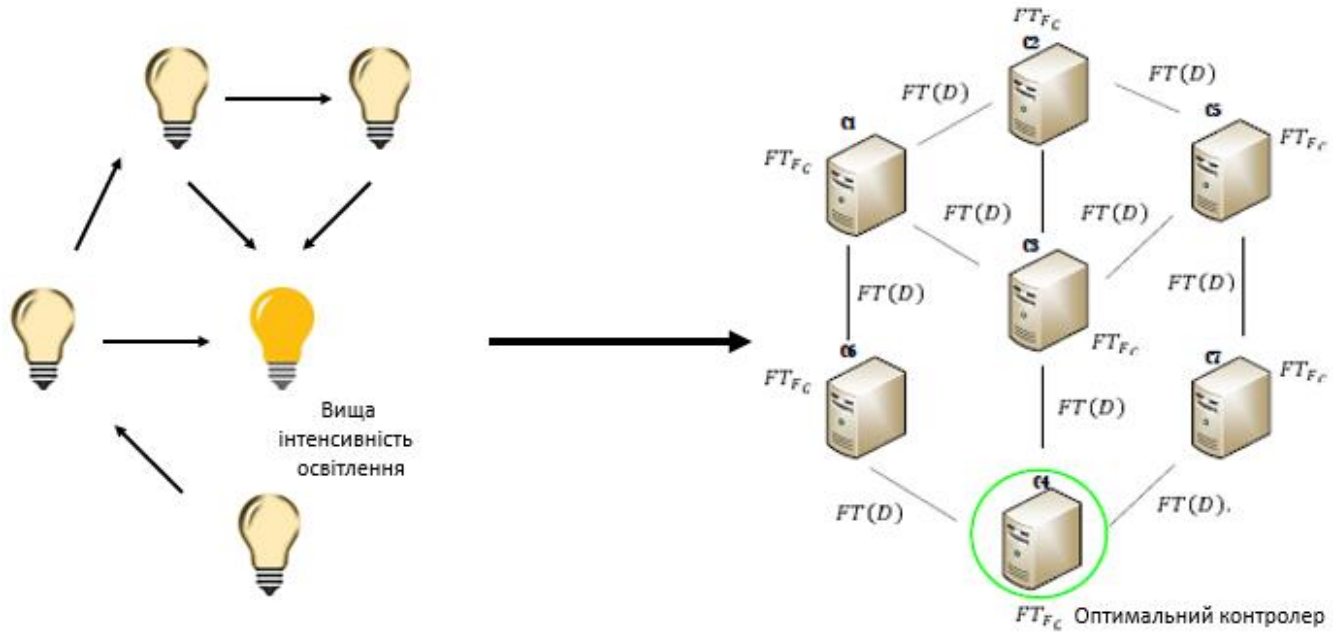

Рис. 4.3. Вибір оптимального регулятора на основі FA.

4.2. Застосування методу мультиконтролерного ПКМ

Після завершення вибору контролера починається розміщення кількох контролерів. У середовищі ПКМ розміщується кілька контролерів, щоб зменшити затримку зв'язку між контролерами та комутаторами. Ефективне розміщення контролера підвищує продуктивність мережі. Для оптимального розміщення контролера я запропонував гібридний метаевристичний алгоритм, який включає алгоритм гармонійного пошуку (АПГ) і оптимізацію роєм частинок (АРЧ).

Алгоритм АПГ легко потрапляє в локальні оптимуми, тому потрібно періодично оновлювати параметри HS за допомогою алгоритму АРЧ. Пропонований АПГ включає три фази: фаза ініціалізації, фаза імпровізації та фаза оновлення. Тут імпровізацію оновлено для трьох процесів, таких як розгляд пам'яті, налаштування висоти та випадковий вибір. Алгоритм АПГ складається з пам'ят, а саме пам'яті гармонії (ПГ), яка включає вектори гармонії, які зберігають цільову функцію АПГ. Спочатку ми ініціалізуємо HM і розмір рою для оцінки функції придатності, яка визначається наступним чином:

$$\begin{bmatrix} h_1^1 & h_2^1 & \dots & h_d^1 \\ h_1^2 & h_2^2 & \dots & h_d^2 \\ \vdots & \vdots & \vdots & \vdots \\ h_1^n & h_2^n & \dots & h_d^n \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_n \end{bmatrix}, \text{де Fitness Function} = \frac{1}{\sum_{d=1}^{B} f(h)_d}. \quad (4.13)$$

Тут функція відповідності оцінюється на основі параметрів розташування та відстані B і d, щоб забезпечити ефективне оптимальне рішення наступним чином. Після завершення ініціалізації, виконується імпровізація гармонії для генерації нового вектора гармонії $[h'_1, h'_2, \dots, h'_t]$.

Кожен новий компонент вектора гармонії h′ генерується за такою формулою:

$$h'_j \leftarrow \begin{cases} h'_j \in P_{HM} with\ Pb\ of\ HMCR \\ h'_j \in P_j with\ Pb\ of\ (1 - HMCR)' \end{cases} \quad (4.14)$$

де HMCR представляє швидкість розгляду гармонічної пам’яті, яка визначає ймовірність вибору компонента. Визначено розрахунок коригування кроку для вибраного h′ наступним чином:

$$h'_j \leftarrow \begin{cases} h_j^n \in P_{HM} with\ Pb\ of\ PAR \\ h'_j\ with\ Pb\ (1 - PAR) \end{cases}, \quad (4.15)$$

де PAR представляє швидкість налаштування висоти, а PHM представляє запропонований гібридний алгоритм АПГ і АРЧ, а h′ представляє оптимальне розташування для розміщення контролера.

Новий гібридний вектор гармонії обчислюється на основі значення цільової функції для кожного P_Best. Якщо нове цільове значення вектора гармонії краще, ніж цільове значення найгіршої гармонії, новий вектор гармонії розглядається в PHM. Найгірше значення вектора гармонії відхиляється від PHM. Оптимальна позиція для розміщення контролера визначається на основі найкращих частинок у рої, яка визначається як P_Best. Він генерує n кількість ітерацій, і найкраща частинка серед усіх вважається G_Best. Позиція та швидкість усіх частинок оновлюються для кожної

швидкості. Поточна швидкість і положення обчислюються за допомогою рівнянь (4.2) і (4.3), наведених вище.

Розрахунок значення ваги визначається наступним чином:

$$W = W_u - (W_u - W_l)(\frac{i}{I_{max}}), \quad (4.16)$$

де Imax представляє загальну кількість ітерацій, а і представляє поточну ітерацію, а Wu і Wl представляють верхню та нижню межі вагових значень. Ці процеси тривають, доки не будуть виконані критерії припинення. Таблиця 4 описує параметри алгоритму АПГ. Рис. 4. ілюструє процес розміщення кількох контролерів.

Таблиця 4.1.

Параметри (АПГ)

Назви параметрів	Символи параметрів	Значення
Пам'ять гармонії	HMCR	0,8
Швидкість розгляду		
Швидкість налаштування висоти	PAR	0,2
Випадковий ранд	Rand	0,1
HS ітерація	H(I)	100
Пам'ять гармонії	HM	5
Мінімальна пропускна здатність	BW	0,1 Мбіт/с
Максимальна пропускна здатність	MBW	0,4 Мбіт/с

Реалізація запропонованого методу МК-ПКМ за допомогою інструменту моделювання CloudSimПКМ із комплектом інтегрованого середовища розробки (IDE) NetBeans 12.5 для виконання моделювання з кількома об’єктами, такими як пристрої, комутатори, хости, контролер і хмара. Цей інструмент моделювання підходить для виконання моделювання та симуляції хмарних об’єктів і служб, включаючи їхні служби, у яких цей симулятор із відкритим вихідним кодом,

створеним лабораторією хмарних обчислень і систем розподілу в Мельбурнському університеті.

Рис. 4.4. Розміщення кількох контролерів на основі гібридної оптимізації.

Спочатку середовище CloudSim створюється за допомогою комутаторів контролерів ПКМ і хостів. Таблиця 4.2. ілюструє конфігурації системи, а таблиця 4.3. показує конфігурацію параметрів запропонованого методу МК-ПКМ.

Таблиця 4.2.

Конфігурації системи

Специфікації ПЗ	Операційна система	Windows 10 Pro (64-розрядна)
Технічні характеристики апаратного забезпечення	IDE	NetBeans 12.5
	Комплект розробки	JDK 1.8
	Симулятор мережі	CloudSimПКМ
	Мова	Java
	Тип топології	Неорієнтований граф
	Жорсткий диск	1 Тб
	ЦП	Intel (R) Core (MT) i7-4590S @ 3,00 ГГЦ
	Оперативна пам'ять	8 ГБ

Таблиця 4.3.

Конфігурації параметрів

Хмарний сервер	Операційна система	Windows 10 Pro (64-розрядна)
Пристрої	Пропускна здатність	100 000 низхідних і висхідних кан.
	Оперативна пам'ять	64 Гб
	Затримка	900 мс
	MIPS	44 800
	Затримка пристроїв	1 мс
	MIPS	1500
	Оперативна пам'ять	4 Гб
ПКМ	Кількість контролерів	6
	Кількість комутаторів	30
	Затримка перемикання	5 мкс
	Пропускна здатність	Змінна

Середовище моделювання цього методу МК-ПКМ показано на Рис. 4.5., яке складається з хостів, комутаторів і кількох контролерів. Хости надсилають дані до контролера через комутатори. Оптимальний контролер вибирається з числа контролерів на основі численних особливостей пакетів. Оптимальний контролер клонується в шість контролерів для виконання розміщення кількох контролерів. Розташування та відстань вважаються для ефективного розміщення мультиконтролера, щоб зменшити проблему розміщення контролера. Оптимальний вибір контролера та розміщення кількох контролерів підвищують ефективність зв'язку між комутаторами та контролерами, а також між контролерами.

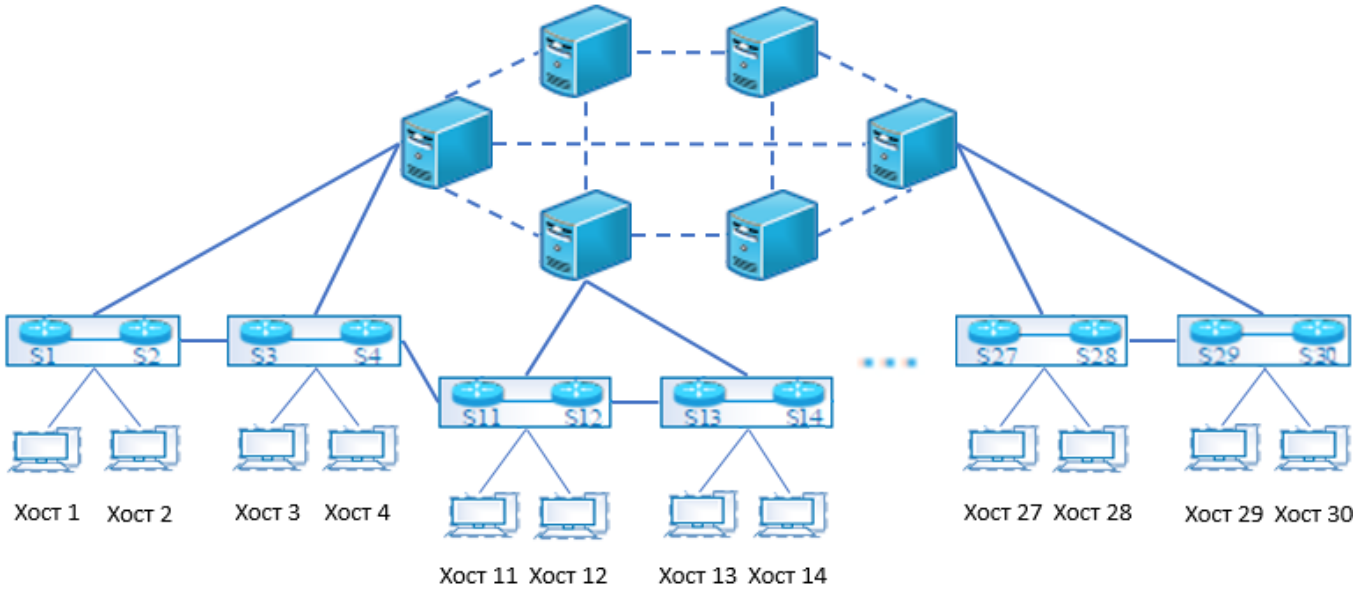

Рис. 4.5. Середовище моделювання МК-ПКМ.

Останнім часом ПКМ надала свої програми рекламним мережам транспортних засобів (VANET). Мобільний характер середовища VANET зіткнувся з серйозними проблемами з точки зору управління мережею. VANET разом із ПКМ під назвою Software-Defined Vehicular Network (SDVN) надає можливість керування мережею за допомогою контролерів. Середовище SDVN потребує кількох контролерів, які слід розмістити в оптимальному місці, щоб зменшити затримку наскрізної обробки в середовищі SDVN. Запропонований підхід МК-ПКМ легко адаптується до середовища VANET з точки зору мобільності та надійності. [17]

Рис. 4.6. позначає схематичне зображення середовища SDVN, яка складається з великої кількості мобільних транспортних засобів, які дозволяють виконувати різноманітні операції, такі як екстрені повідомлення, правила дорожнього руху тощо.

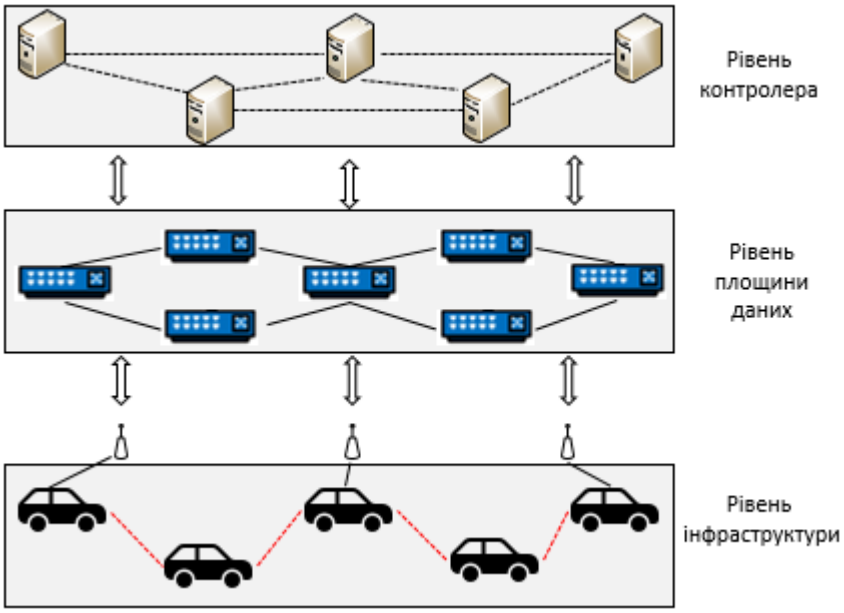

Рис. 4.6. Сценарій застосування методу МК-ПКМ.

Спочатку мережевий граф будується для керування мережею та забезпечує високу масштабованість. Відповідний контролер з високою відмовостійкістю вибирається на основі функцій контролера за допомогою алгоритму FA для надання ефективних послуг у середовищі SDVN. Нарешті, вибраний контролер розміщується в кількох оптимальних місцях за допомогою гібридних алгоритмів оптимізації. Оптимальне розміщення контролерів зменшує затримку між контролерами та контролерами до комутаторів, щоб забезпечити безперебійний зв'язок між ними. [18]

4.3 Дослідження результатів застосування методу МК-ПКМ

Порівняння запропонованого методу МК-ПКМ з декількома існуючими методами, такими як Проблема розміщення ємного контролера з імітацією невдачі нормалізації (ПРЄКІНН) і Проблема розміщення ємного контролера з оптимізацією підв'язкової змійки (ПРЄКОПЗ), виконується в цьому підрозділі, щоб оцінити їх

роботу. Оцінка цих методів виконується шляхом розгляду кількох показників продуктивності, таких як затримка розповсюдження, середній час проходження (СЧП), матриця часу сеансу (ЧС), середня затримка, надійність і пропускна здатність відповідно.

Затримка розповсюдження є одним із важливих показників, який використовується для оцінки затримки між комутаторами та контролерами під час розповсюдження. Затримка поширення ($P_{\text{д}}$) визначається як співвідношення між відстанню (λ) (м) і швидкістю поширення (q) (м/с), у якому формулювання затримки поширення представлено таким чином:

$$P_{\text{д}} = \frac{\lambda}{q}. \tag{4.17}$$

Рис. 4.7. ілюструє порівняння затримки поширення запропонованого методу МК-ПКМ з кількома існуючими підходами, такими як методи ПРЄКОПЗ і ПРЄКІНН, з точки зору кількості ітерацій. Мережа ПКМ із низькою затримкою поширення забезпечує ефективний зв’язок між комутаторами та контролерами. Затримка поширення зменшується при збільшенні кількості ітерацій. У попередніх методах розміщення контролерів виконувалося з урахуванням лише відстані між перемикачами та контролерами. Крім того, погане налаштування алгоритмів призводить до неправильного розміщення контролера, що збільшує затримку поширення.

У запропонованому методі МК-ПКМ розміщення контролера виконується з урахуванням відстані з використанням гібридного алгоритму оптимізації, що підвищує продуктивність розміщення контролера, та як результат зменшує затримку поширення.

Графічні результати показують, що запропонований метод МК-ПКМ досягає низької затримки розповсюдження (від 10 до 26 мс) у порівнянні з методами ПРЄКІНН (24–42 мс) і ПРЄКОПЗ (29–47 мс).

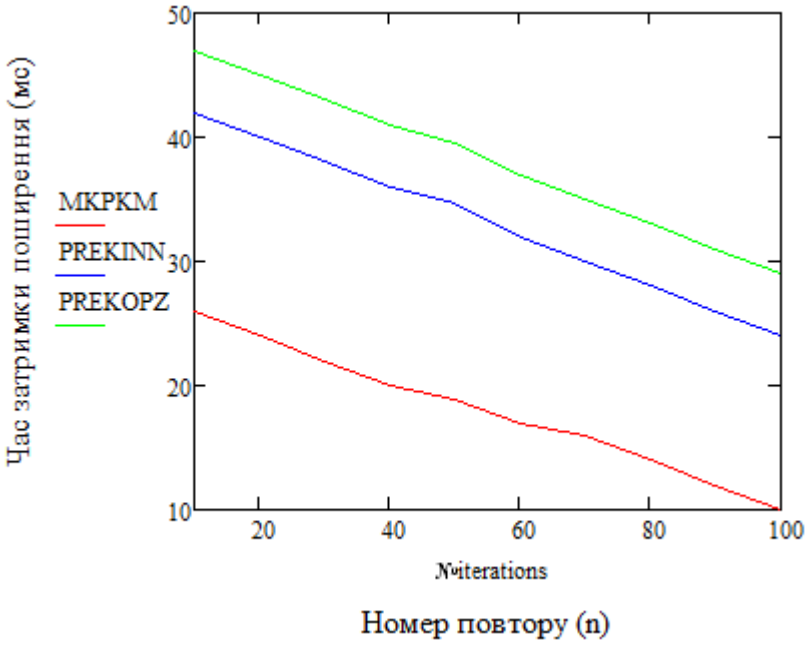

Рис. 4.7. Порівняння затримки поширення.

Таблиця 4.4. описує різницю затримки розповсюдження між запропонованим методом МК-ПКМ і попередніми підходами.

Таблиця 4.4.

Чисельний аналіз затримки поширення (мс)

Метод	Затримка
ПРЄКОПЗ	39,6 ± 0,5
ПРЄКІНН	34,6 ± 0,3
МК-ПКМ	18,8 ± 0,1

Вплив середнього часу проходження пакетів (СЧП) використовується для вимірювання часу між пристроями для передачі та отримання пакетів від джерела до місця призначення. Він вимірюється різницею між часом повернення пакета (ζ) і часом надсилання пакета (δ) і обчислюється в мс, у якому формулювання СЧП (η) представлено таким чином:

$$\eta = \zeta - \delta. \tag{4.18}$$

На Рис. 4.8. представлено порівняння середнього СЧП між запропонованим методом МК-ПКМ і декількома сучасними роботами щодо кількості ітерацій. Низький СЧП у мережі забезпечує високу пропускну здатність. Середнє СЧП збільшується за рахунок збільшення кількості ітерацій. Розміщення контролера розглядалося в попередніх роботах, однак відсутність урахування ефективного контролера призводить до високого СЧП. У запропонованому методі оптимальний регулятор вибрано за допомогою алгоритму FA з урахуванням численних особливостей регулятора, які знижують СЧП у порівнянні з сучасними методами підвищення ефективності ПКМ. Порівняльні результати доводять, що запропонований метод МК-ПКМ забезпечує низький СЧП у порівнянні з іншими існуючими підходами. Запропонований метод МК-ПКМ досягає середнього СЧП приблизно 13 мс, що на 4 мс нижче, ніж метод ПРЄКІНН, і на 8 мс нижче, ніж метод ПРЄКОПЗ.

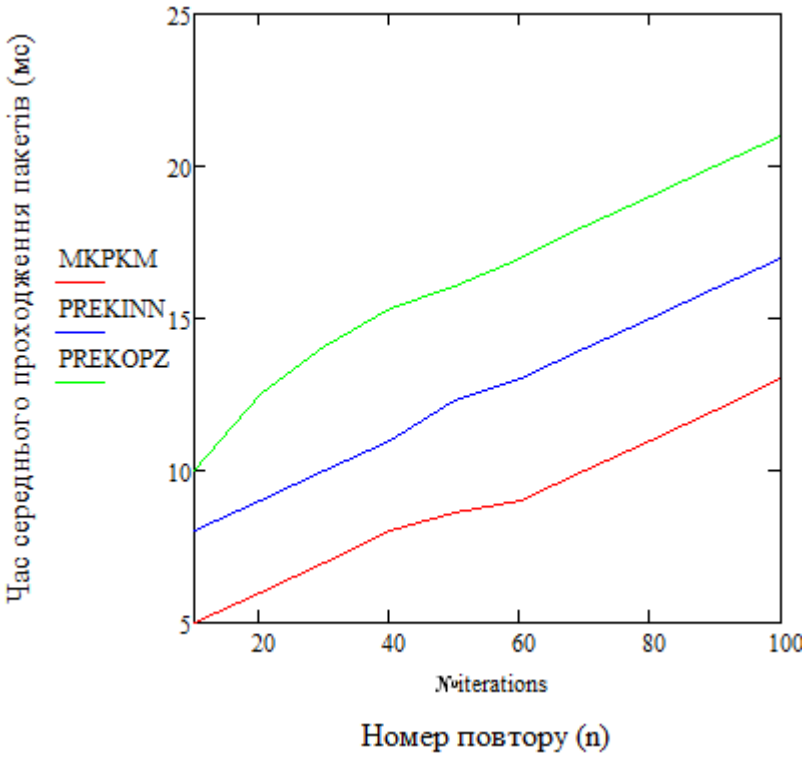

Рис. 4.8. Порівняння середнього часу проходження пакетів.

Зміни середнього СЧП запропонованого методу МК-ПКМ та кількох існуючих методів описані в таблиці 4.5.

Таблиця 4.5.

Чисельний аналіз середнього часу проходження пакетів (мс)

Метод	СЧП пакетів
ПРЄКОПЗ	16,5 ± 0,4
ПРЄКІНН	12,3 ± 0,2
МК-ПКМ	8,65 ± 0,1

Матриця часу сесії (ψ) використовується для розрахунку кількості часу, необхідного для ефективного зв'язку між комутаторами та контролерами. Він вимірюється кількістю комутаторів і положенням серверів у співвідношенні між часом, витраченим на певний сеанс (ζ), до загальної кількості сеансів (σ), який формулюється так:

$$\psi = \frac{\zeta}{\sigma}. \tag{4.19}$$

На Рис. 4.9. показано порівняльний аналіз матриці часу сеансу між запропонованим підходом МК-ПКМ та кількох існуючих робіт за кількістю ітерацій. Мережа з низькою матрицею часу сеансу досягає кращої ефективності передачі. У попередніх роботах розміщення контролера виконувалося з урахуванням найкоротшої відстані між комутаторами та контролерами. Однак відсутність урахування оптимального розміщення контролерів збільшує час для кожного сеансу. Крім того, єдиний контролер також призводить до високої матриці часу сесії. Щоб подолати ці проблеми, оптимальний контролер вибирається в мережі на основі пакетних особливостей з використанням алгоритму FA, який ефективно зменшує матрицю часу сеансу в порівнянні з існуючими роботами. На малюнку показано, що запропонований метод МК-ПКМ досягає низької матриці часового сеансу приблизно 330 одиниць для 100 ітерацій, що на 60 більше, ніж ПРЄКІНН, і на 90 більше, ніж методи ПРЄКОПЗ.

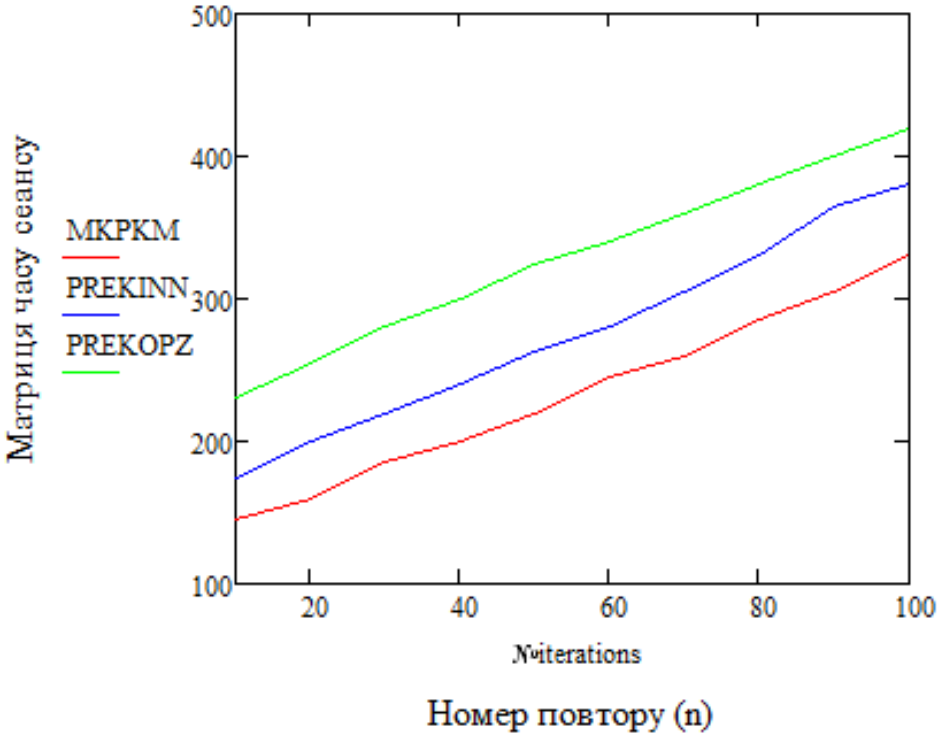

Рис. 4.9. Порівняння матриці часу сеансу.

Графічні варіації матриці ЧС між запропонованим методом МК-ПКМ і сучасними роботами проілюстровано в таблиці 4.6.

Таблиця 4.6.

Чисельний аналіз матриці часу сеансу

Метод	Матриця часу сеансу
ПРЄКОПЗ	324,8 ± 0,5
ПРЄКІНН	262,1 ± 0,4
МК-ПКМ	219,1 ± 0,1

Середня затримка (đ) визначається як кількість додаткового часу, необхідного для доставки пакетів від даних до площини керування в запропонованому методі МК-ПКМ. Середня затримка вимірюється відношенням фактичного розміру пакета (Ѫ) до обсягу доступної смуги пропускання (ѽ), яке формується нижче:

$$đ = \frac{Ѫ}{ѽ}. \tag{4.20}$$

Порівняння запропонованого методу МК-ПКМ з кількома сучасними роботами з точки зору середньої затримки по відношенню до кількості ітерацій показано на Рис. 4.10. Мережа з низькою середньою затримкою досягає високого коефіцієнта доставки пакетів. Середня затримка зростає зі збільшенням кількості ітерацій. У запропонованому методі МК-ПКМ низька середня затримка досягається за допомогою гібридного алгоритму оптимізації, який складається з алгоритмів АПГ та АРЧ, і забезпечує кращі результати для розміщення контролерів, що зменшує середню затримку, тоді як попередні методи виконують розміщення контролера за допомогою єдиного алгоритму оптимізації, що знижує точність розміщення контролера та зменшує середню затримку.

Результати показують, що запропонований метод МК-ПКМ забезпечує низьку середню затримку порівняно з попередніми роботами. Запропонований метод МК-ПКМ має середню затримку приблизно 110 мс, що на 30 мс швидше, ніж метод ПРЄКІНН, і на 60 мс швидше, ніж метод ПРЄКОПЗ. Графічні зміни середньої затримки запропонованого МК-ПКМ та інших підходів описані в таблиці 4.7.

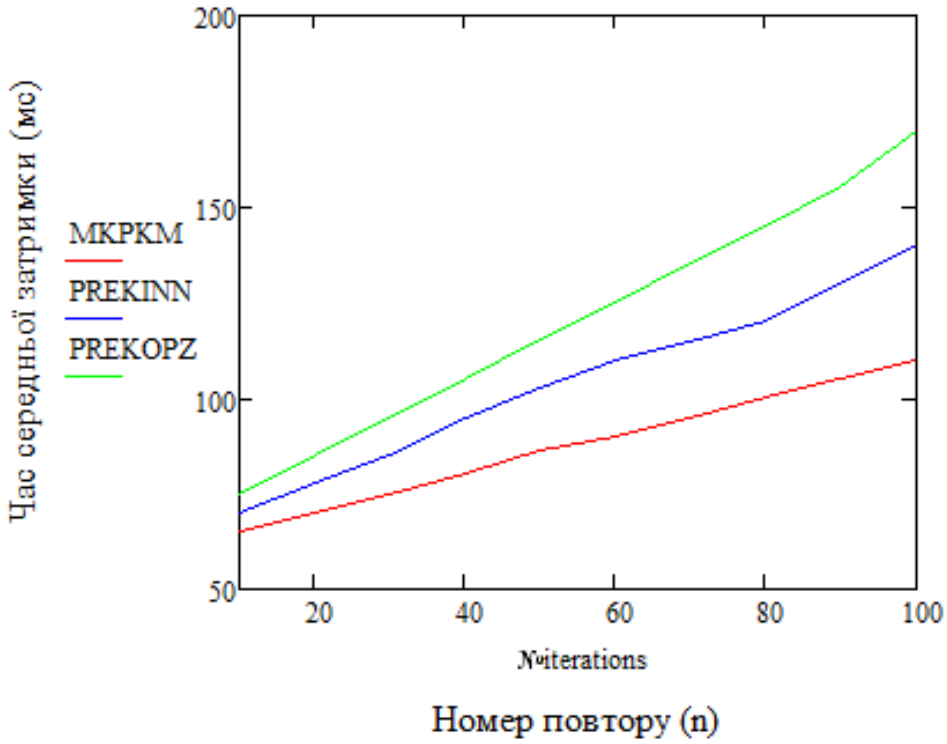

Рис. 4.10. Порівняння впливу середньої затримки.

Таблиця 4.7.

Числовий аналіз середньої затримки (мс)

Метод	Середня затримка
ПРЄКОПЗ	115,5 ± 0,4
ПРЄКІНН	102,5 ± 0,3
МК-ПКМ	86,1 ± 0,1

Вплив надійності використовується для оцінки ефективності запропонованого методу МК-ПКМ з точки зору ефективного оптимального розміщення контролерів. Мережа з високою надійністю забезпечує ефективний зв'язок з високою точністю.

$$RL = max \sum_{v \in V} \sum_{s \in S} p(v, s). \quad (4.21)$$

RL представляє надійність для мінімізації шляху керування між MC-S і p(v, s) вказує на доступну ймовірність шляху керування.

На Рис. 4.11. показано порівняння запропонованого методу МК-ПКМ і кількох попередніх робіт з точки зору надійності на кількість ітерацій. Збільшення кількості ітерацій підвищує надійність. В існуючих методах розміщення контролерів виконувалося з погано налаштованими алгоритмами оптимізації та неефективним зв’язком між контролерами в мережі ПКМ, що знижує надійність мережі.

У запропонованому методі МК-ПКМ ці проблеми розглядаються та виконуються ефективно налаштовані гібридні алгоритми для розміщення контролерів та оптимального вибору контролерів для здійснення ефективного зв’язку між контролерами, що підвищує надійність у порівнянні з сучасними стандартами. З малюнка чітко видно, що запропонований метод МК-ПКМ забезпечує високу надійність у порівнянні з іншими попередніми роботами. Запропонований метод МК-ПКМ досягає надійності приблизно 0,95 для 100 ітерацій, що на 0,065 більше, ніж метод ПРЄКІНН і на 0,035 більше, ніж метод ПРЄКОПЗ для тієї ж кількості ітерацій. Таблиця 11 описує варіації надійності запропонованого методу МК-ПКМ і кількох існуючих робіт.

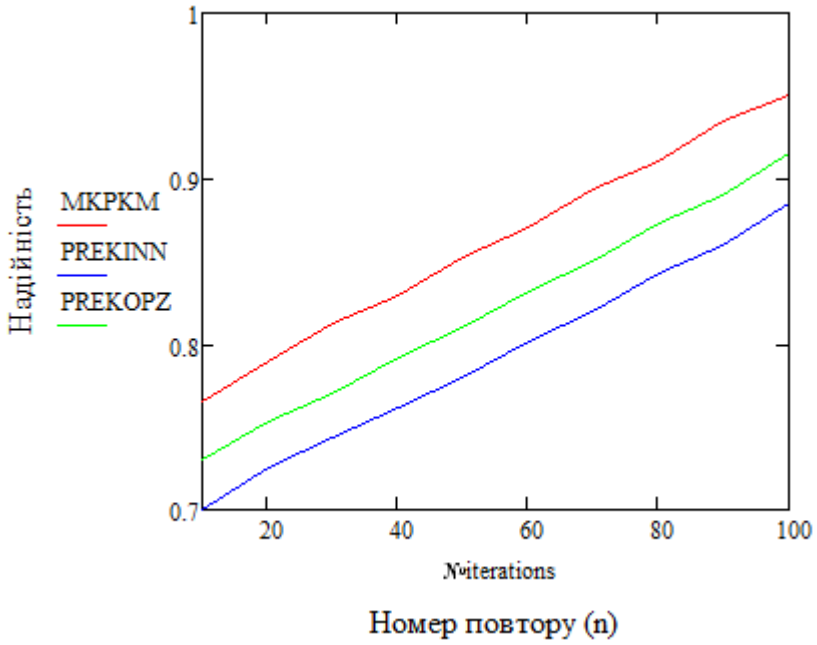

Рис. 4.11. Порівняння надійності.

Таблиця 4.8.

Чисельний аналіз надійності

Метод	Надійність
ПРЄКОПЗ	0,81 ± 0,5
ПРЄКІНН	0,78 ± 0,4
МК-ПКМ	0,852 ± 0,1

Пропускна здатність (ω) мережі визначається як кількість даних, доставлених до приймача від передавача (μ) протягом певного часу (ζ). Розрахунок пропускної здатності формується нижче:

$$\omega = \frac{\mu}{\zeta}. \tag{4.22}$$

На Рис. 4.12. показано порівняння пропускної здатності між кількома попередніми методами та запропонованим методом МК-ПКМ з точки зору кількості комутаторів у мережі. Мережа з високою пропускною здатністю досягає високої швидкості доставки пакетів. На рисунку видно, що пропускна здатність зросла за

рахунок збільшення кількості комутаторів. Порівняльні результати показують, що запропонований метод МК-ПКМ забезпечує високу пропускну здатність порівняно з попередніми підходами. У існуючих методах розміщення контролера виконувалося з урахуванням деяких обмежень, таких як затримка зв'язку, затримка розповсюдження тощо. Однак відсутність урахування відмовостійкості знижує пропускну здатність мережі.

У запропонованому методі МК-ПКМ вибір оптимального контролера здійснюється за допомогою алгоритму FA з урахуванням численних особливостей пакетів, які забезпечують високу відмовостійкість, що підвищує пропускну здатність у порівнянні з сучасними розробками. З рисунку доведено, що запропонований метод МК-ПКМ забезпечує високу пропускну здатність приблизно 230 тис. відгуків/с, що на 15 тис. відгуків/с вище, ніж підхід ПРЄКІНН, і на 40 тис. відгуків/с вище, ніж підхід ПРЄКОПЗ. Варіації пропускної здатності між запропонованим методом МК-ПКМ та іншими існуючими методами описані в таблиці 4.9.

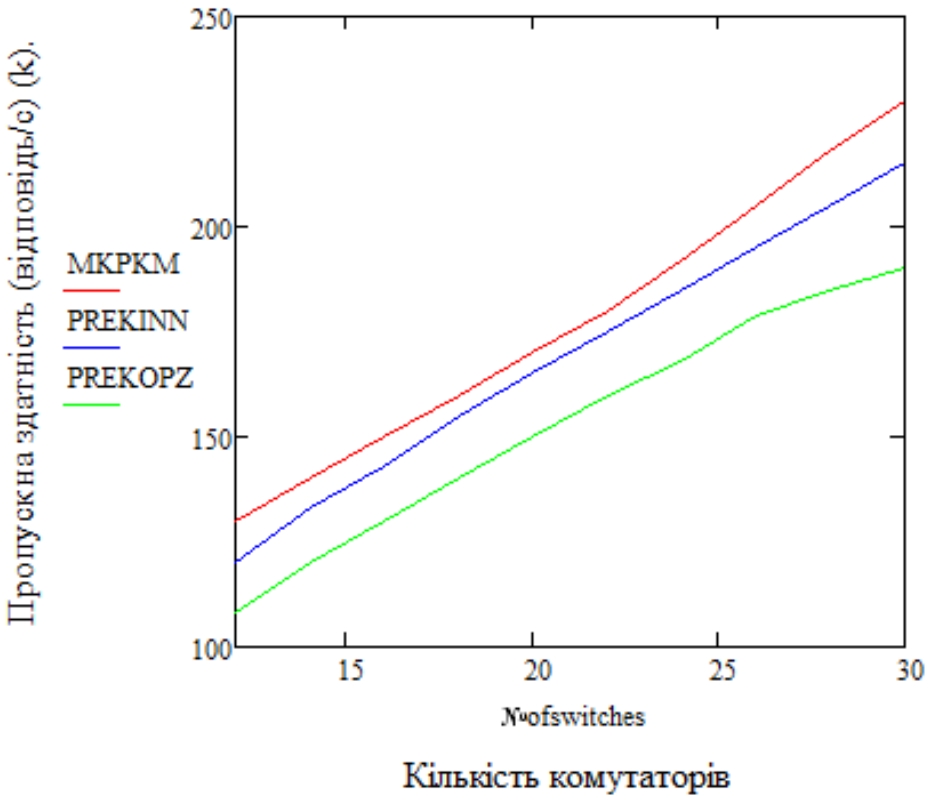

Рис. 4.12. Порівняння пропускної здатності.

Таблиця 4.9.

Числовий аналіз пропускної здатності (відповідь/с) (k)

Метод	Кількість відгуків/с
ПРЄКОПЗ	150,8 ± 0,3
ПРЄКІНН	165,5 ± 0,2
МК-ПКМ	170,9 ± 0,1

Вплив вартості використовується для визначення вартості всієї мережі на основі часу. Мережа з низькою вартістю, яка відповідає всім необхідним, забезпечує ефективну якість обслуговування. Рис. 4.13. ілюструє порівняння вартості по відношенню до часу для запропонованого методу МК-ПКМ і кількох попередніх підходів. На графіку видно, що вартість зростає зі збільшенням часу. У попередніх методах зв'язок між контролерами здійснювався неефективно, що займає більше часу та збільшує вартість.

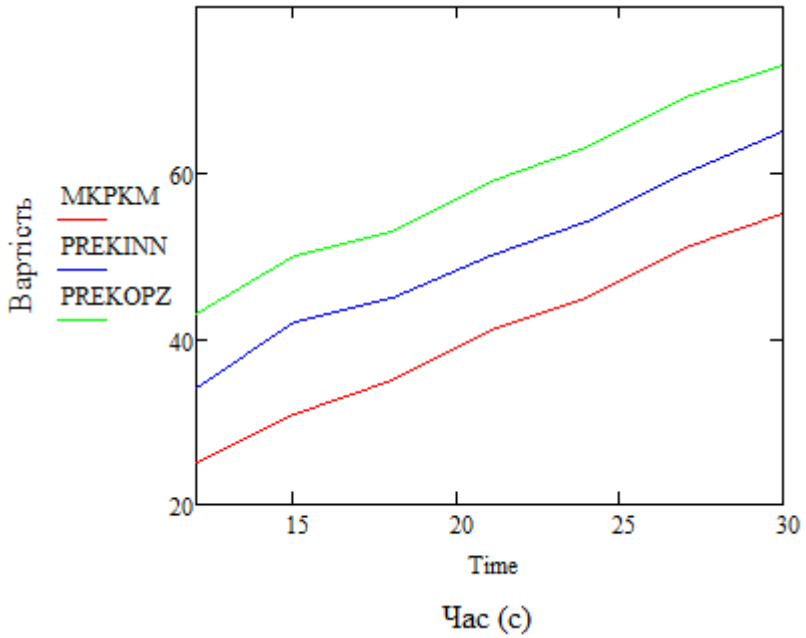

Рис. 4.13. Порівняння вартості.

У запропонованому методі МК-ПКМ зв'язок між комутаторами та контролерами та між самими контролерами ефективно виконується шляхом вибору оптимального контролера та розміщення кількох контролерів за допомогою FA з

урахуванням розташування та відстані, а також використанням кількох контролерів. Розміщення контролера виконується за допомогою гібридних алгоритмів оптимізації з урахуванням особливостей пакетів для подолання цих проблем, які забезпечують ефективний зв'язок, що призводить до низької вартості порівняно з попередніми підходами. Порівняльні результати показують, що запропонований метод МК-ПКМ досягає низької вартості приблизно 55 одиниць, що на 10 нижче, ніж метод ПРЄКІНН, і на 18 нижче, ніж метод ПРЄКОПЗ. Таблиця 4.10. описує варіацію вартості запропонованого методу МК-ПКМ та інших попередніх методів.

Таблиця 4.10.

Числовий аналіз собівартості

Метод	Вартість
ПРЄКОПЗ	50,1 ± 0,4
ПРЄКІНН	42,6 ± 0,2
МК-ПКМ	31,4 ± 0,1

Вплив фітнес-цінності є одним із важливих показників, які використовуються для аналізу значення придатності запропонованого методу МК-ПКМ. Значення придатності обчислюється шляхом оцінки оптимального рішення для проблеми розміщення контролера. Оптимізація з високим значенням придатності забезпечує ефективне оптимальне рішення.

Рис. 4.14. ілюструє порівняння значення придатності між попередніми підходами та запропонованим методом МК-ПКМ з точки зору кількості ітерацій. На графіку чітко видно, що значення придатності зменшується, коли кількість ітерацій збільшується. У методі ПРЄКІНН використовувався змодельований алгоритм оптимізації відпалу, а в методі ПРЄКОПЗ реалізовувався алгоритм оптимізації підв'язкової змії для надання рішень щодо розміщення контролера. Однак значення придатності цих алгоритмів не відповідає проблемі розміщення контролера ефективно через погані механізми адаптації та точність.

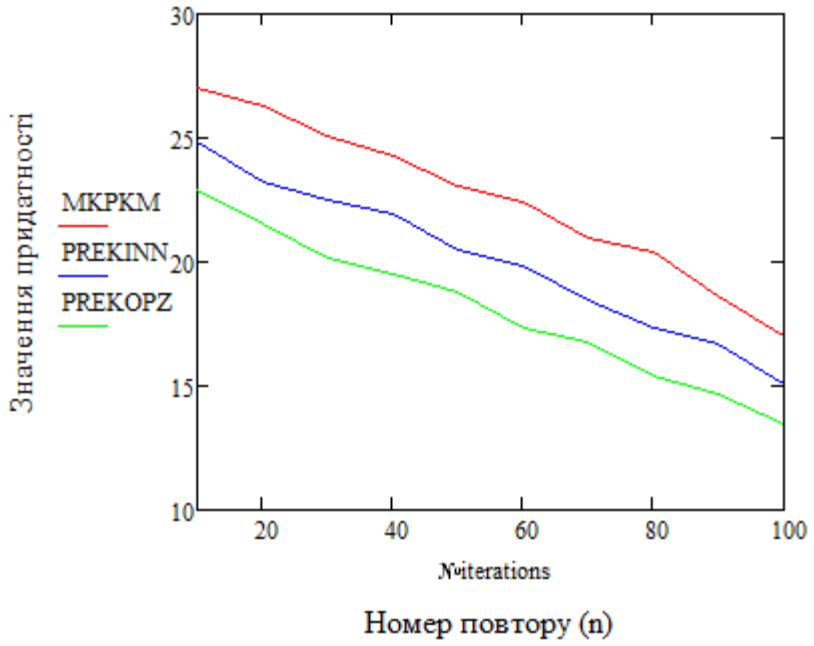

Рис. 4.14. Порівняння значень придатності.

Щоб подолати ці проблеми, я використовую гібридні алгоритми оптимізації, які підвищують значення придатності порівняно з іншими існуючими роботами шляхом динамічної адаптації для збільшення швидкості конвергенції, що підвищує точність розміщення контролера. Графічні результати показують, що запропонований метод МК-ПКМ досягає високого значення придатності порівняно з кількома існуючими роботами: середнє значення приблизно 23,1, що є на 2,65 більше, ніж метод ПРЄКІНН і на 4,3 більше, ніж метод ПРЄКОПЗ. Варіації значень придатності для запропонованого методу МК-ПКМ та інших попередніх методів описано в таблиці 4.11.:

Таблиця 4.11.

Числовий аналіз значень придатності

Метод	Значення придатності
ПРЄКОПЗ	18,8 ± 0,5
ПРЄКІНН	20,45 ± 0,4
МК-ПКМ	23,1 ± 0,1

ВИСНОВКИ ДО РОЗДІЛУ 4

В даний час широке використання мобільних пристроїв розширює масштаби мереж. Традиційні мережі, швидше за все, застаріли для мінливого сценарію, який стикається з проблемами управління мережею та проблемами гнучкості мережі. Щоб полегшити проблеми з традиційними мережами, було розроблено програмно-конфігуровану мережу. ПКМ - нова парадигма, яка підтримує мережеве програмування, розгадуючи мережеве обладнання з рівнем керування. Як правило, програмно-конфігурована мережа складається з трьох площин, а саме: площини даних, площини керування та площини додатків. Площина даних складається з кількох комутаторів, що збирають дані у вигляді пакета з пристроїв і виконують пересилання на площину керування, дотримуючись протоколів ПКМ (тобто OpenFlow). Площина керування складається з контролера, який є серцем ПКМ, що керує всією мережею. Площиною додатків керує адміністратор додатків, політиками якого також керує контролер. Контролер має повноваження видаляти або додавати правила та політики в мережах ПКМ. Таким чином, він покращує програмованість мережі та підтримує мережеве керування.

Спочатку всією мережею ПКМ керує один контролер. Ці єдині контролери програмно-конфігурованих мереж зазвичай підходять для мереж з невеликим покриттям (тобто локальних мереж), однак вони стикаються з одноточковим збоєм і проблемами масштабованості. Використання єдиного контролера ПКМ для обмежень великої мережі з високою затримкою, перевантаженням і збоєм зв’язку в мережі також впливає на продуктивність мережі. Щоб вирішити проблеми в окремих контролерах ПКМ з точки зору масштабованості та затримки, вводиться концепція кількох контролерів, яка полегшує проблему одноточкового збою та забезпечує розподілене інтелектуальне рішення без затримок для мереж ПКМ. У деяких мережах також використовується концепція ПКМ із кількома контролерами та пом’якшується традиційний недолік до певного рівня. Використання кількох контролерів ПКМ викликає проблему розміщення контролерів, яка ставить питання про те, скільки

контролерів необхідно для надання гнучкої послуги в мережі і який контролер вибрано для розгортання мережі.

Вищезазначене питання також пов'язане з оптимальним розміщенням контролерів, задоволенням вимог до комутаторів і вибором високовідмовостійкого контролера. Вибір і розміщення контролерів в оптимальному місці зменшує затримку між кількома контролерами та комутаторами. В типових мережах використовуються евристичні підходи до задач розміщення регулятора; однак вони все ще обмежені в розгляді деяких важливих обмежень (наприклад, не враховують стійкість до відмов контролера та/або не враховують вимоги до комутаторів). Існуючі параметри евристичних алгоритмів стикаються з проблемами конвергенції, які також впливають на розміщення контролера, що впливає на продуктивність мережі. Загалом, проблема розміщення контролера в середовищі з декількома контролерами все ще є відкритою проблемою. У таблиці 4.12. представлено порівняння одного контролера та кількох контролерів:

Таблиця 4.12.

Порівняння одного контролера проти кількох

Один контролер ПКМ	**Кілька контролерів ПКМ**
Отримує глобальне подання мережі	Відсутність глобального подання мережі
Єдина точка збою	Немає єдиної точки збою
Відсутність масштабованості	Масштабована
Легко розгортати лише в застарілих середовищах	Підтримує як застарілі середовища, так і середовища ПКМ
Піддається високій затримці	Менша затримка
Не підходить для мобільних сценаріїв	Підходить для мобільних сценаріїв
Схильна до високого рівня відмов зв’язку	Немає відмов зв’язку
Висока перевантаженість мережі	Відсутня перевантаженість мережі

Програмно-конфігурована мережа - це архітектура, що розвивається, яка забезпечує масштабованість, гнучкість і ефективне керування мережею. Однак оптимальне розміщення контролера стикається з багатьма проблемами, що впливають на продуктивність мережі в цілому. Щоб створити багатоконтролерну ПКМ (МК-ПКМ), яка розгортається в середовищі програмно-конфігурованих мереж, я пропоную підхід, який використовує гібридний алгоритм, що покращує продуктивність мережі. Спочатку запропонована мережа будується на основі теорії графів, яка покращує зв’язок і гнучкість між комутаторами та контролерами. Після цього виконується вибір контролера шляхом підбору оптимального контролера з кількох доступних контролерів на основі функцій контролера за допомогою алгоритму оптимізації firefly, що покращує продуктивність мережі. Нарешті, розміщення кількох контролерів виконується для зменшення затримки зв’язку між комутатором і контролерами. Тут кілька контролерів розміщуються з урахуванням розташування та відстані з використанням гібридного метаевристичного алгоритму, який включає алгоритм гармонійного пошуку та алгоритм оптимізації рою частинок, у якому пропонується алгоритм АРЧ для автоматичного оновлення параметрів гармонічного пошуку. Моделювання розміщення кількох контролерів виконується симулятором мережі CloudsimПКМ, і результати моделювання демонструють запропоновані переваги з точки зору затримки розповсюдження, часу проходження, матриці часового сеансу, затримки, надійності та пропускна здатність.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

5.1. Вступ

Персональні комп’ютери, інші види оргтехніки та пристрої обробки інформації, які вміщають в себе технічні засоби, які перероблюють, передають та приймають інформацію, характеризуються електромагнітними випромінюваннями, які треба мінімізувати для зменшення витоку інформації. Також ці випромінювання негативно впливають на персонал, який обслуговує ці пристрої, так як електромагнітні випромінювання високих частот (особливо від генераторів надвисоких частот, пристроїв для зашумлення приміщень, пристрої вимірювання тощо) можуть призвести до дуже серйозних захворювань.

Інженер програмно-конфігурованих мереж повинен одночасно виконувати розробку програм та бути оператори електронно-обчислювальних машин.

В перщому випадку інженер ПКМ виконує роботу переважно з відеотерміналом та документацією (за потреби) й інтенсивного обміну інформацією з ЕОМ і високою частиною ухвалення рішень. Робота інженера характеризується інтенсивною розумовою та творчою працею з підвищенням напруження зору, можлива концентрація уваги на фоні нервово-емоційного напруження, незмінною робочою позою, загальною гіподинамією та періодичним навантаженням на кисті верхніх кінцівок.

В другому випадку інженер ПКМ виконує роботу, що пов'язана з обліком інформації (одержаної з ВДТ за попереднім запитом), або інформації, що надходить з нього, також супроводжується перервами різної тривалості, та пов'язана з виконанням іншої роботи. Також цей процес характеризується як робота з напруженням зору, частими невеликими фізичними зусиллями, постійним нервовим напруженням середнього ступеня і виконується у вільному темпі.

5.2. Аналіз умов праці на робочому місці інженера програмно-конфігурованих мереж

5.2.1. Організація робочого місця інженера ПКМ.

Кількість робочих місць інженера програмно-конфігурованих мереж визначається прямим рахунком кількості машин, механізмів, комп'ютерного обладнання, комплексів технологічного, а також організаційного оснащення при обслуговуванні (за нормами) кожної одиниці одним інженером. При цьому:

- як одне робоче місце зараховується кілька одиниць обладнання, що обслуговує один інженер за діючими нормами;

- якщо робота виконується одним інженером ПКМ у різних пунктах, то вся робоча зона прикладання праці рахується як одне робоче місце.

На робочому місці інженера ПКМ повинно бути декілька машин, механізмів, ПК, комплексів технологічного та організаційного оснащення, які він буде обслуговувати. Робоче місце інженера програмно-конфігурованих мереж повинно відповідати таким вимогам:

- Організація робочого місця повинна забезпечувати раціональний трудовий процес, якість роботи і безпеку.
- Робоче місце повинно бути добре освітлене.
- Робоче місце повинне бути обладнане трапами, стелажами для збереження інструмента і пристосувань, забезпечене необхідною документацією, у разі потреби обгороджене.
- Прийом їжі на робочому місці заборонений.

5.2.2. Перелік шкідливих та небезпечних виробничих чинників.

5.2.2.1. Бездротові мережі.

Wi-Fi - технологія, що дозволяє пристроям, таким як ПК передавати дані за допомогою бездротових технологій та для виходу домашніх комп'ютерів в Інтернет.

Wi-Fi - друга після стільникового найбільш поширена форма бездротової технології. Як і інші звичайні прилади типу мобільних телефонів, пристроїв Bluetooth, дистанційних пультів управління різноманітними приладами та дверима (наприклад, дверима для гаража) обладнання Wi-Fi випромінює хвилі радіочастоти. Радіовипромінювання є типом неатомної радіації, що на відміну від атомної радіації (випромінюваної, наприклад, рентгенівськими апаратами), не руйнують хімічні зв'язки. Частина випромінювання RF поглинається людським тілом, і ступінь поглинання залежить від того, наскільки близько людина знаходиться до пристрою Wi-Fi і наскільки сильний сигнал.

5.2.2.2. Неіонізуючі електромагнітні поля та випромінювання.

До неіонізуючі електромагнітних полів та випромінювання на робочому місці інженера програмно-конфігурованих мереж можна віднести наступні фактори:

Електростатичні поля та постійні магнітні поля.

Електричні та магнітні поля промислової частоти (50 Гц).

Електромагнітні випромінювання радіочастотного діапазону.

Електромагнітні випромінювання оптичного діапазону.

Лазерне та ультрафіолетове випромінювання.

5.2.2.3. Освітлення.

І останньою, актуальною умовою праці на робочому місці інженера програмно-конфігурованих мереж є освітлення:

Природне (може бути відсутнім або недостатнім).

Штучне (мало або недостатньо освітленості, прямий/відбитий сліпучий відблиск, тощо).

5.2.3. Аналіз шкідливих та небезпечних виробничих чинників, що діють на робочому місці інженера ПКМ.

5.2.3.1 Аналіз бездротових мереж.

На відміну від стільникових пристроїв, де передавач знаходиться в безпосередній близькості від голови і велика частина поглиненого випромінювання RF концентрується в надзвичайно обмеженій області, випромінювання від пристроїв Wi-Fi, як правило, впливає на людське тіло з набагато більшої відстані. Це призводить до дуже низьких середніх енергетичних рівнів поглинання радіохвиль у всіх частинах тіла, порівняно з рівнями FM − радіосигналів. Бездротові локальні мережі (WLANs або Wi-Fi,) для передачі даних використовують радіохвилі, так само, як звичайне радіо і телебачення або мобільні телефони.

В даний час вчені не знайшли жодного наукового доказу того, що WLANs представляють будь-яку загрозу для здоров'я. Останні фактичні дані досліджень Всесвітньої організації охорони здоров'я (ВОЗ):

- отримані результати досліджень не принесли доказів того, що RF, які виходять від базових станцій і бездротових мереж викликають несприятливі медичні ефекти;

- університет Пенсільванії провів 356 вимірювань у 55 містах присутності мережі Wi-Fi в чотирьох країнах в умовах, що перевищують звичайну ступінь впливу сигналу. Це дослідження дійшло висновку, що радіочастотні поля від WLAN, в звичайних сценаріях, працюють на рівнях значно нижчих, ніж граничні значення. У всіх випадках заміряні рівні сигналу Wi-Fi були набагато нижче міжнародних норм і, майже у всіх випадках, набагато нижче інших радіосигналів в тому ж навколишньому середовищі;

- Health Protection Agency (HPA) Великобританії констатує факт того, що Wi-Fi сигнали мають дуже низький рівень впливу і не становлять загрози для здоров'я: немає ніяких послідовних доказів впливів на здоров'я від RF, що не перевищують встановлену норму, і тому немає ніяких причин, для того щоби школи та інші заклади не могли використовувати обладнання Wi-Fi. Фактично, огляд HPA показав, що

емісія WLAN значно нижче норм інструкцій з техніки безпеки: агентство виміряло щільність впливу радіохвиль взагалі, а також в офісі, де розгорнуті мережі WLAN. Отримані показники набагато нижче встановлених норм.

У 2010 році Health Canada опублікував положення, в якому зазначено, що: Wi-Fi - друга найпоширеніша форма бездротової технології, після стільникового зв'язку. Вона широко використовується в школах, офісах, кафе, житлових будинках і т.д. Health Canada запевняє, що вплив радіохвиль за технологією Wi-Fi надзвичайно низький і ніяк не впливає на стан здоров'я. Отже можна стверджувати, що наукові дослідження демонструють, що сигнали Wi-Fi набагато нижче допустимих міжнародних норм і не вимагають обмежень у використанні і додаткових заходів безпеки.

5.2.3.2. Неіонізуючі електромагнітні поля та випромінювання.

Джерелами електромагнітного випромінювання у виробничому приміщенні інженера ПКМ можуть бути: неекрановані робочі елементи високочастотних установок (індуктори, конденсатори, ВЧ-трансформатори, батареї конденсаторів, фідерні лінії, або котушки коливальних контурів тощо). Під час експлуатації ВЧ-, ДВЧ-, УВЧ- передавачів на радіо- та телецентрах джерелами електромагнітного випромінювання є ВЧ генератори, антенні комутатори, різні пристрої складання потужностей електромагнітного поля та комунікації (від генератора до антенного пристрою).

Ступінь опромінення інженерів залежить від кількості передавачів (у деяких зонах, радіо- та телецентрах їх може бути до 20), потужностіцих пристроїв, екранування, розміщення окремих їх блоків усередині та поза приміщеннями.

Для всіх видів зв'язку джерелом електромагнітного випромінювання є передавальні станції. Дії енергії НВЧ діапазону працівники зазнають при регулюванні, настроюванні та випробовуванні радіопередавальних та радіолокаційних станцій.

Електромагнітні поля особливо негативно впливають на організм інженера, що безпосередньо працює з джерелом випромінювання. В діапазоні промислових частот більше негативний вплив на тіло людини має електрична складова поля.

Найчутливішими до ЕМП є нейродинамічні процеси, які прямо чи побічно перемикають хронобіологічні процеси організму на патологічний або стресовий режим функціонування.

При дії ЕМП на тіло людини можливі гострі та хронічні форми порушення фізіологічних функцій організму. Такі порушення можуть виникати в результаті дії електричної складової ЕМП на нервову систему, або дії на структуру кори головного/спинного мозку, а також серцево-судинної системи.

5.2.3.3. Освітлення.

Чинникам зовнішнього середовища, які впливають на організм інженера в процесі праці, відводиться одне із основних, а також головних місць. Даним чинником є освітлення, адже відомо, що людина отримує майже 90% всієї інформації про довкілля завдяки органам зору.

Світло впливає не лише на функцію зору, а й на діяльність організму інженера в цілому:

- активно посилюється обмін речовин,
- збільшується кількість поглинання кисню і відповідно, виділяється більше вуглекислий газ,
- сприятливо впливає на скелетну мускулатуру.

Недостатня кількість або надмірна освітленість, нерівномірне розприділення освітлення в полі зору може втомлювати очі, а також призводити до зниження продуктивності праці. При цьому це впливає на ріст потенційної небезпеки помилкових дій і нещасних випадків. Надмірна яскравість джерел світла також спричиняє головний біль, розлад гостроти зору та різати очі. Світлові відблиски можуть створити тимчасове засліплення.

Освітлення виробничих приміщень інженера програмно-конфігурованих мереж характеризується кількісними та якісними показниками. До основних кількісних показників відноситься: світловий потік, сила світла, яскравість і освітленість. До основних якісних показників зорових умов роботи можна віднести такі показники, як: фон, контраст між об’єктом і фоном, видимість.

5.3. Розробка заходів з охорони праці

5.3.1. Налаштування бездротових мереж.

Відповідно до фактів, що наведені у попередніх пунктах, немає ніяких видимих причин для відмови від тих величезних переваг, які забезпечує технологія Wi-Fi. Стандарти на пристрої Wi-Fi (IEEE 802.11 a/b/g/n) передбачають меншу різноманітність при управлінні вихідною потужністю передавачів пристроїв. До того ж, на вимоги, встановлені в самих стандартах, накладаються обмеження, встановлені різними регіональними нормами. У європейських вимогах вихідна потужність передавачів абонентських терміналів Wi-Fi обмежена значенням 100 мВт (+20 дБп). В реальних абонентських терміналах (телефонах, роутерах тощо) вихідні потужності передавачів Wi-Fi відповідають європейським обмеженням і зазвичай, з сертифікаційних документів не перевищують 60...70 мВт. Реальні вихідні потужності додаткових передавачів Bluetooth і Wi-Fi, вбудованих в мобільні термінали GSM-UMTS-LTE будуть залежати від режиму їх роботи. У контексті теми вихідної потужності пристроїв можна виділити два основні режими:

- режим «майстра», тобто пристрої (хости), керуючі роботою інших підключених до них пристроїв;

- режим «клієнта» − пристрої, що працюють під управлінням хоста, що виконує функції майстра.

У режимі «майстра» пристрій зобов’язаний забезпечувати інші пристрої сигналами синхронізації, тобто передавач буде працювати практично безперервно. У

режимі «клієнта» пристрій включає передавач лише у відведені інтервали часу для передачі інформації на інші пристрої. Таким чином, середня вихідна потужність передавача в режимі «клієнта» в середньому буде помітно нижче, ніж в режимі «майстра». Оскільки передбачити середню вихідну потужність у реальних умовах використання пристроїв Bluetooth і Wi-Fi складно, рекомендовано орієнтуватися на максимальні значення, як на найгірший варіант.

5.3.2. Забезпечення захисту від неіонізуючих електромагнітних полів та випромінювання.

Розпочати потрібно з вимірювання ЕМВ на підприємстві, якщо поруч проведена потужна лінія електропередач. Що дає вимірювання електромагнітного випромінювання? Для забезпечення захисту необхідно екранувати небезпечні місця проведення кабелів.

Можливі джерела ЕМВ: лінії електропередач, що проходять біля і через житлові квартали; стільникові антени, що встановлені на дахах будівель; різноманітні прилади та пристрої мережевого обладнання.

Для вимірювання ЕМП використовуються аналізатори ЕМВ або/та аналізатори низькочастотного електромагнітного поля. Виміряні показники необхідно порівнювати з гранично допустимими нормами, затвердженими Міністерством охорони здоров'я України та з вимогами Євросоюзу.

5.3.3. Забезпечення достатньої кількості освітлення.

Для створення сприятливих умов зорової роботи інженера ПКМ, які б виключили швидку втомлюваність та напруженість очей, виникнення професійних захворювань, та нещасних випадків, а також сприяли підвищенню продуктивності праці та якості продукції, виробниче освітлення повинне відповідати наступним вимогам:

– створювати на робочій поверхні інженера ПКМ освітленість, що відповідає характеру зорової роботи та встановленим нормам роботи;

– унеможливлеювати засліплюючу дію як від самих джерел освітлення, так і від інших предметів, які знаходяться в полі зору інженера;

– забезпечувати достатню рівномірність та постійність рівня освітленості у виробничих інженерних приміщеннях для уникнення частого перефокусування органів зору;

– контроль на робочій поверхні різких та/або глибоких тіней (особливо рухомих);

– забезпечувати достатній контраст поверхонь, які освітлюються, для розрізнення дрібних деталей;

– не створювати шкідливих виробничих факторів (таких, як:шум, теплові випромінювання, небезпечне ураження струмом, пожежо- та вибухонебезпека), що можуть бути небезпечними для інженера ПКМ;

– повинно бути надійним, зручним і простим в експлуатації, а також економічним та естетичним.

Залежно від джерела світла, виробниче освітлення може бути наступним: природним, штучним і суміщеним, при якому недостатнє природне освітлення доповнюється штучним.

Природне освітлення має важливе та необхідне фізіолого-гігієнічне значення для інженера ПКМ. Воно сприятливо впливає на органи зору, стимулює фізіологічні процеси та роботу, підвищує обмін речовин та покращує розвиток організму інженера в цілому. Сонячне випромінювання зігріває та знезаражує повітря в приміщенні, очищуючи його від збудників різноманітних хвороб (наприклад, вірусу грипу) та приємне. Окрім цього, природне світло має і психологічну дію, що створюює в приміщенні для працівників відчуття безпосереднього зв’язку з довкіллям та комфортної роботи.

Природному освітленню властиві і недоліки:

- непостійне в різні періоди доби, року та при різній погоді;

- нерівномірно розподіляється по усій площі виробничого інженерного приміщення;

- при незадовільній організації освітлення може викликати засліплення органів зору.

Природне освітлення поділяється на:

а) бокове (може бути одно- або двостороннє), коли освітлення здійснюється через світлові отвори (вікна) в зовнішніх стінах будівлі;

б) верхнє, коли освітлення здійснюється через ліхтарі та отвори в дахах, а також перекриттях;

в) комбіноване – поєднання цих двох видів освітлення.

На рівень освітленості інженерного приміщення при природному освітленні впливають також такі чинники як: світловий клімат, площа і орієнтація вікон, ступінь чистоти скла у вікнах, пофарбування стін та стелі приміщення, глибина інженерного приміщення, наявність зайвих предметів (заступають вікно як зсередини, так і ззовні приміщення).

Оскільки природне освітлення непостійне впродовж робочого дня, кількісна оцінка цього виду освітлення може проводиться за відносним показником – коефіцієнтом природного освітлення (КПО):

$$КПО = \frac{E_{вн}}{E_{зовн}}, \qquad (5.1)$$

де $E_{вн}$ – освітленість в даній точці приміщення зсередини, яке створюється світлом неба (безпосереднім чи відбитим);

$E_{зовн}$ – освітленість усієї горизонтальної поверхні, що створюється в той самий час світлом повністю відкритого небосхилу ззовні.

Нормовані значення КПО, включно для робочого місцяінженера ПКМ, визначаються Державними будівельними нормами ДБН В.2.5-28-2006. В основі визначення КПО покладено весь розмір об’єкта розпізнавання.

Штучне освітлення може бути загальним та комбінованим. Загальне - коли світильники розміщуються у верхній зоні робочого приміщення інженера (не нижче 2,5 м над підлогою) рівномірно (загальне рівномірне освітлення) або з врахуванням розташування робочого місця інженера ПКМ (загальне локалізоване освітлення). Комбіноване освітлення включає в себе загальне та місцеве. Його доцільно застосовувати при роботі, яка потребує високої точності, а також, якщо необхідно забезпечити створення певного або змінного напрямку світла в процесі роботи. Місцеве освітлення створюється розміщеними світильниками, що концентрують світловий потік безпосередньо на робочих місцях інженерів ПКМ. Застосування лише місцевого освітлення не допускається у роботі інженера з огляду на небезпеку виробничого травматизму та професійних захворювань.

Штучне освітлення передбачається у всіх виробничих приміщеннях, де недостатньо природного світла, а також забезпечує освітлення приміщень в темний період доби. При організації штучного освітлення створюються сприятливі гігієнічні умови для зорової роботи і одночасно враховуються економічні показники. Найменша освітленість робочих поверхонь інженерів у виробничих приміщеннях регламентується ДБН В.2.5-28-2006 і визначається, в основному, характеристикою зорової роботи людини. Норми носять міжгалузевий характе і на їх основі розробляють норми для окремих галузей промисловості. В ДБН В.2.5-28-2006 вісім розрядів зорової роботи, а саме: перших шість характеризуються розмірами об’єкта розпізнавання. Найбільша нормована освітленість складає 5000 лк, а найменша – 30 лк.

Як джерело штучного освітлення широко застосовуються та використовують лампи розжарювання та газорозрядні лампи. Перші відносяться до теплових джерел світла. Дані лампи характеризуються простотою конструкції та виготовлення, зручністю експлуатації, а також широким діапазоном напруг та потужностей. Поряд з перевагами їм також притаманні і суттєві недоліки: велика яскравість, низька світлова віддача (7–20 лм/Вт), відносно малий термін експлуатації лампи (до 2,5 тис. год), переважання жовто-червоних променів освітлення (якщо порівнювати з природним світлом), висока температура нагрівання (до 140 °С і вище), що робить їх

пожежонебезпечними у використанні. Дані лампи використовуються для місцевого освітлення, а також забезпечують освітлення приміщень з тимчасовим перебуванням людей.

Газорозрядні лампи випромінюють світло оптичного діапазону спектру. Основна перевага цих ламп - економічність. Світлова віддача даних ламп становить 40–100 лм/Вт (що в 3–5 разів перевищує світлову віддачу ламп розжарювання). Термін експлуатації лампи – до 10 тис. год, а температура нагрівання (люмінесцентні) досягає 30–60 °С. Окрім того, газорозрядні лампи можуть забезпечувати світловий потік практично будь-якого спектру (шляхом підбирання відповідним чином інертних газів, парів металу, люмінофора). Основним недоліком таких ламп є пульсація світлового потоку, що зумовлює виникнення стробоскопічного ефекту. До недоліків цих ламп можна віднести: складність схеми включення, шум дроселів, значний час між включенням та запалюванням ламп.

5.4. Пожежна безпека виробничого приміщення

Заходи щодо пожежної безпеки інженера ПКМ:

- використання конструктивних елементів та приладівз негорючих і важкозаймистих матеріалів.

- конструктивне проектування та розташування елементів з метою створення полегшеного режиму роботи;

- тепловідвід, охолодження окремих елементів ПКМ;

- вибір стандартної апаратури електрозахисту і стабільних плавких запобіжників;

- висвітлити пожежну профілактику електроустановок: якщо в приміщеннях знаходяться матеріали та речовини, що схильні до займання чи утворення вибухонебезпечної суміші з повітрям, необхідно зробити вибір типу виконання електрообладнання, рівня і виду вибухозахисту відповідно, спосіб прокладки проводів і кабелів;

- за наявності процесів, що супроводжуються утворенням зарядів статичної електрики, розглянути комплекс заходів, для забезпечення зниження небезпеки вибуху або пожежі від іскрового розряду;

- розглянути засоби гасіння пожеж, види апаратури і прилади (тип, кількість, розміщення);

- розробити план та розглянути засоби зв'язку та сигналізації, що забезпечують сповіщання про початок пожежі у виробничому приміщенні;

5.5. Розробка заходів щодо захисту від шкідливого впливу на здоров’я інженера ПКМ

Отже, для нормальної роботи інженера ПКМ потрібно мінімізувати випромінювання від ПК, інших видів оргтехніки та пристроїв обробки інформації. Враховуючи, що у сфері безпеки інформації за останні десять років використання таких пристроїв різко збільшилось, а корпуса пристроїв роблять із полімерних матеріалів (які пропускають ці види випромінювань), надійним технічним засобом їх захисту від випромінювань є застосування екранування у вигляді внутрішнього металевого покриття як місцевого, так і загального без зміни зовнішнього вигляду виробу.

Застосування технології газотермічного напилювання покриттів, що екранують ВЧ і НВЧ працюючих вузлів і блоків ПК, дозволить здійснити захист пристроїв (як тих, що розробляються, так і вже працюючих), незалежно від їх геометрії, розмірів та внутрішньої конфігурації. При цьому автоматично вирішується питання захисту інженера ПКМ від дії електромагнітного випромінювання ПК. Випробування ефективності екранування цих елементів були проведені в режимах тестування відповідних пристроїв (частин ПК, генераторів, іншої оргтехніки тощо). При цьому визначалася напруженість електричного і магнітного полів випромінюваних пристроями в діапазоні частот - 0-1000 МГц. За рахунок цього, одночасно підвищується захищеність пристроїв та зменшується негативний вплив на людину.

Одним із чинників, що негативно впливає на інженера ПКМ, є вібраційні канали її витоку. Захист вібраційних каналів є однією з головних проблем при проектуванні захищених приміщень. Навіть при розмові людей відбуваються вібрації на стінах, стелях, підлозі та вікнах. Для унеможливлення перехоплення цих вібрацій, встановлюються вібраційні пристрої, які своєю дією роблять сигнали мови такими, які неможна розібрати. Таких пристроїв є три види, негативний вплив від кожного виду пристроїв такий:

П'єзоелектричні – пристрої, які випромінюють сигнали НЧ та амплітуди. Саме цьому вони застосовуються при захисті вікон. На людину вони впливають негативно, так як частоти цих коливань дуже низькі, вухо не чує цих частот, але мозок сприймає та через деякий час інженер ПКМ може відчути головний біль.

Електромагнітні – пристрої, які можна використовувати на стінах, стелях та підлогах. Найнебезпечніші, так як є джерелом електромагнітного випромінювання. Вони є одні з найгірших з точки зору інформаційної безпеки, оскільки, створюють коливання ВЧ, які модулюються низькочастотним голосом людини.

Магнітодинамічні – пристрої, які застосовуються для захисту вібраційних каналів витоку інформації через стіни, стелю та підлогу. Вони мають магнітну котушку з залізним осердям всередині, яке створює вібрації. Ця конструкція працює як відбійний молоток, чим створює безліч шуму навколо себе. Працювати в таких умовах дуже складно, саме тому такі прилади використовуються лише в кімнатах для конфіденційних переговорів. Час знаходження в таких кімнатах з увімкненою апаратурою не має перевищувати двадцяти хвилин. Психічний стан працівників у сфері інформаційної безпеки – це одна з найважливіших складових, яка впливає на працездатність людини.

При комплексному захисті приміщень необхідно використовувати всі три види цих пристроїв. Кожне з них має свій негативний вплив на людину. При роботі з дуже важливими документами працівники відчутно хвилюються з того приводу, що можуть зробити помилки. Саме тому робітники цієї сфери повинні кілька разів за рік спілкуватися з психологами (залежно від їх емоційного стану та стажу роботи).

ВИСНОВКИ ДО РОЗДІЛУ 5

Охорона праці інженера ПКМ та у сфері інформаційної безпеки – це дуже складна процедура, яка у нашій країні потребує вдосконалення. Останнім часом спостерігається позитивна динаміка щодо відповідності правового забезпечення цього питання. Також переглядаються норми з допустимих рівнів випромінювання, часу роботи та інших речей, що пов'язані з роботою працівників. Перегляд норм необхідний, тому що деякі з них залишилися ще з радянських часів, а за останні роки швидко і суттєво змінилася техніка та її вплив на людину. Також проводяться досліди зі знаходження нових систем передачі, прийому та обробки інформації, які випромінюють менше енергії, що є позитивним фактором з наступних причин:

По − перше, чим нижче сила випромінювання, тим легше захищати інформаційні повідомлення від перехвату;

По − друге, це позитивно впливає на здоров'я інженерів, так як при зменшенні сили випромінювання, зменшується шкідливий вплив на працівника.

При подальшому розвитку науки цілком вірогідне створення екранів для усунення проникнення випромінювання через них, для забезпечення повного захисту людей та інформації. Також останнім часом все більше уваги приділяється психічному здоров'ю працівників, що дозволяє маюти у своєму штаті психолога. Впровадження нових програм тренінгів, спеціальних вправ з метою забезпечення охорони здоров'я інженерів ПКМ (користувачів технічних засобів захисту інформації).

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1. Вступ

У даному розділі узагальнено поняття про вплив на навколишнє середовище програмно-конфігурованих мереж та Інтернету. Виявлено три основні типи ефектів:

• Основний вплив: прямі наслідки виробництва та використання ПКМ на навколишнє середовище (використання ресурсів і забруднення, пов’язані з виробництвом інфраструктури та пристроїв ПКМ, споживання електроенергії обладнанням ПКМ, утилізація електронних відходів)

• Другорядний вплив: непрямий вплив на навколишнє середовище, пов'язаний із впливом ПКМ на структуру економіки, виробничі процеси, продукти та системи розподілу; основними типами позитивних впливів на навколишнє середовище є дематеріалізація (отримання більшої продукції за менші затрати ресурсів), віртуалізація (заміна матеріальних благ інформаційними товарами) і «демобілізація» (заміна спілкування на відстані подорожами)

• Додатковий вплив: непрямий вплив на навколишнє середовище, головним чином через стимулювання більшого споживання та вищого економічного зростання завдяки ПКМ («ефект відскоку»), а також через вплив на стиль життя та системи цінностей.

ПКМ мають глибокий вплив на навколишнє середовище, як позитивний, так і негативний. Незважаючи на те, що завдяки розповсюдженню ПКМ існують великі можливості для покращення навколишнього середовища та ресурсів, багато з цих можливостей призведуть до поступових змін у довгостроковій перспективі (загальне підвищення продуктивності праці, капіталу та ресурсів). Технологічні та організаційні зміни, зумовлені Інтернетом та іншими ПКМ-мережами, також можуть мати серйозні наслідки для навколишнього середовища, але доказів щодо знака та величини цих наслідків поки що мало.

Взаємозв'язок між розвитком, розповсюдженням і використанням інформаційно-комунікаційних технологій і більш широкою соціальною метою сталого розвитку недостатньо зрозумілий. Докладалися значні та зростаючі зусилля, щоб зрозуміти появу ПКМ як технології «загального призначення» та проаналізувати їхній вплив на економіку та суспільство. До недавнього часу ці дослідження стосувалися переважно певного діапазону впливів, пов’язаних із технологією: зміни в організації праці та продуктивності робітників; створення та втрата робочих місць; прибутковість компаній і галузей промисловості; структурні зміни в економіці та, зрештою, перспективи економічного зростання та національної безпеки. Розвиток комунікаційних мереж, і особливо поява Всесвітньої павутини, спричинили розквіт досліджень, пов’язаних із процесом «глобалізації» в усіх його аспектах; зміна політичної та фіскальної влади національної держави; питання ідентичності, формування груп і нових форм активізму; проблеми управління Інтернетом і його вплив на демократію; «цифровий розрив» тощо. Також було розглянуто низку науково-технічних питань: вплив ПКМ на проведення наукової діяльності; вплив кодифікації знань на технологічну дифузію; моніторинг зміни клімату тощо.

Вплив на стійкість навколишнього середовища лише нещодавно воно стало предметом систематичних досліджень. Частково це пояснюється тим, що вплив ПКМ на навколишнє середовище видається неспівмірним з їхнім величезним впливом на економіку та суспільство загалом. Порівняно з більш традиційними галузями, такими як енергетика, транспорт і виробництво, екологічне навантаження, пов’язане з виробництвом і використанням ПКМ, здається невеликим. Тому цей документ буде зосереджений здебільшого на непрямих впливах. Вони пов’язані з тим, як змінюється та реорганізується людська діяльність, і які наслідки це може мати для навколишнього середовища.

Дослідження зв’язків між ПКМ та екологічною стійкістю є складним і невизначеним завданням. Хоча статистичні джерела про поширення та економічний внесок ПКМ існують, вони, природно, пов’язані з реальністю, що швидко змінюється. Середньострокові та довгострокові прогнози, що стосуються, наприклад, кількості домогосподарств, підключених до Інтернету, або кількості та вартості електронної

комерції в роздрібній торгівлі та ланцюжку поставок сильно відрізняються, іноді на кілька порядків. Дослідження ймовірних майбутніх наслідків зростання цифрової економіки наразі ґрунтуються на гіпотетичному аналізі або аналізі на основі прикладів, що дає попередні та умовні результати. Це особливо вірно для літератури, що стосується більш опосередкованих і довгострокових ефектів, напр. через структурні зміни. Тому велика частина обговорення тут є спекулятивною і буде підлягати перегляду в міру того, як структура цифрової економіки продовжує розгортатися та завершуються ретельніші наукові дослідження.

6.2. Основний вплив програмно-конфігурованих мереж на навколишнє середовище

Прямі негативні впливи на навколишнє середовище виникають у результаті виробництва, використання та утилізації апаратного забезпечення, такого як комп'ютери, екрани, мережеві кабелі тощо. Вони радикально не відрізняються від впливу на навколишнє середовище багатьох інших продуктів, але становлять ряд конкретних екологічних проблем. Прямий позитивний вплив включає використання ПКМ для цілей захисту навколишнього середовища, напр. за допомогою електронного моніторингу токсичних викидів, дистанційного зондування, електронного контролю, загалом покращеної «прозорості» щодо використання екологічних послуг, потенціалу більш дешевого розмежування прав власності на навколишнє середовище.

Основний безпосередній вплив ПКМ на навколишнє середовище переважно пов'язаний із такими чотирма факторами:

1) Виробництво обладнання ПКМ

Сучасні системи ПКМ покладаються на різноманітні продукти з різнорідними характеристиками середовища. До них входять такі групи продуктів, як персональні комп'ютери, мережеві сервери, мобільні телефони, кабелі, супутники, периферійні пристрої (екрани, принтери, сканери тощо) тощо. Сектор все ще розширюється і зараз становить значну частину ВВП у більшості промислово розвинених країн.

Більшість продуктів складається з великої кількості різних компонентів, наприклад, мікросхеми, напівпровідники, друковані плати, електронно-променеві трубки та батареї. Виробництво багатьох із цих компонентів має важливий вплив на навколишнє середовище. Виробництво напівпровідників, наприклад, спричиняє значну кількість викидів у повітря (кислотні пари, леткі органічні сполуки та допінг-гази), викиди у воду (розчинники, мийні розчини, кислоти, метали) та відходів (кремній, розчинники). Виробництво інших компонентів також є екологічним питанням. Використання управління процесами та нових матеріалів, однак, зменшив масштаб проблеми. Наприклад, токсичні розчинники, які колись використовувалися для очищення друкованих плат, були значною мірою усунені завдяки процесам контролю якості. Загалом виробництво обладнання ПКМ призводить до викидів кислот, металів, летких органічних сполук, хлорованих розчинників та інших речовин. Він енергоємний і використовує велику кількість води для охолодження та промивання.

2) Транспортування комплектуючих і виробів.

ПКМ виробляються через глобальні ланцюги поставок. Типовий персональний комп’ютер містить 1500–2000 компонентів, які надходять із усього світу та зазвичай транспортуються повітряним транспортом. Складність і масштаби світового сектору електроніки означають, що сукупний вплив цих ланцюгів постачання на навколишнє середовище є великим. Електронна комерція може спричиняти «звуження» ланцюжка поставок (забезпечуючи більший контроль і зменшуючи кількість кроків), таким чином приносячи вигоди для навколишнього середовища, але вона також може мати протилежний ефект, дозволяючи ланцюжкам поставок стати більш «глобалізованими». і сегментований.

3) Використання ПКМ обладнання

Пристрої ПКМ зазвичай споживають велику кількість електроенергії. Типовий ПК середнього розміру споживає приблизно 150 Вт на годину. Але використання енергії в житлових приміщеннях також зростає завдяки інтеграції ПКМ у всі продукти і навіть товари. До них належать сучасне телевізійне та аудіообладнання, мобільні телефони, ігрові приставки, кишенькові персональні цифрові помічники та багато

інших інформаційних пристроїв. Очікується, що до 2023 року телевізійні приставки (інтегровані декодери приймачів) додадуть приблизно 10 000 ГВт-год електроенергії в Uł (і 0,8 мільйона тонн викидів вуглецю). Втрати в режимі очікування, пов'язані з побутовими електронними товарами, є ще одним основним джерелом споживання енергії. Ці пристрої забезпечують миттєве ввімкнення та споживають 5-15 відсотків спожитої енергії в житлових приміщеннях.

Комп'ютери, інформаційні технології та інші інформаційні пристрої також є найбільшим джерелом зростання попиту на електроенергію в комерційних будівлях. На відміну від приватних персональних комп'ютерів, багато професійних робочих станцій і мережевих серверів, як правило, працюють цілодобово.

Існують численні спроби зменшити споживання електроенергії обладнанням ПКМ. Комп'ютери та особливо ноутбуки часто мають розширені системи керування живленням, які зменшують споживання електроенергії шляхом впровадження різних «режимів низького споживання» після певного часу бездіяльності. Однак підвищення продуктивності та, що важливіше, збільшення розмірів екранів у минулому були збалансовані або надмірно компенсовані цим підвищенням ефективності.

4) Утилізація ПКМ обладнання.

Продуктивність ПКМ подвоюється кожні 18 місяців. Це спостереження виявилося відносно точним не лише щодо швидкості процесора, але також щодо ємності пам'яті та швидкості передачі даних.

Надзвичайно швидкі інноваційні цикли призвели до високого обороту апаратного та програмного забезпечення. У результаті стрімко зростаючий потік електричних та електронних відходів став важливим питанням порядку денного екологічної політики.

Основною проблемою утилізації є вміст металу в електронних відходах. Пристрої ПКМ зазвичай містять значну кількість міді, свинцю та ртуті. Поточна конструкція продукту не дозволяє відокремлювати та переробляти ці метали без подальшої обробки. Ряд інших матеріалів, таких як антипірени та пом'якшувачі пластику, також є причиною екологічних ризиків. Наразі лише незначна частина апаратного забезпечення ПКМ переробляється.

Хоча значні прогалини в даних і технології, що швидко змінюються, не дозволяють надійно оцінити ці наслідки, широко визнано, що виробництво, використання та утилізація ПКМ стали серйозною проблемою екологічної політики. Близько 4% міських відходів зараз припадає на «відходи від електричного та електронного обладнання» (WEEE) і що ця частка має зростати. Значну частину цього матеріалу можна було б економічно переробити, якби були ефективні системи збору та обробки. Однак ці прямі наслідки можуть бути менш значними, ніж потенційно набагато ширші та глибші непрямі наслідки інформаційно-комунікаційних технологій.

6.3. Другорядний вплив ПКМ

Очікується, що ефекти другорядного впливу будуть переважно позитивними. ПКМ сприятимуть розмежуванню економічного зростання та екологічної шкоди. Висуваються дві основні причини.

По-перше, додана вартість, створена використанням інформаційних технологій в економіці, була охарактеризована як пов’язана здебільшого з маніпулюванням ідеями, а не енергією та матеріалами. Інформаційні технології сприяють структурним змінам економіки від енерго- та матеріаломісткої діяльності до інформаційно-інтенсивної діяльності. Ці інвестиції та структурні наслідки для економіки, очевидно, мають велике значення для екологічної ефективності в сукупності, навіть якщо вимірювання цих наслідків виявилося невловимим.

По-друге, і, важливіше, інформаційні технології змінюють спосіб розробки, виробництва, розповсюдження та експлуатації практично кожного продукту та послуги в економіці. Тому економіка розглядається як зростаюча не за рахунок додавання додаткових ресурсів, а за рахунок більш розумного використання ресурсів для отримання більшої вартості. Дійсно, у багатьох галузях повністю нематеріальні активи є критичними компонентами вартості, яку вони створюють. Існують переконливі докази того, що інформаційні технології підвищили продуктивність

праці, але також пропонується різке підвищення продуктивності капіталу та ресурсів. Така ефективність досягається за рахунок змін, що впливають на ряд видів діяльності:

• інтелектуальні виробничі процеси: завдяки ретельному комп'ютерному проектуванню виробничих приміщень і точному контролю операцій під час виробництва, що стало можливим завдяки численним датчикам і автоматизованому контролю.

• інтелектуальне проектування та робота продуктів: завдяки комп'ютерному моделюванню продуктивності продукту створюються «легші» продукти, які використовують менше матеріалів, щоб зробити продукти, які працюють ефективніше; ефективні датчики та засоби керування забезпечують ефективне надання послуг/функцій тоді та де вони потрібні

• реорганізація ланцюгів постачання та організації бізнесу: електронна комерція призводить до закриття роздрібних точок, більш ефективного управління запасами та ланцюгом постачання, зростання «дистанційної роботи»

• інтелектуальна логістика та розподіл: використання засобів зв'язку та комп'ютерних систем управління та відстеження покращує як гнучкість (точно вчасно), так і ефективність систем розподілу.

• процес «електронної матеріалізації»: заміна матеріальних благ нематеріальними послугами (наприклад, придбання програмного забезпечення через Інтернет безпосередньо, а не на диску, розробка «електронного паперу»)

• Мережевий ефект, що сприяє розповсюдженню кодифікованої інформації: використання комп'ютерів, цифрових засобів зв'язку та мереж може сприяти швидшій кодифікації та рутинізації багатьох видів економічної діяльності, що приносить інтеграцію та підвищення ефективності (також з відповідними перевагами для навколишнього середовища).

Але цей перелік потенційних позитивних впливів супроводжується невизначеністю щодо того, чи будуть вони реалізовані. Хороші емпіричні докази, з яких можна винести узагальнені уроки, нечисленні. Дослідження «парадоксу продуктивності» (тривала дискусія щодо відсутності доказів зв'язку між продуктивністю праці та інвестиціями в ПКМ) повторюється в проблемах, з якими

стикаються аналітики, коли роблять сильні висновки про зв’язки між ПКМ та продуктивністю навколишнього середовища/ресурсів. Те, що докази дійсно існують, здається, збентежує оптимістичне читання.

• збільшення продуктивності ресурсів є повільним: ПКМ стали інтегрованими у виробничі процеси та нові продукти протягом тривалого періоду (понад 20 років). Докази більшості секторів свідчать про те, що підвищення продуктивності ресурсів відбувається, як правило, повільно, і лише частину можна пояснити розповсюдженням ПКМ. Дематеріалізація є давньою історичною тенденцією.

• можливості для електронної матеріалізації можуть бути обмеженими: заміна «байтів на біти» може в деяких випадках бути повною (MP3, електронні книги), але кількість товарів і послуг, де це може бути досягнуто, може бути обмеженою. Для більшості товарів ІТ інтегровані в доставку товару чи послуги, але не замінюють їх. Дійсно, використання електроніки може призвести до більшого навантаження на навколишнє середовище, пов’язаного з використанням продукту (прикладом є швидке розповсюдження батарей для живлення інтелектуальних функцій у споживчих товарах).

• неповна заміна: багато товарів і послуг, які підтримуються ПКМ або Інтернетом, надходитимуть «на додаток» до існуючих товарів і послуг, особливо під час початкової фази переходу.

• Взаємозв'язок між віртуальною та матеріальною економікою: Віртуальна економіка тісно вбудована в реальну, матеріальну економіку. Зростання віртуальної економіки, швидше за все, призведе до змін і зростання матеріальної економіки. Наприклад, електронна комерція, швидше за все, залежатиме від розвитку швидшої, гнучкішої транспортної інфраструктури з більшою пропускною здатністю.

Найважливішим негативним ефектом другорядного впливу може бути неповна заміна існуючих структур і видів діяльності, що призведе до ще більшої шкоди навколишньому середовищу. Прикладом може служити випадок «безпаперового офісу». Використання комп’ютерів у бізнес-адмініструванні не замінило звичайну документообіг, а доповнило її, і обіцянка екологічно чистого «безпаперового офісу» не справдилася. Подібним чином нові логістичні системи для роздрібної електронної

комерції можуть призвести до додаткового транспорту, якщо вони є не інтегровані з існуючими системами або якщо споживачі суттєво не зменшують кількість індивідуальних поїздок за покупками.

Вважається, що інформаційні технології забезпечують великий потенціал для зменшення використання енергії та матеріалів. Вони відіграють ключову роль у дебатах про ефективне використання ресурсів. Прихильники цієї концепції стверджують, що передові технології можуть підвищити екологічну ефективність багатьох продуктів і процесів на кілька сотень відсотків, дозволяючи роз'єднати криву економічного зростання та криву шкоди для навколишнього середовища. Хоча інші технології та структурні зміни також вважаються важливими, найбільші сподівання покладаються на дематеріалізацію через електронні комунікації.

Розробка, виробництво та розповсюдження продуктів і послуг включають дуже складні процеси, в яких інформаційні технології відіграють дедалі важливішу роль. ПКМ використовуються різними способами для оптимізації вкладення праці, капіталу та природних ресурсів. Незважаючи на необхідність скорочення витрат, оптимізація процесів за допомогою ПКМ загалом принесла користь навколишньому середовищу. Це відбувається не лише тому, що за багато екологічних ресурсів потрібно платити (у більшості промислово розвинутих країн є плата за воду, стічні води, відходи, електроенергію), а й тому, що ефективні процеси, як правило, менше забруднюють навколишнє середовище. Позитивний вплив ПКМ на навколишнє середовище впливає на багато різних аспектів виробничого процесу.

1) Інтелектуальні виробничі процеси

ПКМ дозволяють симулювати складні виробничі системи, щоб перевірити та переглянути витрати, використання матеріалів і викиди в навколишнє середовище варіантів проектування перед придбанням систем. Після введення в експлуатацію недорогі датчики по всій установці в поєднанні з комунікаційними мережами та комп'ютерними засобами керування можуть забезпечити ефективну та гнучку роботу. Сучасні виробничі системи можуть мати десятки тисяч вбудованих мікропроцесорів, які керують клапанами, вимірюють температуру, визначають колір рідин та виконують інші завдання. Ці пристрої все частіше об'єднуються в мережу,

покращуючи якість, безпеку та зменшуючи відходи. Сьогодні до 40% вартості нового виробничого процесу припадає на системи управління. Точне електронне керування має важливе значення для мінімізації викидів. Покращений контроль означає, наприклад, що матеріал не витрачається, тому що хімічний процес не завершено або тому, що помилки залишаються непоміченими, виробляючи партії непридатного продукту. Відходи, як правило, є показником неефективності та поганого дизайну та функціонування процесу. Покращення продуктивності ресурсів такого типу досягалося в промисловості послідовно відтоді, як комп'ютери вперше були введені у виробництво

2) Розумне проектування та експлуатація продуктів і послуг

Використання програмного забезпечення для проектування та інструментів моделювання призводить до зменшення відходів (під час виробництва та експлуатації), створює продукти, які є більш «придатними для використання» та менш марнотратними, а також продукти, які втілюють більше інновацій, у тому числі інновацій, які є корисними для навколишнього середовища. Автоматизоване проектування є ознакою проектування продуктів і процесів і наразі воно поширене. Такі концепції, як «дизайн для навколишнього середовища» та «дизайн для переробки», можна легше інтегрувати в інноваційні процеси за допомогою цих інструментів проектування та моделювання. Конкретні ефекти важко виміряти, а відносну значущість програмного забезпечення для проектування важко відокремити від інших розробок, таких як досягнення в нових матеріалах і металургії.

Багато складних продуктів (споживчі товари тривалого користування) містять мікропроцесорні елементи керування, які дозволяють їм реагувати на зміну умов продуктивності та умов навколишнього середовища. Вбудовані елементи керування покращують функціональність продукту, але також впливають на його екологічні характеристики. Усі споживчі товари, а в майбутньому також менш складні продукти містять мікропроцесори для контролю їхньої поведінки за змінних умов. Серед іншого, вони контролюють викиди в навколишнє середовище, а також використання тепла, води та інших ресурсів. Удосконалені системи керування також мають вирішальне значення для управління новими складними гібридними технологіями. Ці

нові системи потребуватимуть контролю за заряджанням і розряджанням акумуляторів і новими системами накопичення енергії та іншими операціями.

Крім підвищення ефективності, заміна матеріалів та енергії інформацією також була запропонована як така, що веде до екологічних переваг. Заміни можуть бути частковими (дематеріалізація) або повними (віртуалізація). Найяскравішими прикладами цих ефектів є заміна «традиційних» носіїв цифровою інформацією. У більш широкому сенсі наводиться аргумент, що персональні комп'ютери та інші пристрої збільшать легкість, з якою інформація може бути засвоєння та передана, тим самим зменшуючи транзакційні витрати та усуваючи багато екологічних витрат, пов'язаних з паперовими транзакціями.

3) Розумний розподіл і логістика

Збільшення кодифікації знань і координації завдяки інформаційним технологіям допомогло зробити ланцюги поставок більш ефективними. Зменшення та швидше переміщення запасів призводить до значного, хоча й одноразового, скорочення рівня втрат. Тиск ринку також може сприяти подальшим покращенням. Електронний бізнес-бізнес (B2B) біржі закупівель і реверсивні аукціони спрямовані на зменшення витрат, запасів і втрат у ланцюжку поставок і збільшення використання наявних потужностей. Останні два фактори створюють безпосередні переваги для навколишнього середовища через збільшення продуктивності ресурсів – зменшення використання енергії та матеріалів і відходів. Однак деяке підвищення ефективності може бути компенсовано попитом на високу швидкість і своєчасну доставку, що призведе до зниження рівня використання транспортних засобів. Яка з цих тенденцій переважатиме, певною мірою залежить від структури цін і транспортних систем.

Збільшення можливостей замовлення, які електронний бізнес надає як підприємствам, так і споживачам, призведе до більш географічно розширених моделей поставок, а отже, до більшої інтенсивності транспортування товарів. Існує чимало доказів того, що це відбувається в глобальному масштабі. Найкращим об'єктивним показником є високі темпи зростання повітряних вантажних перевезень, який частково зумовлений електронним бізнесом. Зростаюча складність управління

спеціалізованим ланцюгом постачання як імпортерами, так і експортерами, а також створення он-лайн ринків у більшості секторів, ймовірно, посилять цю тенденцію.

Торгівля, керована електронним бізнесом, була б менш інтенсивною у транспортуванні, якби більше товарів можна було доставляти морським та залізничним транспортом, а не повітряним та автомобільним транспортом. Однак електронна комерція зазвичай вимагає швидких і дуже гнучких ланцюжків поставок, тоді як залізничний і морський транспорт є найповільнішими та найменшими. Гнучкі режими, з високими витратами на інфраструктуру та залежністю від регулярних масових поставок. Цей внутрішній недолік посилюється повільнішим проникненням електронного бізнесу в залізничний і морський сектори.

Онлайн-замовлення збільшує кількість постачальників і зменшує середні розміри замовлень, що ускладнить розподіл екологічної відповідальності між учасниками мережі. За останнє десятиліття загальною тенденцією в ланцюгах постачання є робота з меншою кількістю постачальників, особливо з ключовими постачальниками «першого рівня» (які часто координують внесок постачальників «другого рівня»). Однак розвиток «платформ» електронної комерції B2B полегшує пошук від більшої кількості постачальників із ширшого географічного діапазону. Особливо це стосується предметів технічного обслуговування, ремонту та експлуатації, а також товарів, які складають основну частину закупівель B2B за вартістю. Основним рушієм є пошук нижчих операційних витрат на пошук товарів і укладання контрактів на їх придбання.

Організаційні та особисті зв'язки між клієнтами та постачальниками можуть бути послаблені B2B обмінами, що ускладнює окремим клієнтам чинити неофіційний тиск з метою вдосконалення. Найкращим засобом подолання цих сил, ймовірно, будуть процедури попередньої кваліфікації щодо екологічних і соціальних показників. Альтернативним або додатковим варіантом було б вимагати від покупців надавати екологічну та соціальну інформацію про товари, які вони продають, можливо, на основі стандартизованих параметрів.

4) Зміна відносин між продавцем і покупцем

Масова адаптація – виробничі системи, які виробляють продукцію для індивідуальних споживачів – була запропонована як майбутній принцип організації бізнесу, так само як масове виробництво на конвеєрі було організуючим принципом бізнесу за фордизму. У моделі масового виробництва компанії підтримують відносини «від телефону до багатьох» зі споживачами. Споживчий попит прогнозується, і для задоволення цього попиту розроблено обмежену кількість продуктових ліній. За допомогою брендингу та реклами споживачів спонукають купувати товари, які вже виготовлені та є на полицях магазинів. На стабільних товарних ринках ця модель добре працює. Але є багато можливостей для неефективності: нові лінії продуктів, які не продаються; перевиробництво через зміни у смаках чи економіці; нові технології, які роблять продукти застарілими.

ПКМ та Інтернет роблять можливим масове налаштування, тому що вони забезпечують насичений обмін інформацією між компаніями та окремими клієнтами (приватними чи комерційними). Основним ефектом може бути різке скорочення запасів. Як показали комп'ютери Dell, у таких швидкозмінних галузях, як електроніка, де вартість комп'ютерних чіпів та інших компонентів знецінюється з кожним днем, є очевидні бізнес-вигоди від скорочення запасів обладнання та машин, які незабаром застаріють.

Було запропоновано декілька екологічних переваг для масового налаштування. По-перше, виробництво можна більш точно адаптувати до споживчого попиту, зменшуючи енергію, пов'язану зі складуванням продукції. По-друге, надлишкові запаси та втілені в них відходи зменшаться. По-третє, продукти та послуги можуть бути розроблені для точніше відповідає функціональності, бажаній споживачем, таким чином підвищуючи екологічну ефективність, з якою вона використовується. По-четверте, виробника можна перетворити на постачальника послуг для кінцевого споживача, пропонуючи нові можливості для бізнесу, водночас створюючи умови для того, щоб право власності (і відповідальність) на продукти, що надають послуги, залишалося за постачальником послуг.

5) Організація роботи

Дистанційна робота. Основні передбачувані екологічні переваги дистанційної роботи полягають у зменшенні потреби в офісних приміщеннях, що веде до економії енергії, а також у зменшенні кількості поїздок на роботу, що забезпечує економію енергії, зменшення забруднення повітря та зменшення заторів. Хоча в деяких випадках ця економія може бути досягнута, є також докази того, що в деяких секторах послуг працівники можуть стати більш перипатичними.

У той час як ПКМ та Інтернет-послуги можуть замінити деякі матеріальні товари та послуги, заміна рідко буває повною. Неповна заміна справді може призвести до нового попиту та інвестицій у товари та інфраструктуру, а отже, призвести до більшого використання ресурсів і забруднення.

Ймовірно, це явище виникне у сфері логістики. Збільшення онлайн-покупок зараз створює нові транспортні структури. Наприклад, ряд роздрібних мереж розпочали великі операції електронної комерції, що потребує нових (або розвитку існуючих) кол-центрів, складів, центрів збору та пакування, транспортних засобів доставки тощо. Ця нова інфраструктура, якою інтелектуально керують за допомогою ПКМ, має потенціал бути більш ефективною, ніж велика кількість індивідуальних поїздок за покупками, особливо якщо вони замінюють поїздки до торгових центрів за містом. Проте переваги для навколишнього середовища відбудуться лише в тому випадку, якщо ці нові інфраструктури призведуть до очікуваних ефектів заміни.

Деякі споживачі можуть вибрати частину своїх покупок в Інтернеті (наприклад, важкі або дешеві товари), але все одно їхати в центр міста, щоб купити інші товари. Подібних явищ можна очікувати і в інших областях. Ці нестабільні моделі заміщення будуть найбільш очевидними в період переходу (і накладання) між традиційною системою та системою, що базується на ПКМ. Але, як і у випадку з «безпаперовим офісом», перехідний період може тривати багато років, оскільки поведінка споживачів не завжди відповідає очікуванням тих, хто прогнозує віртуалізацію економіки. Твердження про ефект заміщення необхідно ретельно оцінювати. Багато хто залишається спекулятивним.

Інформаційні технології можуть у деяких випадках призвести до «рематеріалізації» економічної діяльності. Незважаючи на те, що багато цифрових

пристроїв (ПК, стільникові телефони) були суттєво мініатюризовані та «дематеріалізовані», вони також значно збільшили здатність кінцевого споживача споживати. Посилюючи конкуренцію, інтегруючи ринки та знижуючи ціни, ці пристрої надають нові можливості для споживання як матеріальних, так і нематеріальних товарів і послуг. Зокрема, Інтернет збільшує «охоплення» споживачів з точки зору вибору та географічно. Одним із конкретних прикладів рематеріалізації є доступ до документів через Інтернет, що дозволяє отримати друковану паперову копію лише кількома клацаннями миші.

Електронна комерція також може забезпечити легший доступ до ринків для постачальників у віддалених місцях і до товарів для знедолених споживачів. Хоча це явище може мати суспільно корисні наслідки, наслідки для транспорту є проблематичними. Ці ефекти тепер можна ідентифікувати в усьому світі. Наприклад, індійські фермери використовували Інтернет, щоб перевірити ціни на регіональних ринках, які можуть бути набагато вищими, ніж ті, що пропонують місцеві торговці (<loyd 2000). Тепер вони обходять їх і транспортують свою продукцію безпосередньо на регіональний ринок. Хоча це означало довші перевезення - до 00 км - ціни, які вони можуть отримати, іноді на 50% вищі, ніж місцеві.

6.4. Додатковий вплив на навколишнє середовище

Ефекти додаткового впливу пов’язані з процесами зворотного зв’язку, які можуть мати протиінтуїтивні результати. Це потенційно найсильніші наслідки, але їх також важко оцінити. Добре відомим механізмом зворотного зв’язку є так званий «ефект відскоку», який часто спостерігається в транспортному та енергетичному секторах. Це відбувається, коли підвищення ефективності (прямо чи опосередковано) стимулює новий попит, який урівноважує (або навіть надмірно компенсує) позитивний вплив на навколишнє середовище. Скептики побоюються, що економічний розвиток, який стимулюють ПКМ, може нівелювати описані вище екологічні переваги. Чи зможе дематеріалізація економіки встигати за підвищенням темпів зростання ВВП, стимульованим широким розповсюдженням ПКМ, залежить

головним чином від колективного вибору споживачів. Чи будуть гроші та час, звільнені завдяки використанню ПКМ, витрачені на споживання екологічно шкідливих товарів і послуг чи через попит на менш відчутні послуги? Анекдотичні дані наразі свідчать про те, що ефект відскоку є реальною загрозою для поступового підвищення ефективності. Наприклад, здається, існує позитивна кореляція між використанням електронної пошти та діловими поїздками, причому одне стимулює інше. Подібною історією є спостереження про те, що після програмного забезпечення другим за величиною ринком електронної комерції є продаж квитків онлайн на транспортні послуги. Процес соціальної та культурної глобалізації може стати ще одним ефектом третього порядку. Якщо глобальні комунікаційні технології (супутникове телебачення, Інтернет, електронна пошта) об'єднають різні культури, це, ймовірно, також призведе до більшого матеріального обміну, особливо через торгівлю та подорожі на великі відстані.

ПКМ та Інтернет глибоко впливають на структуру економіки, змінюючи відносний розмір і важливість промислових секторів і підгалузей, а також розмір і демографічну структуру (народження, виживання, смерть) фірм. На перший погляд, здається, що ці зміни матимуть позитивний вплив на екологічну стійкість, особливо через зростання «легких» послуг за рахунок «важкого» виробництва. Але чистий ефект цих структурних змін залежатиме від балансу між відносним балансом цих «освітлюючих» ефектів та протидії впливу економічного зростання (що все ще призводить до чистого зростання попиту на матеріальні ресурси), а також фізичних інвестицій. які генеруються, щоб уможливити та мотивувати Інтернет-економіку.

На макроекономічному рівні поняття дематеріалізації (або гіпотеза «інтенсивності використання») вперше обговорювалося в 1900-х роках і створило гіпотезу «Екологічної кривої лузнеца» (ЕЇС). Загалом це стверджує, що під час процесу індустріалізації економіки інтенсивніше використовують матеріальні ресурси (сталь, цемент, енергоносії), доки не буде досягнуто порогу, після якого структурні зміни в економіці (занепад виробництва та зростання сфери послуг) призводять до поступово менш інтенсивне використання матеріалів.

ПКМ роблять значний внесок у структурні зміни, які зменшують відносну ресурсомісткість економіки. Це відбувається через зростання послуг, пов'язаних з IT (наприклад, розробка програмного забезпечення, Інтернет-послуги, нові рекламні та маркетингові послуги тощо), і через зростання традиційних послуг (наприклад, фінансових послуг). Сектори послуг підтримуються матеріальною інфраструктурою та транзакціями (наприклад, транспортні послуги) і не є такими «чистими», як іноді представляють. Однак вони, як правило, створюють вищу додану вартість із меншим впливом на навколишнє середовище.

Поширення ПКМ пришвидшує ці триваючі структурні зміни і, отже, сприяє поступовому покращенню відносної ефективності використання ресурсів. Але емпіричні дані також показують, що в абсолютному вираженні ці економіки все ще «матеріалізуються» (тобто стають важчими). Надто оптимістична оцінка також була б недоречною, оскільки структурні зміни не змогли вирішити низку важливих екологічних проблем, таких як втрата біорізноманіття, землекористування, відходи та зміна клімату. Здається, вони тісно пов'язані із загальною економічною діяльністю, а не з конкретними галузевими подіями.

Термін «ефект відскоку» використовується для опису ряду ефектів зворотного зв'язку, які часто суперечать інтуїції, які компенсують або надмірно компенсують підвищення екологічної ефективності. Ці наслідки спостерігалися, наприклад, у транспортному секторі, де успішні заходи щодо зменшення трафіку призвели до звільнення доріг, що, у свою чергу, стимулювало новий трафік і зростання заторів. Ефект відскоку може бути викликаний двома основними ефектами: падіння цін і збільшення потужності.

Оскільки всі описані механізми (і більш конкурентні відкриті глобальні ринки) сприяють більш ефективному використанню природних ресурсів, ціни на сировину та інші виробничі ресурси (електроенергію, газ, метали тощо) матимуть тенденцію до зниження. Тиск витрат, який є одним із головних факторів підвищення екоефективності, зменшується, а підвищення ефективності використання ресурсів може сповільнитися. Виробники матеріалів, на які падає попит, зазнають економічних збитків і будуть намагатися знайти нові ринкові можливості.

Оскільки багато матеріалів мають потенціал для заміни, наприклад, вікна можна виготовляти з дерева, пластику та алюмінію, можна отримати доступ до нових ринків екологічно шкідливих матеріалів.

Другий механізм – генерація нової потужності. Багато додатків ПКМ дозволяють краще керувати часом, грошима, робочою силою, транспортною інфраструктурою тощо. Це призводить до нових потужностей, які неминуче будуть заповнені. Ключове питання полягає в тому, чи витрачаються час і гроші, виручені завдяки використанню ПКМ, більш чи менш шкідливо для навколишнього середовища.

Нарешті, нові інформаційні технології матимуть більший вплив на соціальні цінності, стиль життя та культуру. Хоча ці зміни та їхній вплив на навколишнє середовище залишаються дуже спекулятивними, слід зазначити, що зараз точаться жваві дебати.

Одним із широко обговорюваних трендів є можлива поява нового зеленого консьюмеризму, заснованого на нових можливостях інформаційних технологій. Загалом очікується, що багатші суспільства перейдуть до постматеріалістичних цінностей. Системи ПКМ могли б дозволити споживачам і громадянському суспільству втілити ці цінності в купівлю та інші рішення. Наприклад, нові інформаційні онлайн-сервіси могли б надати споживачам більше інформації про «етичну» ефективність конкуруючих продуктів і дати їм можливість взяти на себе більше відповідальності за спосіб життя та звички, які менш обтяжливі для навколишнього середовища. Споживачі, маючи можливість робити свідомий вибір щодо продуктів на основі екологічних критеріїв, могли б стимулювати більш екологічно відповідальне виробництво та інновації.

З іншого боку, той факт, що мережі ПКМ зменшують важливість географічної відстані, також може призвести до повторної мобілізації не лише товарів, а й робочої сили та дозвілля. Більший зв’язок між людьми, який забезпечується електронною поштою та Інтернетом, майже напевно стимулюватиме бажання зустрітися безпосередньо, поділитися матеріальними благами та відчути специфіку місць.

ВИСНОВКИ ДО РОЗДІЛУ 6

Використання програмно-конфігурованих мереж має серйозні економічні наслідки, і з них витікає широкий спектр як позитивних, так і негативних впливів програмно-конфігурованих мереж на навколишнє середовище. Загалом другорядний вплив на проектування та роботу продуктів і послуг є позитивним для навколишнього середовища. Однак існує велика невизначеність щодо додаткового впливу на споживчу поведінку, сукупний попит і структуру економічного зростання (чи є зростання суттєво дематеріалізованим). Здається дуже вірогідним, хоча неможливо підтвердити, що буде невідповідність між можливостями підвищення екологічної ефективності на мікрорівні та використанням ресурсів і впливом на навколишнє середовище в сукупності. Багато ефектів заміщення мають обмежене екологічне значення, лише часткові, або можуть стимулювати нові форми споживання, що породжує нові екологічні навантаження. Існує навіть можливість того, що можна було б назвати процесом «рематеріалізації» Нової економіки, оскільки ціни на сировину падають, а споживачі все більше віддаляються від екологічних наслідків свого споживання.

Зв’язок між ПКМ та навколишнім середовищем є дуже позитивістським, що визначає можливості та спирається на докази конкретних випадків. Зараз з’являється більш систематичний аналіз повної складності зв’язку, але доказова база, на основі якої можна зробити висновки, все ще слабка. Інша проблема полягає в тому, що більшість досліджень «орієнтовані на майбутнє», спекулюють про наслідки технологічних і ринкових змін, які ще не відбулися і які все ще є дуже невизначеними.

Методи оцінки впливу включають якісні рахунки, дуже спрощене концептуальне моделювання можливих переваг (якщо А замінити на Б, це призведе до заощаджень на В). Загалом вони не в змозі впоратися з ефектами зворотного зв’язку через реакцію ринкового попиту та поведінку споживачів.

Існує потреба у значно кращому моніторингу та оцінці зв’язків між підвищенням продуктивності (праці, капіталу та навколишнього середовища), що спричинене ПКМ, і фактичними екологічними показниками промислово розвинутих

економік. ОЕСР могла б відіграти важливу роль у створенні основи для моніторингу та аналізу цих змін, надаючи вкрай необхідні емпіричні докази та надаючи міжнародну перспективу.

ВИСНОВКИ

Дане дослідження стосується основних проблем затримки між контролерами та вибору контролерів. Існуючі мережі включають затримку між контролерами для перемикання, тоді як інші мережі включають затримку між контролерами. Однак вони обмежені високою затримкою, оскільки контролер не був розміщений у точному місці. Існуючий евристичний алгоритм також не має проблем з конвергенцією, що також впливає на розміщення контролера. Вибір контролерів перед розгортанням викликає серйозне занепокоєння, однак у більшості мереж вибір контролера не розглядається, що також призводить до зниження продуктивності мережі в ПКМ.

Враховуючи, вищезазначені проблемами в існуючих мережах, це дослідження пропонує забезпечити ефективне вирішення проблеми. Основна мета цього дослідження полягає в тому, щоб полегшити проблеми з розміщенням контролера в середовищі з декількома контролерами. Для досягнення цієї мети було поставлено такі задачі:

• Поліпшити масштабованість мережі шляхом побудови мережі як графової структури;

• Підвищити продуктивність мережі шляхом вибору оптимального контролера з високою відмовостійкістю за допомогою алгоритму оптимізації;

• Для мінімізації затримки розповсюдження між міжконтролерами та комутаторами за допомогою гібридних метаевристичних алгоритмів.

Запропонований підхід МК-ПКМ (Програмно-конфігурована мережа на основі кількох контролерів) вирішує проблему розміщення контролера для покращення продуктивності мережі в середовищі ПКМ. Мережа побудована у вигляді графа для підвищення масштабованості, зв’язності та гнучкості мережі, що підвищує ефективність зв’язку та зменшує затримку поширення зв’язку. Таким чином, основні внески цього дослідження визначаються наступним чином:

• По-перше, оптимальний контролер вибирається з кількох контролерів за допомогою алгоритму оптимізації Firefly, який покращує продуктивність мережі шляхом вибору оптимального контролера для керування мережею;

• По-друге, розміщення кількох контролерів виконується за допомогою гібридного алгоритму гармонійного пошуку та алгоритму оптимізації рою частинок, що зменшує затримку зв'язку між комутатором і контролером шляхом вибору оптимального місця для розміщення контролера.

Продуктивність запропонованої роботи оцінюється на основі кількох показників продуктивності, таких як затримка розповсюдження, час проходження в обидві сторони, матриця часу сеансу, затримка, надійність, пропускна здатність, вартість і значення придатності.

У даній роботі наведено попередні знання про гібридний метаевристичний алгоритм, який називається алгоритмом гармонійного пошуку і алгоритмом оптимізації рою частинок , щоб забезпечити краще розуміння запропонованої роботи.

Також у цій кваліфікаційній роботі наголошується на обговоренні ефективності запропонованого підходу МК-ПКМ. Загальний метод пропонується для усунення існуючих проблем у розміщенні ПКМ контролера. Побудова мережі як графічної структури підтримує масштабованість мережі та покращує пропускну здатність. Загальна продуктивність мережі підвищується шляхом вибору оптимального контролера з урахуванням різних функцій контролера, які використовують алгоритм оптимізації. Вибрані оптимальні контролери розподіляються та розміщуються в оптимальному місці за допомогою гібридного метаевристичного алгоритму, який враховує затримку між контролерами та затримку між контролерами та комутаторами відповідно.

Дані алгоритми застосовуються для ефективного розгортання кількох контролерів, щоб зменшити затримку зв'язку та розповсюдження та підвищити пропускну здатність і надійність. Побудова мережі виконується для покращення масштабованості та з'єднання між комутаторами та контролерами. Після цього вибирається оптимальний контролер на основі характеристик за допомогою алгоритму оптимізації, що покращує продуктивність мережі в середовищі ПКМ.

Нарешті, кілька контролерів розміщуються на основі вибраного контролера за допомогою гібридного метаевристичного алгоритму, який збільшує швидкість конвергенції, що зменшує затримку розгортання та затримку зв’язку в середовищі. Моделювання виконується інструментом моделювання CloudsimПКМ, і результати моделювання показують, що запропонований підхід МК-ПКМ досяг кращої продуктивності при розміщенні кількох контролерів порівняно з іншими сучасними розробками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. F. Hu, "Network Innovation through OpenFlow and SDN: Principles and Design", CRC Press, (2014). [Електронний ресурс] – Режим доступу до ресурсу: http://dx.doi.org/10.1201/b16521.
2. A. Al-Shabibi. Programmable virtual networks: From network slicing to network virtualization, July 2013. [Електронний ресурс] – Режим доступу до ресурсу: http://www. slideshare.net/nvirters/virt-july2013meetup
3. EU Future Internet Research and Experimentation Initiative. [Електронний ресурс] – Режим доступу до ресурсу: http://www.ict-fire.eu/.
4. M. Caesar, N. Feamster, J. Rexford, A. Shaikh, and J. van der Merwe. Design and implementation of a routing control platform. In *Proc. 2nd USENIX NSDI*, Boston, MA, May 2005.
5. NSF Future Internet Design. [Електронний ресурс] – Режим доступу до ресурсу: http://www.nets-find.net/.
6. OpenFlow Switch Consortium, "OpenFlow Switch Specification Version 1.0. 0.", (2009) [Електронний ресурс] – Режим доступу до ресурсу: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.0.0.pdf.
7. SDN Revolution Started It All [Електронний ресурс] – Режим доступу до ресурсу: https://opennetworking.org/sdn-definition/
8. Сетевая технология OpenFlow (SDN) / Семенов Ю.А. – ИТЭФ-МФТИ, 2014.
9. Open Networking Foundation. [Електронний ресурс] – Режим доступу до ресурсу: https://www.opennetworking.org/.
10. OpenFlow Tutorial [Електронний ресурс] – Режим доступу до ресурсу: http://archive.openflow.org/wk/index.php/OpenFlow_Tutorial.
11. L. Yang, R. Dantu, T. Anderson, and R. Gopal. *Forwarding and Control Element Separation (ForCES) Framework*. Internet Engineering Task Force, Apr. 2004. RFC 3746.

12. D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, Firstquarter 2017.
13. Rosle, M.S.; Mohamad, M.S.; Choon, Y.W.; Ibrahim, Z.; González-Briones, A.; Chamoso, P.; Corchado, J.M. A Hybrid of Particle Swarm Optimization and Harmony Search to Estimate Kinetic Parameters in Arabidopsis thaliana. *Processes* 2020, *8*, 921.
14. Bala, N.M.; bin Safei, S. A Hybrid Harmony Search and Particle Swarm Optimization Algorithm (HSPSO) for Testing Nonfunctional Properties in Software System. *Stat. Optim. Inf. Comput. (SOIC)* 2021, *10*, 3.
15. Torkamani-Azar, S.; Jahanshahi, M. A new GSO based method for SDN controller placement. *Comput. Commun.* 2020, *163*, 91–108.
16. Ramya, G.; Manoharan, R. Enhanced optimal placements of multi-controllers in SDN. *J. Ambient. Intell. Humaniz. Comput.* 2021, *12*, 8187–8204.
17. G. Weikum and G. Vossen, Transactional Information Systems: Theory,Algorithms, and the Practice of Concurrency Control and Recovery.San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2001.
18. Aravind, P.; Varma, G.S.; Reddy, P.P. Simulated annealing based optimal controller placement in software defined networks with capacity constraint and failure awareness. *J. King Saud Univ. Comput. Inf. Sci.* 2021.