МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 15.00.00.000 ПЗ

Група ІПм-24-1

Груб`як Віталій

2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Груб`як Віталій Ярославович

(прізвище, ім'я, по батькові)

УДК 004.9

(індекс)

МАГІСТЕРСЬКА РОБОТА

Порівняльний аналіз транспортних рівнів мобільних протоколів

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Груб`як В.Я.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Піх Володимир Ярославович, к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Івано-Франківськ – 2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**

доц. В.В. Бандура

“ 04 ” вересня 2025 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Груб`яку Віталію Ярославовичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ Порівняльний аналіз транспортних рівнів мобільних протоколів”

керівник проекту (роботи) Піх В.Я., к.т.н., доцент

затверджені наказом закладу вищої освіти від “ 05 ” листопада 2025 р. № 695/7

2. Строк подання студентом проекту (роботи) 15 грудня 2025 р.

3. Вихідні дані до проекту (роботи) Теоретичні концепції та формальні моделі побудови та функціонування інформаційних технологій мобільних протоколів

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1. Аналіз предметної області дослідження протоколів мобільності
2. Дослідження та опис протоколів мобільності транспортного рівня
3. Методи та архітектури управління мобільністю протоколів на транспортному рівні
4. Представлення таксономії архітектур мобільності на транспортному рівні

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Комплексна схема управління мобільністю (рис. 1.1)
2. SIGMA архітектура (рис. 1.2)
3. Реалізація стека протоколу M-TCP (рис. 1.3)
4. Схема роботи протоколу Freeze-TCP (рис. 1.4)
5. Структурні блоки RCP (рис. 1.5)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2025 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	14.09.2025	виконано
2	Аналіз предметної області дослідження протоколів мобільності	29.09.2025	виконано
3	Дослідження та опис протоколів мобільності транспортного рівня	15.10.2025	виконано
4	Методи та архітектури управління мобільністю протоколів на транспортному рівні	08.11.2025	виконано
5	Представлення таксономії архітектур мобільності на транспортному рівні	19.11.2025	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	14.12.2025	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 79 с., 29 рис., 3 табл., 39 джерел.

Тема: Порівняльний аналіз транспортних рівнів мобільних протоколів

Мета магістерської роботи - проведення порівняльного аналізу транспортних протоколів мобільності, визначення їх архітектурних особливостей, переваг і недоліків, а також формування узагальненої класифікації підходів.

Об'єкт дослідження - процеси управління мобільністю в мережах, орієнтовані на забезпечення безперервності з'єднань у середовищах із динамічно змінною топологією.

Предмет дослідження - архітектури, протоколи та методи управління мобільністю на транспортному рівні.

Результати дослідження

В роботі запропоновано узагальнену таксономію архітектур мобільності транспортного рівня, яка класифікує протоколи за принципами організації управління з'єднаннями.

Висновок

Виконано вдосконалення підходів до порівняльної оцінки транспортних протоколів мобільності з урахуванням критеріїв адаптивності, прозорості, надійності та ресурсної ефективності.

МОБІЛЬНІСТЬ, ТРАНСПОРТНИЙ РІВЕНЬ, ПРОТОКОЛИ МОБІЛЬНОСТІ, УПРАВЛІННЯ З'ЄДНАННЯМИ, ГЕТЕРОГЕННІ МЕРЕЖІ, БЕЗШОВНА ПЕРЕДАЧА, АДАПТИВНІСТЬ, МАСШТАБОВАНІСТЬ.

ABSTRACT

Master Thesis: 79 pp., 29 fig., 3 tab., 39 sources.

Thesis Subject: Development and adaptation of template models of cloud solutions and services

Object of research: information problems of recognition of classes of complex objects with the use of artificial neural networks.

Research goal: research of architecture and methods of using intelligent image recognition system using neuroclassifications.

Subject of research: models and methods of artificial neural networks for solving recognition problems.

The results

The paper describes the structures and methods of learning artificial neural networks with competitive learning to solve problems of recognition of complex objects.

Conclusion

The models of the three-dimensional map of features which allows to carry out visualization of results of recognition and identification of objects in three-dimensional space are investigated.

CLOUD SERVICES, CLOUD SOFTWARE, DESIGN PATTERNS, MODEL, MICROSERVICE, CLOUD ARCHITECTURE, SCALING, INFRASTRUCTURE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACK - Acknowledgement

MH - Mobile host

M-TCP - Migrate TCP

MMSP - Mobile Multimedia Streaming Protocol

SCTP - Stream Control Transmission Protocol

ZWA - Zero Window Advertisement

ZWP - Zero Window Probes

M-UDP - Mobile UDP

mSCTP - Mobile SCTP

RCP - Receiption Control Protocol

BARWAN - Bay Area Research Wireless Access Network

BS - Base Station

CN - corresponding node

CWND - Congestion Window

ВСТУП

Актуальність теми.

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням мобільності користувачів, різноманіттям пристроїв доступу та розширенням масштабів використання гетерогенних мереж. Підвищення вимог до швидкості, надійності та безперервності з'єднань у мобільних середовищах створює потребу в удосконаленні механізмів управління мобільністю на різних рівнях мережевої моделі OSI. Традиційні рішення, що реалізують мобільність на мережевому рівні (зокрема Mobile IP), мають низку обмежень, пов'язаних із затримками під час передачі обслуговування (handover), високими вимогами до маршрутизації та відсутністю прозорості для застосунків.

У цьому контексті актуальності набувають протоколи мобільності транспортного рівня, здатні забезпечити адаптивне управління з'єднаннями, збереження стану сеансів і підвищення ефективності передачі даних у динамічних умовах зміни мережевої топології. Такі протоколи, як MSOCKS, SIGMA, RCP, R²CP, M-TCP та Freeze-TCP, демонструють потенціал до реалізації безшовної мобільності та гнучкого контролю перевантаження без суттєвих змін у мережевій інфраструктурі.

Магістерська робота спрямована на системний аналіз, класифікацію та порівняльну оцінку транспортних протоколів мобільності з метою визначення їх ефективності, переваг, обмежень та перспектив використання в умовах мереж нового покоління (5G/6G). Результати дослідження можуть бути використані для подальшого розвитку технологій передачі даних, проектування мобільних архітектур і вдосконалення засобів управління з'єднаннями у гетерогенних мережах.

Зростання популярності мобільних пристроїв, розвиток бездротових технологій і поширення сервісів, що потребують стабільного мережевого з'єднання (відеоконференції, потокове мовлення, хмарні застосунки),

формують нові вимоги до інфраструктури зв’язку. Забезпечення безперервності обслуговування при зміні точки доступу є критично важливим для якості користувацького досвіду та ефективного функціонування розподілених систем.

Однак існуючі рішення, реалізовані на мережевому рівні, не завжди відповідають цим вимогам через централізованість управління, високу складність реалізації та залежність від специфіки мережевих протоколів. Транспортний рівень, на відміну від мережевого, має більший потенціал адаптації завдяки своїй близькості до прикладного шару, можливості контролю параметрів з’єднання та збереження стану сеансу навіть за зміни IP-адреси.

Дослідження транспортних протоколів мобільності є актуальним завданням сучасної інформатики, оскільки воно дозволяє забезпечити узгодження мобільності, надійності та ефективності в рамках наскрізної взаємодії. Особливе значення це має для мобільних і мультиінтерфейсних середовищ нового покоління, де інтеграція міжмережевих технологій і високошвидкісних з’єднань вимагає гнучких транспортних рішень.

Метою магістерської роботи є проведення порівняльного аналізу транспортних протоколів мобільності, визначення їх архітектурних особливостей, переваг і недоліків, а також формування узагальненої класифікації підходів.

Об’єктом дослідження є процеси управління мобільністю в мережах, орієнтовані на забезпечення безперервності з’єднань у середовищах із динамічно змінною топологією.

Предметом дослідження є архітектури, протоколи та методи управління мобільністю на транспортному рівні.

Для досягнення поставленої мети в роботі вирішено такі завдання:

1. Провести аналіз предметної області управління мобільністю та класифікувати протоколи за рівнями моделі OSI.

2. Визначити ключові критерії ефективності транспортних протоколів мобільності.

3. Дослідити архітектуру, принципи функціонування та характеристики протоколів.

4. Виконати порівняльний аналіз механізмів управління мобільністю та критеріїв їх оптимізації.

5. Сформувати таксономію архітектур транспортного рівня за ознаками структурної організації та функціональних властивостей.

У роботі **використано сукупність теоретичних і аналітичних методів**, серед яких: метод системного аналізу, метод порівняльного аналізу, структурно-функціональний аналіз, метод експертного узагальнення.

Наукова новизна отриманих результатів

Проведено комплексний порівняльний аналіз сучасних транспортних протоколів мобільності з урахуванням параметрів адаптивності, масштабованості, прозорості та надійності.

Практичне застосування результатів

Отримані результати можуть бути використані при проектуванні та оптимізації транспортних протоколів у мобільних мережах, у процесі розроблення рішень для безшовного handover у мультимережевих середовищах та при моделюванні систем управління з’єднаннями для мобільних застосунків і хмарних сервісів;

Структура магістерської роботи. Робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 79 сторіноку і містить 29 рисунків, 3 таблиці, список використаних джерел із 39 найменуваннями.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ ПРОТОКОЛІВ МОБІЛЬНОСТІ

1.1. Актуальність дослідження протоколів мобільності на транспортному рівні

Мобільність інтернет-хостів (вузлів) є фундаментальною особливістю сучасних мережевих архітектур, дозволяючи обчислювальним вузлам змінювати своє розташування, переміщуючись між різними підмережами. З метою забезпечення безперебійного зв'язку для мобільних користувачів було розроблено низку протоколів мобільності, які функціонують на різних рівнях мережевої моделі.

Протокол Mobile IP був започаткований для реалізації механізмів управління мобільністю інтернет-хостів на мережевому рівні (рівень 3). Однак, мобільність на транспортному рівні (рівень 4) потенційно здатна нівелювати значну частину обмежень, властивих схемам мережевого рівня. З огляду на це, було запропоновано та досліджено різноманітні підходи щодо впровадження мобільності саме на транспортному рівні.

1.1.1. Класифікація протоколів

У межах цієї роботи ми здійснюємо аналітичний огляд низки існуючих протоколів мобільності транспортного рівня. Протоколи класифікуються відповідно до їхньої базової концептуальної моделі та порівнюються на основі комплексу критеріїв оцінки.

Комплексна схема управління мобільністю зазвичай інтегрує такі ключові компоненти:

- Передача обслуговування (Handover)
- Міграція з'єднання (Connection Migration)
- Управління розташуванням (Location Management)

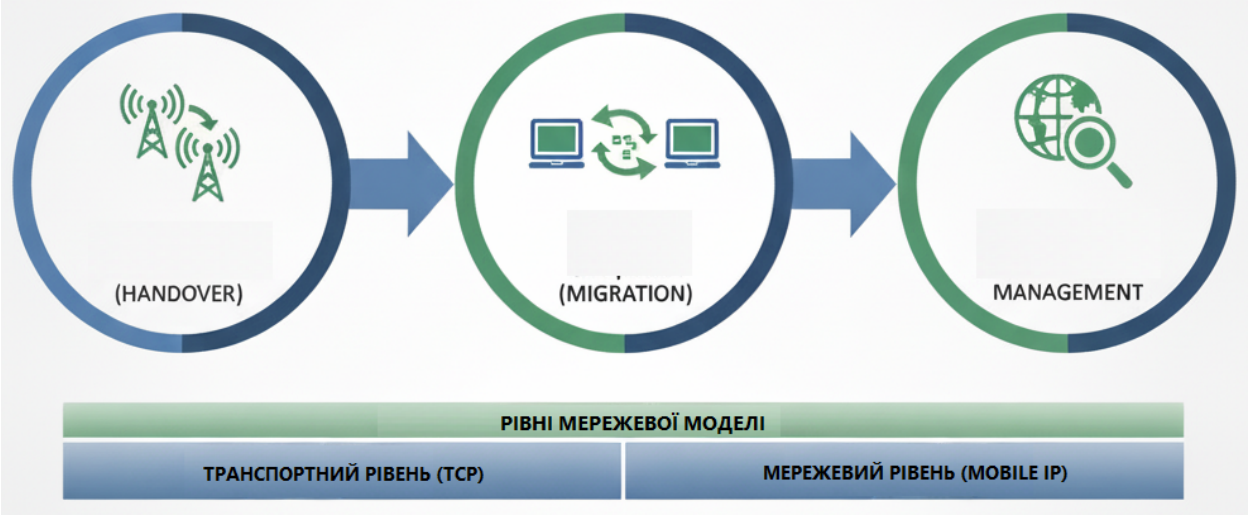

Рис. 1.1. Комплексна схема управління мобільністю

1.1.2. Критерії оцінки схем мобільності

Для об'єктивного визначення та порівняння ефективності схем мобільності було розроблено відповідні критерії оцінки. До цих критеріїв належать, але не обмежуються ними, наступні показники:

- Продуктивність передачі обслуговування (затримка та успішність)
- Втрата пакетів та затримка (під час міграції)
- Стійкість до збоїв
- Вимоги до модифікації мережевої інфраструктури
- Тип підтримуваної мобільності
- Підтримка різноманітності IP-адрес (IP Diversity)
- Безпека
- Масштабованість

У подальших розділах цієї роботи вищезазначені критерії використовуються як методологічна основа для класифікації та критичного аналізу запропонованих схем мобільності.

Архітектура Інтернету ґрунтується на п'ятирівневій моделі (фізичний, канальний, мережевий, транспортний рівні та рівень застосунків), кожен з яких має чітко визначені функціональні обов'язки. Оскільки механізми мобільності можуть бути реалізовані на різних рівнях стеку протоколів, виникає фундаментальне дослідницьке питання щодо визначення

оптимального рівня для ефективного управління мобільністю. Було проведено низку досліджень, спрямованих на оцінку переваг та недоліків управління мобільністю на різних рівнях, зокрема на мережевому та транспортному, які є найбільш широко досліджуваними.

Встановлено, що реалізація мобільності на транспортному рівні здатна ефективно долати значні обмеження, притаманні схемам мережевого рівня, таким як Mobile IP.

1.2 Огляд сучасних викликів та архітектур

1.2.1 Потреба в багатоінтерфейсній мобільності

Мобільні вузли майбутнього покоління будуть оснащені множинними мережевими інтерфейсами для залучення переваг оверлейних мереж. Однак, більшість існуючих систем мобільності не забезпечують повної підтримки для одночасного використання цих інтерфейсів. Потреба в такій підтримці виникає в умовах наявності декількох варіантів підключення, що характеризуються різними параметрами, як-от: вартість, покриття, затримка та пропускна здатність. Це дозволяє застосункам динамічно обирати інтерфейс, який найкраще відповідає вимогам до передачі конкретного типу даних.

У цій роботі пропонується архітектура мобільності транспортного рівня, яка надає мобільним вузлам (МВ) можливість не лише змінювати точку підключення до мережі Інтернет, але й здійснювати деталізований контроль над тим, які мережеві інтерфейси використовуються для різних потоків вхідних і вихідних даних.

1.2.2 Основи управління мобільністю

Інтернет початково проектувався для статичних хостів у дротових мережах. Широке розповсюдження бездротових технологій спричинило зростання попиту на мобільність хостів, що стимулювало розробку

різноманітних схем управління мобільністю. Управління мобільністю охоплює дві основні операції:

- Передача обслуговування (Handover) - процес зміни точки підключення мобільним пристроєм при збереженні активної комунікації з вузлом-партнером.

- Управління розташуванням (Location Management) - завдання визначення (отримання IP-адреси) поточного розташування мобільного хоста (MH) для ініціювання та встановлення з'єднання. Ефективна схема управління розташуванням повинна надавати коректну адресу MH і бути прозорою для вузлів-партнерів.

1.2.3 Протоколи мобільності транспортного рівня

Існує велика кількість протоколів мобільності транспортного рівня, що базуються на різних критеріях та підходах. На відміну від Mobile IP, який є схемою мережевого рівня, що забезпечує прозорість мобільності для вищих рівнів, збільшуючи при цьому навантаження на інтернет-інфраструктуру, схеми транспортного рівня використовують наскрізний (end-to-end) підхід. Цей підхід мінімізує необхідність модифікації базової інтернет-інфраструктури, перекладаючи відповідальність за управління мобільністю на кінцеві хости.

Приклади протоколів мобільності транспортного рівня включають: MSOCKS, SIGMA, RCP, Freeze-TCP, R²CP, MMSP, I-TCP, M-TCP, M-UDP, BARWAN, TCP-R, mSCTP та інші.

1.2.4 Критерії порівняльного аналізу

Повноцінна схема управління мобільністю ґрунтується на трьох основних принципах: передача обслуговування, міграція з'єднання та управління розташуванням. Для об'єктивного оцінювання та порівняння ефективності різних схем мобільності необхідна розробка чітких критеріїв оцінки.

1.3. Дослідження механізмів управління мобільністю в IP-мережах на транспортному рівні

1.3.1. Виклик мобільності та розділення ідентичності/розташування

Масове поширення мобільних обчислювальних платформ (ноутбуки, смартфони, КПК) зі стійким підключенням до мережі Інтернет стимулювало інтенсивні дослідження у сфері підтримки мобільності в IP-мережах. Сучасні мобільні термінали (МТ) функціонують як повноцінні кінцеві системи, проте їхня природа суперечить фундаментальним припущенням, на яких базується протокол IP: традиційна кінцева система є статичною і має єдину точку підключення. У такій класичній моделі єдиний ідентифікатор – IP-адреса – репрезентує як ідентичність терміналу, так і його мережеве розташування.

Для мобільних мереж такий підхід є неадекватним. З одного боку, необхідний постійний ідентифікатор для розрізнення терміналів; з іншого — необхідна інформація про поточне розташування для забезпечення коректної маршрутизації пакетів. Таким чином, ключова проблема мобільності в IP-мережах полягає у відокремленні ідентичності від розташування.

1.3.2. Еволюція управління мобільністю та підхід транспортного рівня

Традиційно проблема мобільності вирішувалася на мережевому рівні (наприклад, Mobile IP). Однак, сучасні підходи зосереджені на реалізації мобільності на транспортному рівні за допомогою наскрізної (end-to-end) концепції. Реалізація цієї концепції вимагає модифікації існуючих протоколів транспортного рівня.

Хоча протокол TCP є найбільш поширеним в Інтернеті і був модифікований для підтримки наскрізної мобільності, його архітектура не завжди є ідеальною платформою для нетрадиційних механізмів підтримки мобільності. Мережева архітектура Інтернету, що складається з п'яти рівнів, передбачає специфічні обов'язки для кожного рівня. Для досягнення

ефективного управління мобільністю на транспортному рівні необхідно вирішити низку критичних питань, зокрема:

- Втрата пакетів та затримка
- Контроль перевантаження
- Міграція з'єднання
- Вимоги до інфраструктури
- Управління розташуванням

1.3.3. Порівняльний аналіз схем управління мобільністю на транспортному рівні

В рамках цього дослідження проводиться порівняльний аналіз шести ключових протоколів мобільності транспортного рівня: MSOCKS, SIGMA, Migrate TCP (M-TCP), Freeze-TCP, RCP та R²CP. Порівняння ґрунтується на таких важливих критеріях, як процес передачі обслуговування, прозорість для верхніх рівнів, втрата/затримка пакетів, масштабованість, стійкість до збоїв, безпека, підтримка різноманітності шляхів та необхідність зміни інфраструктури.

Таблиця 1.1.

Ключові протоколи та механізми

Протокол	Ключовий механізм мобільності	Управління розташуванням	IP-різноманітність	Зміна інфраструктури
MSOCKS	TCP Splice, Проксі, Декілька IP-адрес	Не вказано	Підтримується	Не вимагається (кінцеві вузли)
SIGMA	М'яка передача (Область перекриття), Оновлення DNS	DNS-оновлення	Підтримується	Не вимагається (кінцеві вузли)
Migrate TCP	Міграція з'єднання (Token), жорстка передача	DNS-оновлення	Не вказано	Не вимагається
Freeze-TCP	Заморожування з'єднання (нульове вікно)	Не вказано	Не підтримується	Зміни лише на мобільному клієнті
RCP	Орієнтований на отримувача (REQ-DATA handshake)	Не вказано	Не вказано	Не вказано
R²CP	Орієнтований на отримувача, м'яка передача, агрегація смуги	Може бути інтегровано	Підтримується	Не вказано

Проведемо детальний огляд обраних протоколів.

MSOCKS використовує TCP Splice для міграції з'єднання та підтримує множинні IP-адреси через проксі-механізм. Дозволяє MT вибирати мережевий інтерфейс для даних, зберігаючи надійність TCP без відома вузла-партнера (CN). SIGMA (Seamless IP Diversity Mobile Architecture) - комплексна схема, що підтримує безперебійну IP-різноманітність. Використовує механізм м'якої передачі в області перекриття підмереж, з подальшим оновленням DNS-запису для управління розташуванням. Значущість полягає в контролі високої затримки та втрати пакетів.

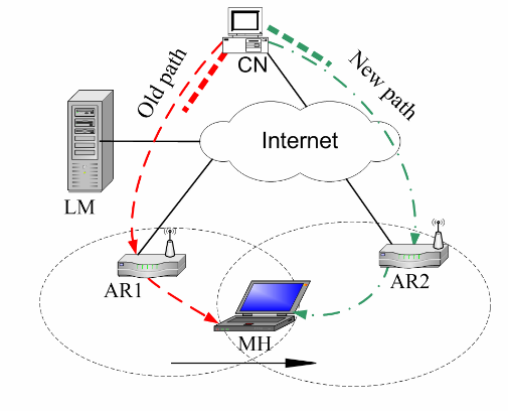

Рис. 1.2. SIGMA архітектура

Migrate TCP (M-TCP) - прозора схема, що базується на міграції з'єднання за допомогою токена. Використовує DNS для управління розташуванням. Спрямована на забезпечення безперервності обслуговування для довготривалих сесій.

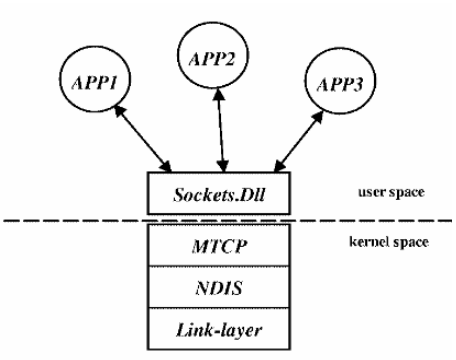

Рис. 1.3. Реалізація стека протоколу M-TCP

Freeze-TCP реалізує справжній наскрізний підхід, не вимагаючи участі посередників. Дозволяє MT призупиняти (заморожувати) TCP-з'єднання під час передачі обслуговування, оголошуючи нульовий розмір вікна CN, що зменшує втрату пакетів ціною збільшення затримки. Вимагає змін лише на стороні мобільного клієнта.

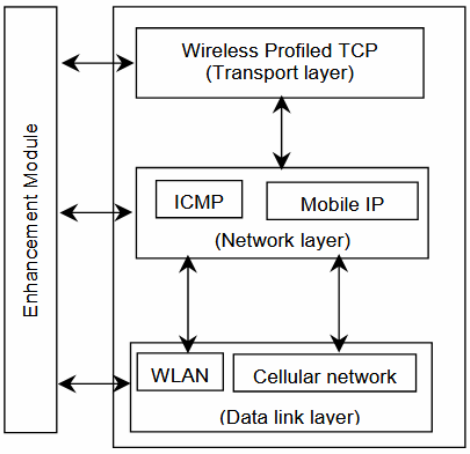

Рис. 1.4. Схема роботи протоколу Freeze-TCP

RCP (Reception Control Protocol) - протокол, орієнтований на отримувача (MH), що забезпечує кращий контроль перевантаження та відновлення втрат порівняно з TCP. Використовує REQ-DATA квитування, де отримувач контролює передачу даних. Структурні блоки RCP представлені на рисунку 1.5.

R²CP (Radial Reception Control Protocol) - розширення RCP, яке перекладає відповідальність за контроль перевантаження на отримувача. Підтримує гетерогенні бездротові з'єднання, IP-різноманітність та м'яку передачу обслуговування, дозволяючи агрегацію пропускної здатності через декілька інтерфейсів.

Наведемо короткий опис інших схем мобільності.

I-TCP (Indirect TCP) - схема, що вимагає шлюзу для розділення зв'язку: TCP-з'єднання між CN і шлюзом та I-TCP-з'єднання між шлюзом і MH. Шлюз забезпечує мобільність, ізолюючи CN від змін.

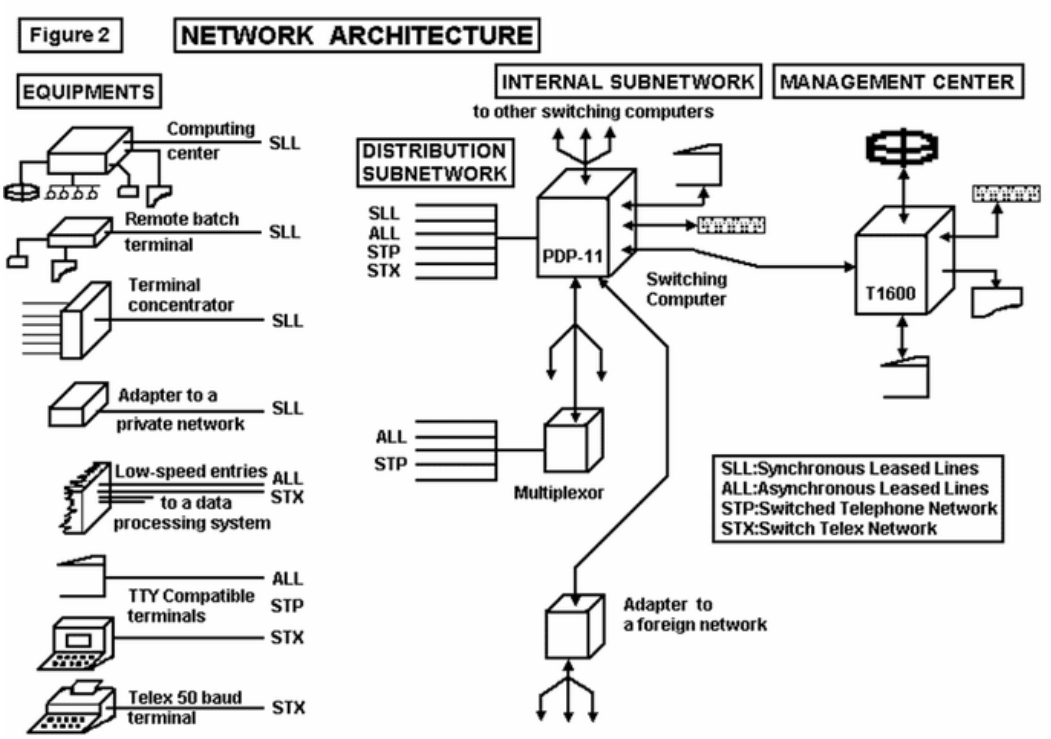

Рис. 1.5. Структурні блоки RCP

mSCTP (Mobile SCTP) - протокол, що підтримує IP-різноманітність та м'яку передачу обслуговування, подібну до SIGMA, але не включає управління розташуванням.

M-UDP (Mobile UDP) - реалізація UDP, що підтримує мобільність через шлюз (подібно до I-TCP/M-TCP), але не підтримує IP-різноманітність або управління розташуванням.

BARWAN (Bay Area Research Wireless Access Network) - рішення для гетерогенних оверлейних мереж, орієнтоване на шлюз. Вимагає обізнаності застосунку про мобільність, оскільки рішення про передачу обслуговування приймається на рівні застосунку.

Хоча традиційні схеми мобільності, такі як Mobile IP, працюють на мережевому рівні, підхід наскрізної мобільності на транспортному рівні пропонує більш гнучкі та менш інвазивні рішення. Проаналізовані протоколи демонструють різні стратегії вирішення фундаментальної проблеми розділення ідентичності та розташування, пропонуючи компроміси між прозорістю, затримкою/втратою пакетів та вимогами до інфраструктури.

Висновки до розділу

У першому розділі проведено теоретичний аналіз предметної області управління мобільністю в комп’ютерних мережах, що дозволило визначити основні підходи та тенденції у розвитку протоколів транспортного рівня. Здійснено класифікацію існуючих протоколів і визначено ключові критерії оцінки їх ефективності, серед яких – прозорість для застосунків, затримка передачі, масштабованість і безпека. Встановлено, що традиційні рішення, орієнтовані на мережевий рівень, не завжди забезпечують необхідну продуктивність у гетерогенних середовищах. Показано, що саме транспортний рівень здатний гнучко адаптуватися до змін у топології мережі та стану з’єднання.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТА ОПИС ПРОТОКОЛІВ МОБІЛЬНОСТІ ТРАНСПОРТНОГО РІВНЯ

У цьому розділі здійснюється обговорення та детальний аналіз шести ключових протоколів управління мобільністю, що функціонують на транспортному рівні: MSOCKS, SIGMA, RCP, R²CP, Freeze TCP та Migrate TCP. Основна увага буде зосереджена на архітектурі, механізмах та продуктивності протоколу MSOCKS.

2.1. Аналіз протоколу MSOCKS

Протокол MSOCKS реалізується за допомогою архітектури, що включає проміжний вузол — проксі-сервер, який інтегровано у шлях комунікації між мобільним вузлом (МВ) та вузлом-партнером (ВР, або кореспондентський хост).

2.1.1. Функціонал проксі MSOCKS

Для кожного потоку даних від МВ до ВП, проксі підтримує стабільний потік даних до ВП, ефективно ізолюючи ВП від будь-яких варіацій, пов'язаних з мобільністю. Паралельно, проксі може динамічно встановлювати та розривати з'єднання з МВ, що є необхідним для міграції потоків даних між різними мережевими інтерфейсами або підмережами.

Проксі-сервер виступає посередником у зв'язку "сервер-клієнт" і може надавати додаткові послуги від імені будь-якої зі сторін:

- Надання обчислювальних ресурсів, яких бракує клієнту.

- Переформатування інформації від сервера для відповідності МВ (наприклад, оптимізація зображень GIF для малих екранів).

- Застосування стиснення даних для зменшення вимог до пропускної здатності на ділянці між МВ та проксі, яка часто є низькоякісним бездротовим з'єднанням.

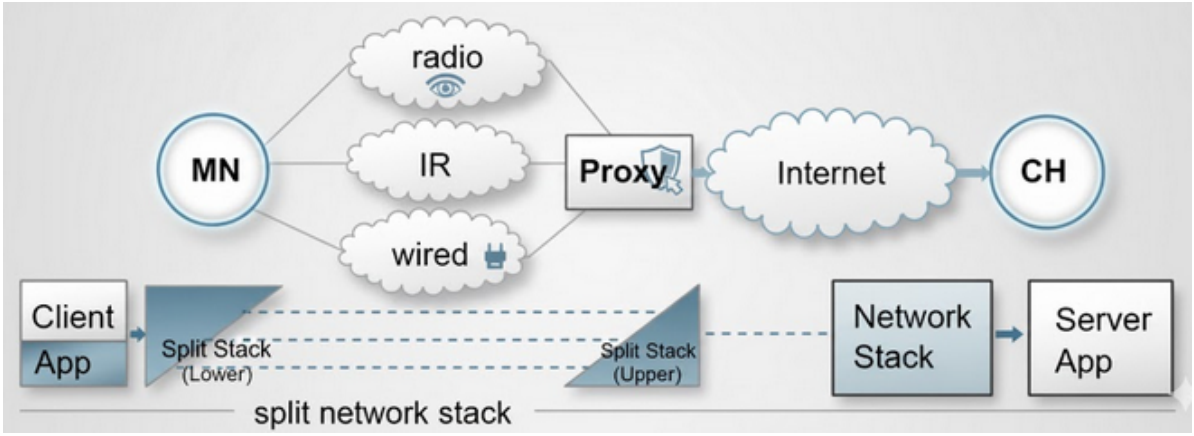

Рис. 2.1. Типова мережева топологія, що ілюструє розташування проксі між мобільним вузлом та вузлом-партнером

Таким чином, MSOCKS являє собою гнучку систему, що забезпечує безперервність з'єднання МВ при зміні його точки підключення.

2.1.2. Архітектура MSOCKS

Архітектура MSOCKS базується на ключовій технології, відомій як TCP Splice.

TCP Splice — це механізм, який дозволяє вузлу, де термінуються два незалежні TCP-з'єднання, логічно об'єднати ці два з'єднання. Це створює одне ефективне наскрізне TCP-з'єднання між кінцевими точками двох оригінальних з'єднань.

Архітектура MSOCKS складається з трьох основних компонентів:

1. Процес проксі MSOCKS - працює на машині проксі на рівні користувача.

2. Модифікації ядра (Kernel Modification) - внесені в ядро машини проксі для забезпечення функціональності TCP Splice.

3. Бібліотека MSOCKS - функціонує під рівнем застосунку на мобільному вузлі.

Схема на рисунку 2.2 демонструє, як MSOCKS Proxy створює два сегменти наскрізного шляху:

- Статичний сегмент (внизу) - між вузлом-партнером та проксі-сервером. Це з'єднання є постійним, забезпечуючи необізнаність Вузла-Партнера про мобільність.

- Мобільний сегмент (зліва) - між мобільним вузлом та проксі-сервером. Це з'єднання може змінюватися (розриватися та відновлюватися з новою IP-адресою), дозволяючи мобільному вузлу переміщатися між підмережами.

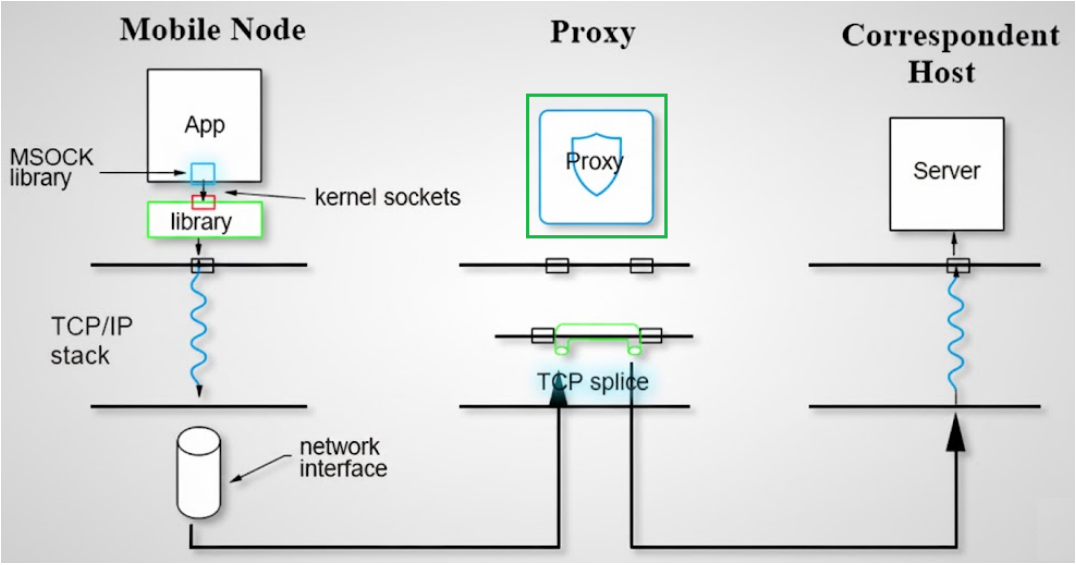

Рис. 2.2. Частини, позначені зеленим кольором, ілюструють зміни, внесені MSOCKS до стандартних компонентів клієнт-серверної системи на основі проксі

Завдяки TCP Splice, дані прозоро передаються між цими двома сегментами, забезпечуючи безперервність сесії.

2.1.3. Протокол MSOCKS

Процес встановлення з'єднання починається з перехоплення бібліотекою MSOCKS виклику connect() застосунку та його трансформації у виклик Mconnect().

1. З'єднання МВ-Проксі: Mconnect ініціює стандартне TCP-з'єднання від МВ до проксі, використовуючи відповідну IP-адресу.

2. Передача інформації: через це з'єднання бібліотека надсилає проксі адресу та порт ВП, а також необхідну аутентифікаційну інформацію.

3. З'єднання Проксі-ВП: Після аутентифікації МВ, проксі встановлює з'єднання з бажаним ВП.

4. Сплайсинг та Синхронізація: Проксі об'єднує з'єднання МВ-Проксі та Проксі-ВП за допомогою TCP Splice. Після успішного налаштування проксі надсилає МВ остаточне повідомлення OK, яке містить ідентифікатор з'єднання. Цей ідентифікатор є ключовим для подальшого повторного підключення.

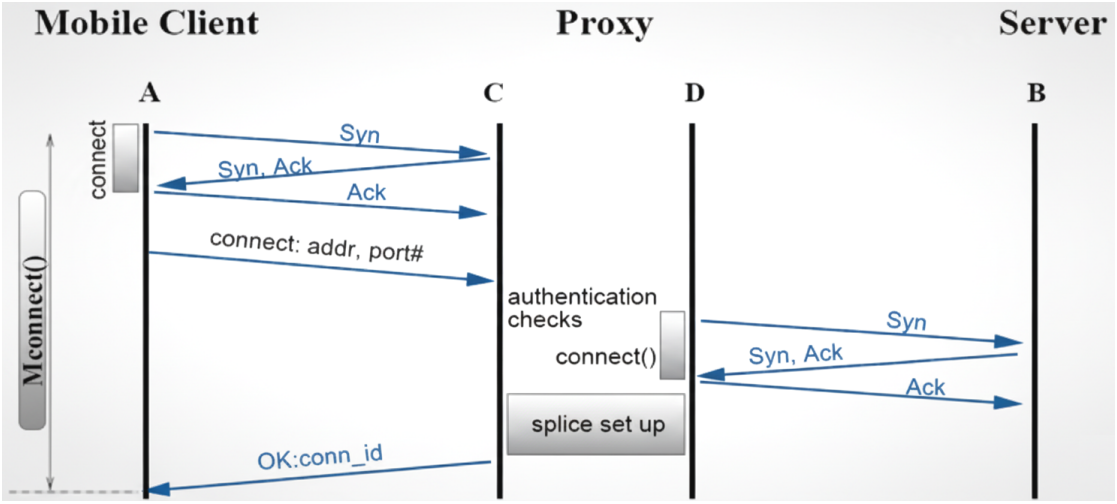

Рис. 2.3. Встановлення з'єднання між клієнтом MSOCK та вузлом-партнером через Проксі MSOCK

Механізм сплайсингу дозволяє виконувати повторне підключення (re-splice) навіть за наявності даних, що передаються, або під час жорсткої передачі обслуговування (hard handover), коли попередження про зміну адреси відсутнє. Протокол MSOCKS RECONNECT у поєднанні з TCP Splice гарантує збереження надійних, послідовних семантик TCP наскрізного зв'язку.

1. Розрив З'єднання: З'єднання МВ-Проксі розривається (наприклад, через зміну підмережі та отримання нової IP-адреси, або перемикання інтерфейсу).

2. Нове З'єднання МВ-Проксі: Бібліотека MSOCKS відкриває новий сокет і підключається до проксі.

3. Повідомлення Про Повторне Підключення: Бібліотека MSOCKS надсилає проксі повідомлення RECONNECT, вказуючи:

- Ідентифікатор з'єднання старого сеансу.

- Лічильник прочитаних даних (Read Counter): Кількість байтів, прочитаних застосунком з потоку даних.

- Лічильник записаних даних (Write Counter): Кількість байтів, записаних застосунком у потік даних.

4. Заміна та Сплайсинг: Проксі використовує новий сокет для сплайсингу зі статичним з'єднанням Проксі-ВП, замість старого з'єднання МВ-Проксі. Старе з'єднання закривається.

5. Синхронізація: Проксі надсилає бібліотеці MSOCKS повідомлення OK з лічильниками запису та "порятунку" даних (rescue counters), що дозволяє бібліотеці завершити сплайсинг на стороні МВ.

Як результат застосунок МВ та ВП залишаються повністю необізнаними про факт переключення.

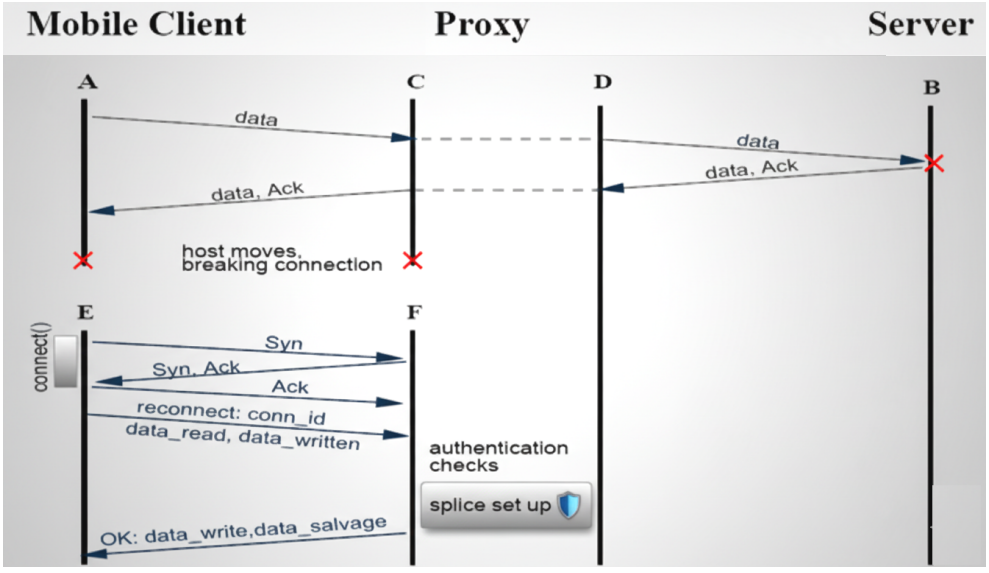

Рис. 2.4. Діаграма обміну пакетами для мобільного вузла, що повторно підключається до існуючого з'єднання

На діаграмі (рис. 2.4) зображено обмін пакетами, що відбувається, коли з'єднання між мобільним вузлом і проксі-сервером розривається з певної причини (наприклад, мобільний вузол переміщується й отримує нову IP-адресу, або він бажає перемкнути сесію з одного мережевого інтерфейсу на інший).

1. Ініціація Нового Сокета: Після розриву з'єднання з проксі-сервером бібліотека MSOCKS відкриває новий сокет (позначений як E на діаграмі) та використовує його для встановлення з'єднання з проксі-сервером.

2. Передача повідомлення про реконфігурацію: Бібліотека MSOCKS передає повідомлення про реконфігурацію до проксі-сервера. Це повідомлення містить ідентифікатор старого з'єднання до сервера, а також:

- Лічильник зчитаних даних (data-read counter): інформує проксі-сервер про кількість байтів даних, які застосунок зчитав зі з'єднання.

- Лічильник записаних даних (data-written counter): інформує проксі-сервер про кількість байтів даних, які застосунок записав у з'єднання.

3. З'єднання та Закриття: Проксі-сервер здійснює сплайсинг (з'єднання) нового з'єднання до з'єднання «проксі-сервер», замінюючи старе з'єднання «мобільний вузол-проксі», і закриває старе з'єднання.

4. Фіналізація Реконфігурації: Після налаштування сплайсу проксі-сервер надсилає повідомлення OK до бібліотеки MSOCKS. Це повідомлення містить лічильники запису даних (data write counter) та лічильники збереження даних (data salvage counters), які надають бібліотеці MSOCKS вказівки щодо завершення сплайсу на стороні мобільного вузла.

Застосунок і сервер залишаються повністю неінформованими про факт здійснення перемикання. Ця методологія забезпечує прозорість реконфігурації для кінцевих точок зв'язку

2.1.4. Продуктивність

Однією з ключових проблем є швидкість, з якою MSOCKS здатен відновлювати TCP-з'єднання після прийняття рішення про

перемаршрутизацію. Час, необхідний проксі-серверу для повторного об'єднання двох з'єднань, є незначним. Основна затримка при відновленні з'єднання обумовлена часом, необхідним для встановлення нового TCP-з'єднання та передачі повідомлення RECONNECT, що, у свою чергу, критично залежить від часу проходження сигналу в обидва кінці (RTT) для конкретної мережевої технології, на яку здійснюється переключення.

Протокольний аналіз показує, що максимальна швидкість, з якою мобільний вузол може обґрунтовано відновлювати TCP-сесії, обмежується одним відновленням на 2.5 RTT: 1.5 RTT для встановлення з'єднання, 0.5 RTT для передачі повідомлення RECONNECT OK та 0.5 RTT для передачі даних.

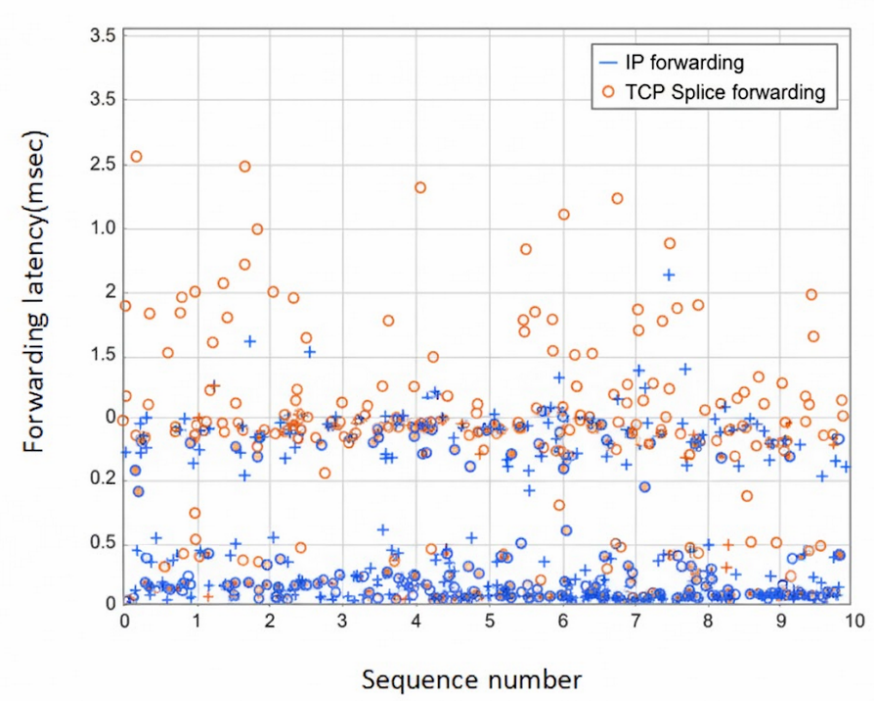

Рис. 2.5. Порівняння затримки IP-пересилання із затримкою TCP Splice-пересилання

На рисунку 2.5 представлено порівняння затримки пакетів у TCP-з'єднанні, маршрутизованому через IP-форвардинг на тестовій машині, із затримкою пакетів у TCP-з'єднанні, об'єднаному на тій же тестовій машині.

Вісь X на рисунку відповідає порядковому номеру пакету. Дані більш масштабного експерименту узагальнено в таблиці 2.1.

Таблиця 2.1.

Резюме затримок пересилання (мс)

Метод Пересилання	**Середнє значення (мс)**	**Стандартне відхилення (мс)**
IP-пересилання	0.4038	0.0960
TCP Splice-пересилання	0.4444	0.1120

Аналіз показує, що додаткова затримка, внесена механізмом TCP Splice, є невеликою, що підтверджує його ефективність як бази для підтримки мобільності.

2.2. Архітектура мобільності SIGMA на основі різноманітності IP-адрес

SIGMA (Seamless IP diversity based Generalized Mobility Architecture) є архітектурою, що забезпечує безперебійну передачу обслуговування (handover) для мобільних хостів. Її функціонування базується на протоколі SCTP (Stream Control Transmission Protocol), який є новим надійним транспортним протоколом, розробленим IETF для транспортування сигнальних повідомлень SS7 через IP-мережі. Порівняно з існуючими схемами handover, що ґрунтуються на Mobile IP, SIGMA демонструє значне зниження затримки handover, мінімізацію втрати пакетів, зменшення сигнального трафіку та загальне покращення пропускної здатності системи.

Існуючі протоколи мобільності транспортного рівня реалізують мобільність як наскрізну послугу, не вимагаючи модифікації інфраструктури мережевого рівня. Проте, значна частина цих протоколів не орієнтована на зменшення високих затримок та втрат пакетів, що виникають під час процесу handover. На відміну від них, SIGMA вирішує проблеми високої затримки та

втрати пакетів, забезпечуючи "безперебійність", що означає низьку затримку та низьку втрату пакетів. Фундаментальна концепція SIGMA полягає в розділенні функцій керування розташуванням та передачі даних, а також у досягненні безперебійного handover шляхом використання різноманітності IP-адрес. Це дозволяє підтримувати активним старий шлях передачі даних під час налаштування нового шляху в процесі handover.

2.2.1. Детальний опис процедури handover в SIGMA

Процедура handover в архітектурі SIGMA включає наступні етапи:

Крок 1: Отримання нової IP-адреси.

Як показано на рисунку 2.6, процес підготовки до handover починається, коли мобільний хост (MH) переміщується в зону радіопокриття, що перекривається двома сусідніми підмережами. Після отримання анонсу маршрутизатора від нового маршрутизатора доступу (AR2), MH ініціює отримання нової IP-адреси (IP2 на рисунку 2.6). Цей процес може бути реалізований за допомогою різних методів, таких як DHCP, DHCPv6 або автоконфігурація адреси без збереження стану IPv6 (SAA).

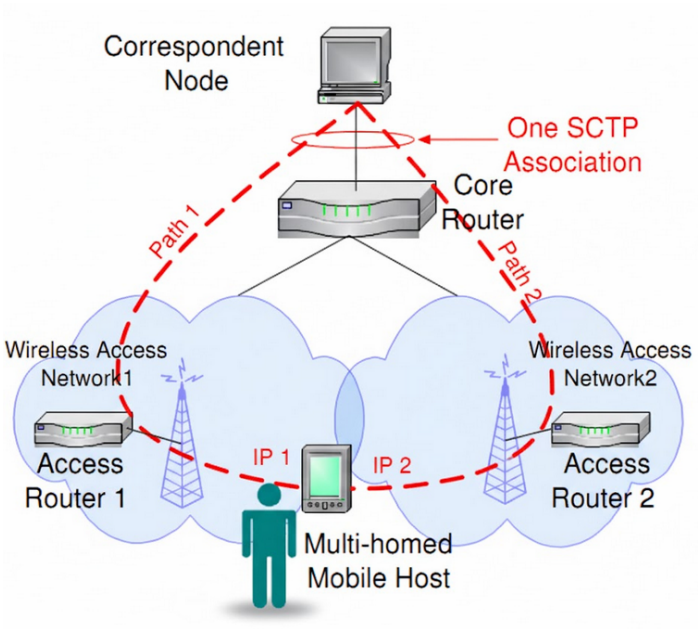

Рис. 2.6. З'єднання за протоколом SCTP з мобільним вузлом, що має кілька домашніх адрес

Крок 2: Додавання IP-адрес до асоціації.

Після успішного отримання IP-адреси IP2 на кроці 1, MH повинен проінформувати кореспондентний вузол (CN) про доступність нової IP-адреси. Це здійснюється за допомогою опції динамічної реконфігурації адрес SCTP. Ця опція визначає два нові типи чанків (ASCONF та ASCONF-ACK) та кілька типів параметрів (Додати IP-адресу, Видалити IP-адресу, Встановити основну адресу тощо).

Крок 3: Перенаправлення пакетів даних на нову IP-адресу.

При подальшому переміщенні MH в зону покриття бездротової мережі доступу 2, CN може перенаправляти трафік даних на нову IP-адресу IP2 для підвищення ймовірності успішної доставки даних до MH. Це завдання виконується шляхом надсилання чанку ASCONF від MH до CN, після чого CN встановлює IP2 як свою основну адресу призначення для MH.

Крок 4: Оновлення менеджера розташування (LM).

SIGMA використовує менеджер розташування, який підтримує базу даних, що містить відповідність між ідентичністю MH та його поточною основною IP-адресою. MH може використовувати будь-яку унікальну інформацію як свою ідентичність, наприклад, домашню адресу (як у MIP), доменне ім'я або відкритий ключ, визначений в інфраструктурі відкритих ключів (PKI). Важливою відмінністю між SIGMA та MIP є те, що в MIP функції керування розташуванням та пересилання трафіку даних об'єднані, тоді як у SIGMA вони розділені для прискорення handover та забезпечення більш гнучкого розгортання.

Крок 5: Видалення або деактивація застарілої IP-адреси.

Коли MH виходить з зони покриття бездротової мережі доступу 1, нові або повторно передані дані не повинні направлятися на адресу IP1. В SIGMA MH інформує CN про неактивність IP1 для передачі даних, надсилаючи CN чанк ASCONF для видалення IP1 зі списку доступних IP-адрес призначення CN. Менш агресивний спосіб запобігання надсиланню даних CN на IP1 полягає в оголошенні MH нульового вікна приймача (відповідно до IP1) CN.

Деактивація, а не повне видалення IP-адреси, дозволяє SIGMA більш гнучко адаптуватися до зигзагоподібних рухів MH та повторно використовувати раніше отриману IP-адресу (IP1) до закінчення терміну її дії. Це призводить до зменшення затримки та сигнального трафіку, пов'язаних з отриманням нової IP-адреси.

2.2.2. Діаграма синхронізації

На рисунку 2.7 представлено послідовність сигналізації, задіяної в SIGMA. Тут припускається, що для отримання нової IP-адреси MH використовує IPv6 SAA. Слід зазначити, що до видалення старої IP-адреси на CN вона завжди може отримувати пакети даних паралельно з обміном сигнальними пакетами.

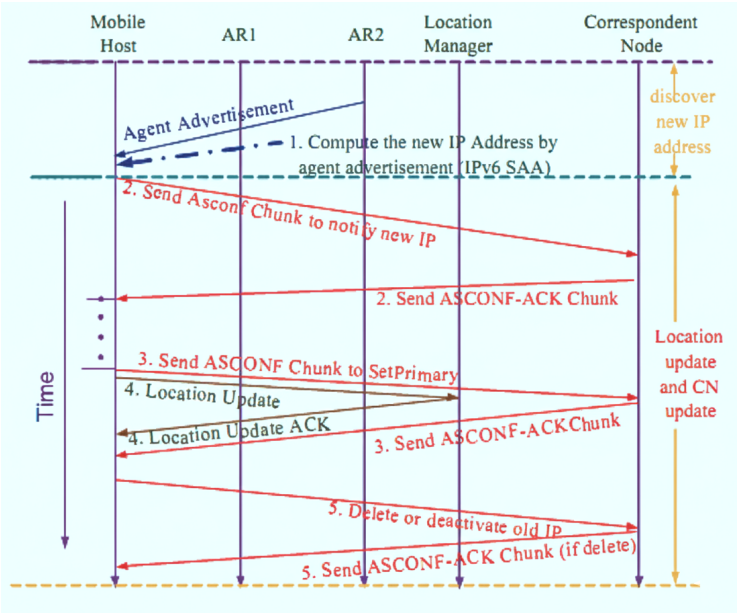

Рис. 2.7. Часова діаграма SIGMA

2.3. Архітектура, механізми функціонування та порівняльний аналіз протоколу керування RCP

Протокол керування прийомом (RCP) реалізує парадигматичний зсув, переносячи відповідальність за забезпечення надійності передачі даних та

контроль перевантаження з вузла-відправника на вузол-отримувач. Даний протокол, будучи орієнтованим на отримувача, по суті, є аналогом TCP у своїх загальних операційних принципах, однак надає досконаліші механізми для управління перевантаженням, відновлення втрачених пакетів та оптимізації енергоспоживання порівняно з підходами, що покладаються на відправника. Особливої актуальності набуває той факт, що в контексті сучасних тенденцій, де мобільні хости все частіше оснащуються множинними мережевими інтерфейсами для доступу до гетерогенних бездротових мереж, демонструється, що протокол, орієнтований на отримувача, такий як RCP, здатний слугувати потужним та комплексним рішенням транспортного рівня для таких багатодомних (multi-homed) хостів. Оцінка продуктивності RCP проводиться з подвійною метою: для демонстрації його сумісності з TCP (TCP-friendliness) та для висвітлення його унікальних переваг відносно протоколів, орієнтованих на відправника.

2.3.1. Транспозиція функціональних обов'язків

Протокол керування передачею (TCP) класифікується як транспортний протокол, орієнтований на з'єднання, що забезпечує надійну та впорядковану доставку даних прикладному рівню. Функціонування даного протоколу базується на чотирьох ключових механізмах: управлінні з'єднанням, контролі потоку, контролі перевантаження та забезпеченні надійності.

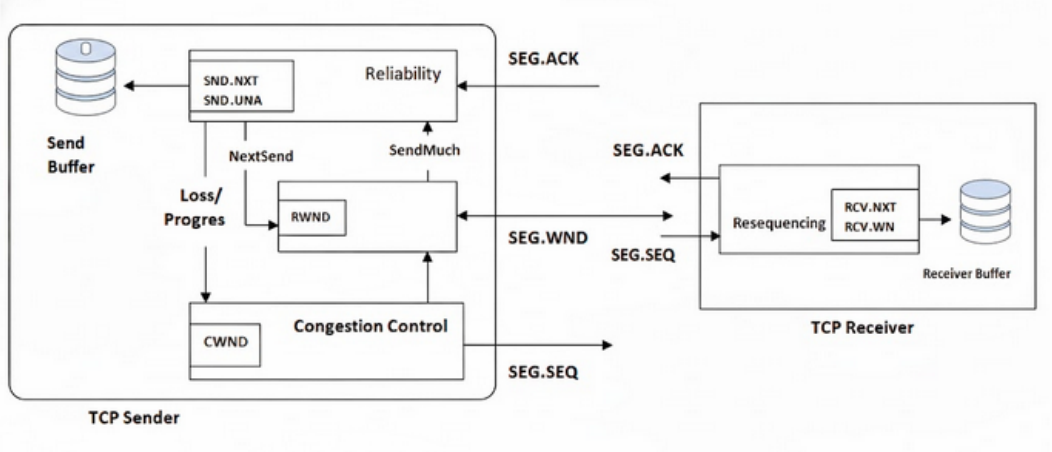

Рис. 2.8. Підхід TCP, орієнтований на відправника

На рисунку 2.8 представлена схематична діаграма взаємодії між відправником та отримувачем у рамках протоколу TCP, а також наведено декілька змінних стану.

Управління з'єднанням є фундаментальною вимогою для будь-якого протоколу, орієнтованого на з'єднання, з метою синхронізації станів між взаємодіючими вузлами. Після встановлення з'єднання відправник у TCP контролює процес передачі даних. Він вилучає дані зі свого буфера, керуючись обсягом, який може прийняти отримувач (контроль потоку), та пропускною здатністю, яку може підтримувати мережа (контроль перевантаження). Отримувач, у свою чергу, виконує перевпорядкування отриманих сегментів та надсилає підтвердження про їх доставку. Надійність передачі даних досягається за допомогою механізмів виявлення та відновлення втрат, які реалізовані на стороні відправника. Очевидно, що управління з'єднанням є процесом, який не може бути реалізований однобічно, а вимагає участі обох сторін. Щодо інших зазначених функцій, то в той час як TCP застосовує підхід, орієнтований на відправника, RCP делегує ці повноваження отримувачу, як це ілюстровано на рисунку 2.9.

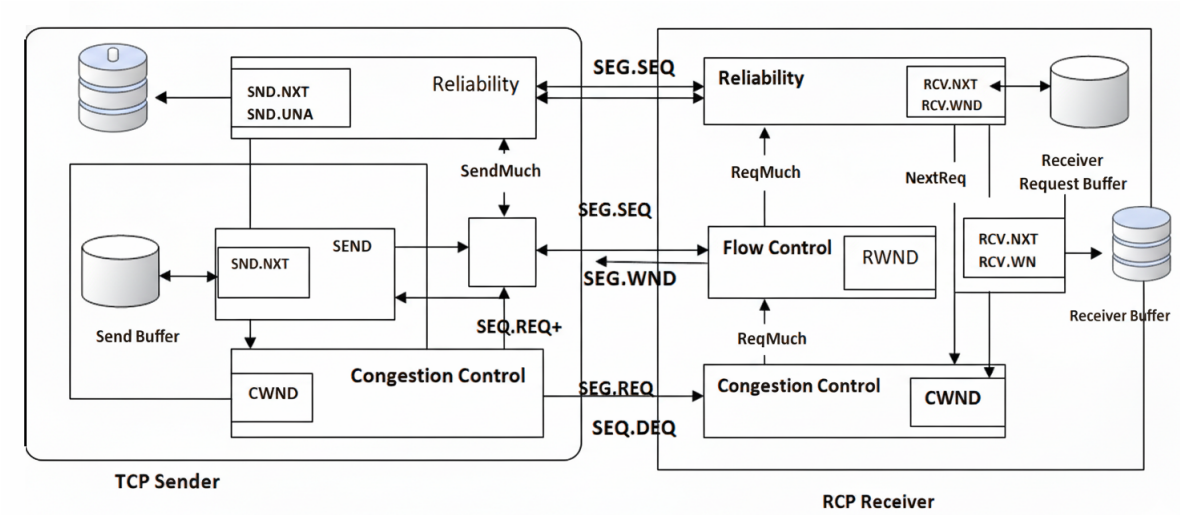

Рис. 2.9. Підхід TCP, орієнтований на отримувача

На відміну від отримувача в TCP, функціонал якого обмежується відправкою підтверджень без можливості впливу на послідовність та

номенклатуру даних, що передаються, отримувач в RCP здійснює явний контроль над цими аспектами та над процесом надійної доставки даних. Більше того, отримувач в RCP повністю контролює пропускну здатність, яку може використовувати з'єднання, застосовуючи той самий алгоритм на основі ковзного вікна, що і відправник у TCP. Нарешті, хоча контроль потоку в TCP є функцією, що залучає відправника, в RCP він виконується виключно на стороні отримувача. Таким чином, отримувач в RCP визначає як обсяг даних, який може бути переданий відправником (через контроль перевантаження та потоку), так і специфічні дані, що підлягають передачі (через механізм надійності).

2.3.2. Загальний огляд протоколу RCP

У протоколі RCP, оскільки контроль за передачею даних переноситься від відправника до отримувача, парадигма управління DATA-ACK, властива TCP, стає незастосовною. Натомість, для імітації властивостей самосинхронізації (self-clocking) TCP, RCP використовує механізм квитування REQ-DATA для передачі даних. У рамках цього механізму будь-яка передача даних відправником ініціюється явним запитом (REQ) від отримувача. Еквівалентно, RCP використовує потік вхідних даних для синхронізації запитів на нові дані. Відправник підтримує лише буфер відправки з єдиним вказівником (SND.NXT), що позначає максимальний порядковий номер, який було надано. Після встановлення з'єднання отримувач ініціює запит даних від відправника на основі початкового розміру вікна перевантаження. Еволюція його вікна перевантаження проходить ті ж фази, що й у TCP: повільний старт, уникнення перевантаження, швидка повторна передача та швидке відновлення. Ключова відмінність у функціонуванні полягає в тому, що будь-який тригер для активації контролю перевантаження визначається на основі прибуття (або неприбуття) сегментів даних. Наприклад, втрата пакету детектується за фактом отримання трьох невпорядкованих сегментів даних, а не на основі

дубльованих підтверджень. Після виявлення втрати сегмента, RCP зменшує розмір свого вікна перевантаження та повторно надсилає відповідний REQ-пакет, запитуючи втрачений сегмент. На завершення, отримувач виконує перевпорядкування даних та передає впорядкований потік даних прикладному рівню.

2.3.3. Механізм квитування REQ-DATA

У механізмі квитування DATA-ACK протокол TCP використовує кумулятивні підтвердження для досягнення стійкості до втрат пакетів. З метою імітації цієї стійкості та забезпечення толерантності до втрат на зворотному шляху, RCP дозволяє отримувачу надсилати запити у двох режимах: кумулятивному або вибірковому (pull), встановлюючи відповідний прапор вибіркового запиту (PUL - pull) у заголовку пакета. За замовчуванням, отримувач використовує кумулятивний режим для запиту нових даних і переходить до вибіркового режиму лише для повторної передачі запитів на втрачені сегменти. Коли відправник отримує запит із встановленим прапором PUL, він надсилає виключно той сегмент даних, який вказано в заголовку.

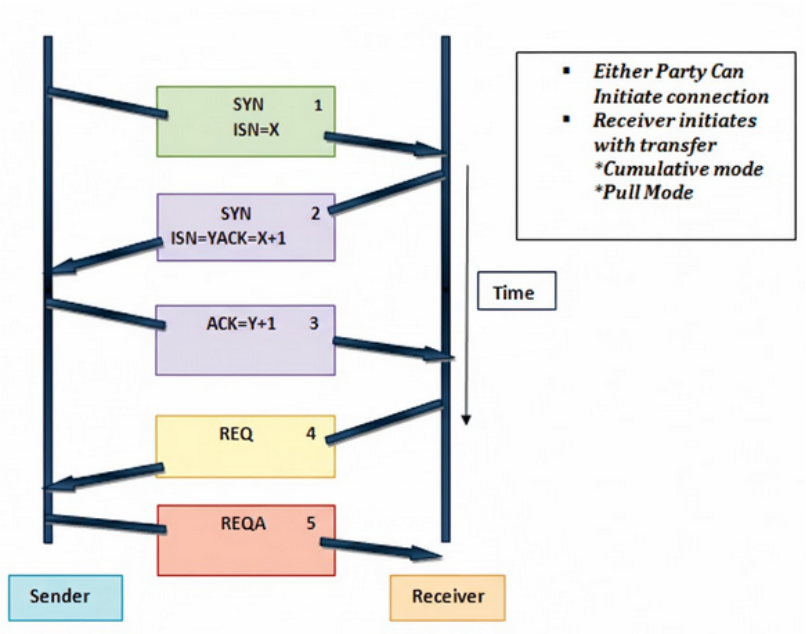

Рис. 2.10. Транспозиція функцій TCP

В іншому випадку, відправник здійснює кумулятивну передачу даних, починаючи з SND.NXT, які ще не були відправлені. Отже, втрата REQ-пакета в кумулятивному режимі має наслідки, аналогічні втраті ACK-пакета в TCP. Для захисту REQ-пакетів у вибірковому режимі від втрат, RCP застосовує механізм, подібний до того, який використовується в TCP для захисту опції SACK. Отримувач включає в заголовок REQ-пакета інформацію про останні блоки послідовних номерів (використовується три блоки, аналогічно до SACK), які він запитував. Відправник, окрім буфера відправки, підтримує циклічний буфер, що містить останні блоки послідовних номерів (три блоки), які він надіслав. При отриманні запиту, відправник перевіряє узгодженість між блоками в REQ та своїм циклічним буфером. Будь-яка розбіжність інтерпретується як індикація втрати REQ і буде відновлена відправником. Слід зазначити, що запит на конкретний сегмент даних у вибірковому режимі буде перенесений щонайменше у чотирьох послідовних REQ-пакетах.

2.3.4. Управління з'єднанням

Аналогічно до TCP, ініціювати встановлення з'єднання в RCP може як відправник, так і отримувач. Процедура встановлення з'єднання складається з ідентичного тристороннього квитування SYN-SYN+ACK-ACK, що використовується в TCP. Проте, після встановлення з'єднання, замість того, щоб відправник надсилав перший сегмент даних, отримувач в RCP передає перший REQ-пакет із початковим порядковим номером. Відправник, у свою чергу, передає перший сегмент даних лише після отримання цього запиту. Процедура завершення з'єднання в RCP також реалізована аналогічно до TCP.

2.3.5. Контроль перевантаження

У протоколі RCP отримувач відповідає за виконання контролю перевантаження та підтримує відповідні параметри, включаючи розмір вікна перевантаження (CWND) та інформацію про час кругового затримання

(RTT). Оскільки RCP є аналогом TCP, він використовує той самий алгоритм контролю перевантаження на основі ковзного вікна. Фази повільного старту, уникнення перевантаження, швидкої повторної передачі та швидкого відновлення ініціюються та завершуються за тими ж принципами, що й у TCP. Хоча ідентичний алгоритм адаптації вікна (адитивне збільшення, мультиплікативне зменшення) може бути реалізований на будь-якій стороні для контролю перевантаження, семантика вікна перевантаження та тригери для його модифікації (збільшення чи зменшення) є відмінними. У TCP розмір вікна перевантаження обмежує кількість непідтверджених даних у мережі, і відправник використовує отримання ACK-пакетів для просування вікна. Натомість, у RCP розмір вікна перевантаження обмежує кількість невиконаних REQ-запитів у мережі, а отримувач використовує отримання DATA-сегментів для просування свого вікна.

2.3.6. Контроль потоку

Контроль потоку дозволяє отримувачу обмежувати обсяг даних, що знаходяться в дорозі, відповідно до доступного простору в його буфері. Це актуально в ситуаціях, коли отримувач очікує, поки прикладний процес зчитає (і звільнить) впорядковані дані, або очікує на прибуття невпорядкованих сегментів. У RCP запит надсилається лише за умови, що отримання відповідних даних не спричинить переповнення буфера на стороні отримувача. Цього можна досягти шляхом створення фіктивного заповнювача (placeholder), що не містить даних, у буфері прийому для кожного запитаного сегмента. Нові запити генеруються по мірі звільнення простору в буфері. На відміну від TCP, у RCP, оскільки отримувач підтримує буфер прийому і має повний контроль над обсягом даних, який може надсилати відправник, контроль потоку є внутрішньою функцією отримувача. Примітно, що RCP також вимагає наявності поля вікна (SEG.DEQ) у заголовку пакета, щоб інформувати відправника про найвищий послідовний номер отриманих даних (що може бути обчислено на стороні

відправника за формулою SEG.REQ - SEG.DEQ), тим самим дозволяючи відправнику видаляти ці дані зі свого буфера відправки. Опція масштабування вікна, що використовується в TCP, може бути застосована до RCP аналогічним чином.

2.3.7. Забезпечення надійності

Як показано на рисунку 2.9, у протоколі RCP функції перевпорядкування сегментів та забезпечення надійності поєднані на стороні отримувача. Після отримання сегмента даних від відправника, отримувач розміщує його у відповідному місці буфера та оновлює вказівник RCV.NXT після процесу перевпорядкування. У TCP, оскільки надійність реалізована на стороні відправника, а перевпорядкування — на стороні отримувача, значення RCV.NXT передається у вигляді кумулятивного підтвердження (ACK) відправнику для здійснення виявлення втрат. Проте RCV.NXT надає обмежену інформацію про стан буфера прийому, через що ранні реалізації TCP, що покладалися виключно на кумулятивні ACK, стикалися з проблемою відновлення не більше однієї втрати за один час кругового затримання (RTT), а також часто провокували спрацьовування тайм-аутів. Для вирішення цього обмеження була запропонована опція вибіркового підтвердження (SACK), за допомогою якої відправник TCP намагається побудувати бітову карту буфера отримувача в структурі даних, відомій як "scorecard". Однак у RCP отримувач має прямий доступ до буфера прийому, що дозволяє йому своєчасно та точно виконувати виявлення та відновлення втрат без необхідності використання механізму SACK.

2.3.8 Підтримка гетерогенних інтерфейсів

Коли зони покриття різних технологій доступу до мережі перекриваються, стає можливою реалізація безшовної передачі обслуговування на канальному рівні. Проте такі передачі не завжди транслюються в аналогічну безшовність на транспортному рівні. Зокрема,

коли мобільний хост переходить з одного інтерфейсу на інший зі зміною IP-адреси, що обробляється протоколом Mobile IP, значна затримка, пов'язана з реєстрацією у домашнього агента, потенційно може призвести до втрати пакетів після завершення передачі на канальному рівні. Щоб запобігти негативній реакції TCP на втрату пакетів під час передачі обслуговування, мобільний хост повинен інформувати відправника про прийняте рішення. У ситуаціях, що вимагають зворотного зв'язку, протокол, орієнтований на отримувача, демонструє переваги порівняно з протоколом, орієнтованим на відправника, завдяки локалізації необхідної інформації. Однак, хоча існує можливість "заморозити" TCP-з'єднання на час передачі, така зупинка викликає переривання в обслуговуванні та не дозволяє користувачам використовувати переваги безшовної передачі.

Одним із рішень для уникнення затримок без залежності від інфраструктурної підтримки є використання протоколу мобільності на транспортному рівні для забезпечення наскрізної мобільності хоста. Коли мобільний хост приймає рішення виконати вертикальну передачу обслуговування, він може створити новий "потік даних" для передачі через нову IP-адресу, щойно новий інтерфейс стане активним. За допомогою такого підходу мобільний хост може одночасно використовувати декілька TCP-з'єднань (потоків), не відчуваючи переривань, доки канальний рівень підтримує безшовну передачу. Отже, протокол, орієнтований на отримувача, має значні переваги у такому сценарії, оскільки отримувач може точно контролювати, які дані та в якому обсязі надсилати через кожен канал, базуючись на стані (наприклад, силі сигналу) кожного інтерфейсу. Більше того, якщо отримувач приймає рішення про переключення на інший механізм контролю перевантаження після передачі обслуговування, це рішення не вимагає участі відправника. В іншому випадку, відправник був би змушений не тільки підтримувати множинні механізми контролю, але й забезпечувати плавний перехід між ними для активного з'єднання.

2.4. Архітектура транспортного протоколу R²CP для динамічного управління з'єднаннями в мобільних середовища

R²CP розшифровується як RADIAL RECEPTION CONTROL PROTOCOL (радіальний протокол керування прийомом). У сценаріях, коли мобільний хост здійснює передачу обслуговування між різними інтерфейсами під час активного з'єднання, він може утилізувати наступні функціональні можливості, що підтримуються транспортним протоколом:

1. Безшовна передача обслуговування без залежності від інфраструктурної підтримки.

2. Міграція сервера для забезпечення безперервності сервісу.

3. Агрегація пропускної здатності шляхом використання декількох активних інтерфейсів.

2.4.1. Операційна модель, орієнтована на отримувача

Для досягнення оптимальної продуктивності мобільному хосту може знадобитися застосування механізмів контролю перевантаження, специфічних для конкретної мережі або інтерфейсу. Коли мобільний хост оснащений гетерогенними бездротовими інтерфейсами, протокол, орієнтований на отримувача, надає йому можливість вільно застосовувати бажаний механізм контролю перевантаження залежно від обраного інтерфейсу або мережі доступу, до якої він мігрує, без залучення віддаленого сервера. Крім того, під час періодів мобільності може виникнути необхідність у передачі обслуговування від одного сервера до іншого (для безперервності сервісу) або у зміні кількості серверів, до яких він підключений (для агрегації пропускної здатності). Таким чином, для мобільного хоста є архітектурно вигідним застосування протоколу, орієнтованого на отримувача, з спрощеною архітектурою відправника, що дозволяє мобільному хосту контролювати надійну доставку даних від одного чи кількох відправників. Будучи протоколом, орієнтованим на отримувача,

який делегує мобільному хосту управління такими аспектами, як контроль перевантаження та надійність, R²CP позиціонується як ідеальний протокол для цільового середовища.

Існуючі транспортні протоколи демонструють деградацію продуктивності під час передачі обслуговування між гетерогенними мережами через значну затримку, що вноситься протоколом Mobile IP. Хоча були запропоновані рішення для наскрізної мобільності хоста без залежності від інфраструктури, вони не вирішують цю проблему повною мірою через одностанову архітектуру TCP, яка підтримує лише один блок керування передачею (TCB) на з'єднання. Коли передачі обслуговування на канальному рівні анулюють стан, що підтримується на транспортному рівні (наприклад, через зміну IP-адрес), транспортний протокол повинен відповідним чином модифікувати свій стан для досягнення мобільності транспортного рівня. Хоча існуючі рішення інтелектуально виконують міграцію з'єднання, вони провокують втрату пакетів, перезаписуючи старий стан одразу після створення нового. Ідеальне рішення для міграції стану, однак, повинно забезпечувати співіснування обох станів у рамках з'єднання протягом часу, необхідного для передачі обслуговування (з урахуванням пакетів, що знаходяться в транзиті). Отже, для підтримки прозорої мобільності хоста без інфраструктурної підтримки транспортний протокол повинен бути здатним обробляти множинні стани. Даний протокол розроблено як багатостанове розширення RCP.

R²CP динамічно створює та видаляє стани RCP відповідно до кількості активних інтерфейсів. Він ефективно підтримує множинні стани на мобільному хості без необхідності явної підтримки з боку віддаленого сервера. На стороні відправника не потрібні жодні модифікації RCP для підтримки багатостанової роботи на стороні отримувача. Оскільки це розширення є специфічним для отримувача, воно дозволяє мобільному хосту встановлювати багатопунктове з'єднання з кількома серверами, тоді як у

пов'язаних дослідженнях множинні стани обмежуються рамками одноадресного (unicast) з'єднання.

2.4.2. Архітектурний огляд

На рисунку 2.11 представлено архітектурний огляд R²CP та його ключові структури даних. З'єднання R²CP складається з одного отримувача та одного або декількох відправників, які можуть розташовуватися на одному або кількох хостах. Хоча одноадресне з'єднання R²CP функціонально еквівалентне з'єднанню RCP, багатопунктове з'єднання R²CP можна розглядати як агрегацію декількох з'єднань RCP, чиї приймальні кінці координуються механізмом R²CP на стороні отримувача.

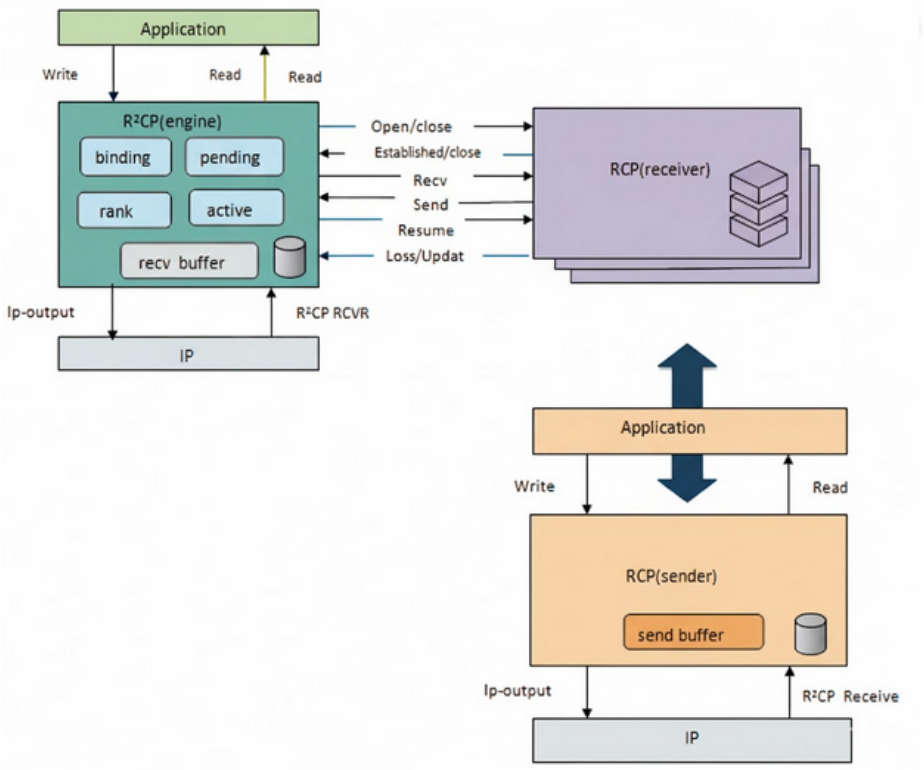

Рис. 2.11. Архітектура R²CP

Віртуальні з'єднання, що існують між отримувачем R²CP та окремими відправниками, іменуються RCP-каналами (RCP pipes). Коли застосунок на мобільному хості ініціює з'єднання R²CP, створюється один RCP-канал між

активним інтерфейсом та віддаленим сервером. При передачі обслуговування на інший інтерфейс створюється новий RCP-канал, після чого старий може бути видалений. Однак, якщо агрегація пропускної здатності можлива (старий інтерфейс залишається активним) і доцільна (вказана застосунком), старий канал не деактивується. У випадку міграції сервера створюється новий RCP-канал між новоактивним інтерфейсом та новим сервером. Коли в з'єднанні R²CP співіснують декілька RCP-каналів, механізм R²CP виконує планування передачі для мінімізації невпорядкованого надходження даних. Оскільки дані запитуються через різні канали, їх потоки можуть бути несуміжними. Отже, в R²CP запит завжди передається у вибірковому режимі (pull mode), щоб відправник передавав лише явно запитані дані. Для спрощення виявлення та відновлення втрат кожен RCP-канал внутрішньо підтримує локальний простір порядкових номерів, який механізм R²CP транслює в глобальний простір номерів для агрегованого з'єднання і навпаки.

2.4.3. Управління з'єднанням та контроль перевантаження

При створенні RCP-каналу, R²CP ініціює процедуру встановлення з'єднання за допомогою виклику open(). Процедура ідентична стандартному управлінню з'єднанням в RCP. Після успішного встановлення канал повідомляє R²CP через виклик established(). З'єднання R²CP вважається встановленим, коли хоча б один з його каналів переходить у цей стан. При видаленні каналу R²CP використовує виклик close() для ініціації процедури завершення. З'єднання R²CP закривається, коли всі його канали завершують роботу.

Контроль перевантаження в з'єднанні R²CP виконується індивідуально для кожного каналу. Кожен RCP-канал відповідає за регулювання обсягу даних, що передаються відповідним маршрутом. R²CP визначає, який механізм контролю перевантаження використовувати для кожного інтерфейсу, відкриваючи відповідний RCP-канал. Передбачається, що вибір

механізму є зовнішнім рішенням, яке надається R²CP через системну конфігурацію або опції сокету.

Оскільки R²CP управляє загальним буфером прийому, він відповідає за контроль потоку агрегованого з'єднання. R²CP тимчасово зупиняє запитуючий RCP-канал, якщо виявляє, що кількість невиконаних запитів дорівнює доступному простору в буфері, і відновлює його роботу через виклик resume(), коли простір звільняється. Механізм контролю потоку на рівні окремих RCP-каналів не буде функціональним, оскільки вони не оперують з фактичними сегментами даних. R²CP також відповідає за інформування відправників про те, які дані можна видалити з їхніх буферів, використовуючи поле SEG.DEQ.

R²CP несе основну відповідальність за надійну передачу даних агрегованого з'єднання. Ця мета досягається шляхом підтримки інформації про прив'язку для всіх сегментів даних. Після прив'язки сегмента до конкретного RCP-каналу, відповідальність перебирає на себе відповідний канал. Однак, якщо RCP-канал виявляє втрату сегмента і повідомляє про це R²CP через виклик loss(), R²CP відв'язує відповідний сегмент і делегує його надійну передачу наступному доступному каналу.

2.4.4. Безшовна передача обслуговування

При передачі обслуговування між гетерогенними мережами ключовою проблемою є аспекти, пов'язані зі зміною IP-адреси та затримкою реєстрації. Багатостанова архітектура R²CP дозволяє відкривати множинні канали, асоційовані з бездротовими інтерфейсами. Зберігаючи старе з'єднання активним під час налаштування нового, застосунок може безперервно передавати та отримувати дані через будь-який або обидва інтерфейси. Навіть за наявності затримки налаштування або фази повільного старту для нового каналу (RCP-2), існування старого каналу (RCP-1) дозволяє агрегованому з'єднанню функціонувати без перерв. Цей підхід кардинально

відрізняється від рішень, що використовують одностанові транспортні протоколи.

2.4.5. Міграція сервера

Ключовою відмінністю R²CP від інших багатостанових протоколів є здатність підтримувати міграцію кінцевих точок. Завдяки архітектурі, орієнтованій на отримувача, відправник не підтримує жорстко заданих станів з'єднання (наприклад, таймерів повторної передачі). Оскільки мобільний хост контролює, які дані отримувати, міграція від одного сервера до іншого може бути реалізована шляхом припинення запитів до старого сервера та ініціації запитів до нового.

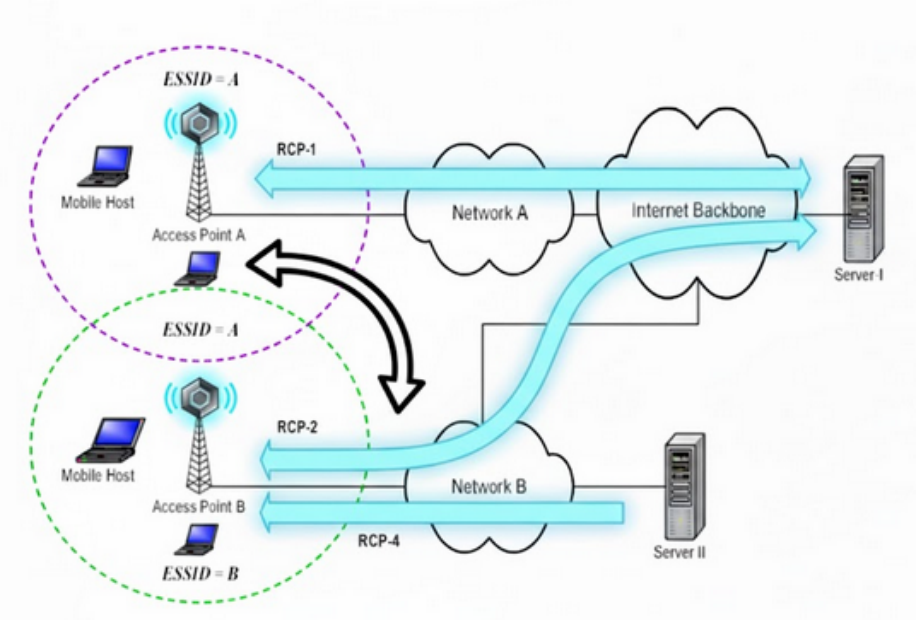

Рис. 2.12. Тестовий сценарій R²CP

Як ілюстровано на рисунку 2.12, при переміщенні мобільного хоста до мережі B він отримує доступ до реплікованого сервера (Сервер-II). Оскільки наскрізний маршрут від мобільного хоста (через інтерфейс B) до Сервера-II характеризується меншим часом кругового затримання (RTT) та вищою пропускною здатністю, хост ініціює процедуру міграції сервера від Сервера-I до Сервера-II.

На початковому етапі з'єднання R²CP встановлює RCP-канал (RCP-1), використовуючи мережеву адресу A та адресу Сервера-I. Після переміщення мобільного хоста до мережі B та прийняття рішення про міграцію, протокол R²CP створює новий RCP-канал (RCP-3), що з'єднує мережеву адресу B з адресою Сервера-II. (Варто зазначити, що якби міграція не виконувалася, був би створений канал RCP-2 між мережевою адресою B та початковим Сервером-I).

Після встановлення нового RCP-каналу мобільний хост запитує лише ті сегменти даних, що не були доставлені Сервером-I, замість того, щоб ініціювати передачу з початкового байта. Методології, що застосовуються для забезпечення безшовної передачі обслуговування, також є релевантними для реалізації безшовної міграції сервера. Аналізуючи вміст свого буфера прийому, R²CP може формувати запити на несуміжні (non-contiguous) блоки даних від Сервера-II.

Таким чином, міграція сервера з використанням R²CP унеможливлює надлишкову передачу даних, на відміну від підходу на основі TCP, де відправник передає виключно впорядкований потік даних. Хоча підтримка вибіркового отримання даних реалізована в деяких протоколах прикладного рівня (наприклад, запити діапазону в HTTP 1.1), R²CP забезпечує цю функціональність на транспортному рівні без необхідності будь-якої спеціалізованої підтримки з боку серверного застосунку.

2.4.6. Агрегація пропускної здатності

У випадках, коли старе з'єднання залишається активним після передачі обслуговування, для мобільного хоста є доцільним досягнення агрегованої пропускної здатності шляхом одночасного використання обох інтерфейсів. R²CP дозволяє співіснування декількох RCP-каналів в одному з'єднанні та виконує ефективне планування для розподілу трафіку (striping), що дозволяє легко досягти агрегації. Для оцінки продуктивності було проведено симуляційне моделювання, де R²CP порівнювався з трьома підходами:

Ідеальний (теоретична сума пропускних здатностей), APPS (розподіл на рівні застосунку) та R²CP-s (спрощена версія R²CP з плануванням FIFO).

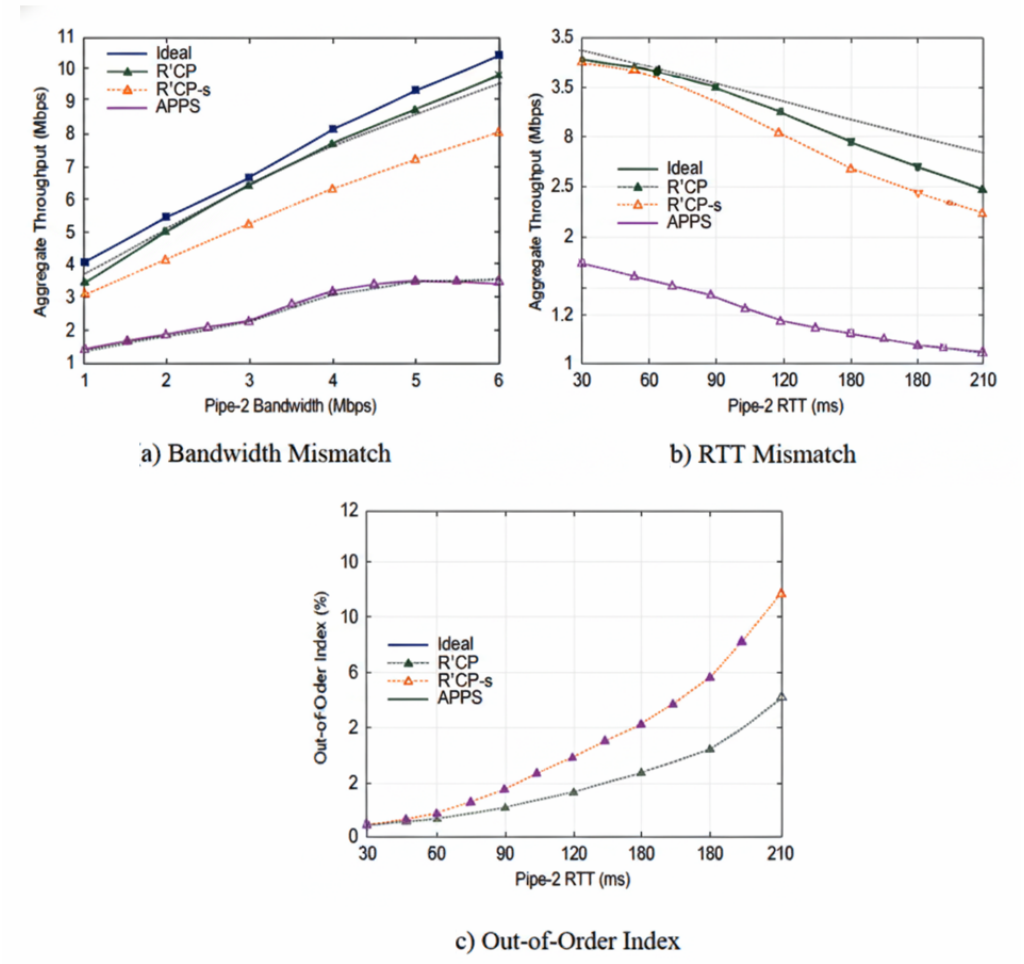

Рис. 2.13. Продуктивність R²CP

Результати (рис. 2.13) демонструють наступне:

- при невідповідності пропускних здатностей (рис. 2.13 a), R²CP та R²CP-s досягають практично ідеальної продуктивності.

- при невідповідності часу кругового затримання (RTT) (рис. 2.13 b), продуктивність R²CP-s значно погіршується, коли розбіжність RTT перевищує коефіцієнт 3, через часті невпорядковані надходження пакетів. Натомість R²CP, завдяки інтелектуальному плануванню, продовжує демонструвати продуктивність, близьку до ідеальної.

- аналіз заповненості буфера (рис. 2.13 c) підтверджує, що планування в R²CP-s та APPS призводить до значних черг і блокувань, тоді як R²CP

підтримує ефективне використання буферного простору навіть за значних розбіжностей у характеристиках каналів.

Висновки до розділу

Другий розділ присвячено детальному аналізу архітектури та функціональних можливостей основних протоколів транспортного рівня – MSOCKS, SIGMA, RCP та R²CP. Для кожного з них розглянуто принципи організації з’єднань, механізми передачі обслуговування, управління перевантаженнями та забезпечення надійності. Показано, що протоколи відрізняються за ступенем централізації управління, вимогами до інфраструктури та підтримкою багатоінтерфейсної взаємодії. Здійснено порівняльний аналіз продуктивності й визначено фактори, що впливають на затримки при handover та стабільність з’єднання. Результати розділу стали основою для систематизації архітектур мобільності та подальшої розробки узагальненої таксономії транспортних протоколів.

РОЗДІЛ 3. МЕТОДИ ТА АРХІТЕКТУРИ УПРАВЛІННЯ МОБІЛЬНІСТЮ ПРОТОКОЛІВ НА ТРАНСПОРТНОМУ РІВНІ

3.1. Представлення методів оптимізації TCP для мобільних мереж та обґрунтування переваг наскрізного підходу Freeze-TCP

Експоненціальне зростання популярності бездротових послуг та кількості їх абонентів, а також поширення портативних обчислювальних пристроїв зумовлює актуальність та складність проблеми забезпечення мобільності користувачів в Інтернеті, що привертає значну увагу дослідницької спільноти. Після відносної стандартизації базового протоколу Mobile IP, дослідники зосереджують увагу на механізмах підвищення продуктивності на всіх рівнях мережевого стека для гарантування високої якості обслуговування на рівні кінцевого користувача.

Протокол TCP є фундаментальним компонентом транспортного рівня в стеку протоколів Інтернету. Його призначення — надання надійного сервісу, орієнтованого на з'єднання, поверх базової ненадійної мережі. Відтак, TCP став об'єктом численних досліджень, спрямованих на оптимізацію та покращення його роботи в різноманітних середовищах, що характеризуються гетерогенними підмережами з відмінними пропускними здатностями та затримками (наприклад, TCP у бездротових, супутникових та низькошвидкісних послідовних каналах).

У даній роботі спочатку аналізуються проблеми функціонування TCP у мобільних середовищах. Далі представлено огляд запропонованих рішень із зазначенням їхніх переваг та недоліків. На завершення представлено наше рішення — Freeze-TCP.

3.1.1 Управління TCP та мобільне середовище

TCP використовує механізм ковзного вікна для забезпечення надійної, послідовної доставки даних, а також для контролю потоку та

перевантаження. Цей процес графічно ілюстровано на рисунку 3.1, де вікно зсувається праворуч. Розмір вікна (W) визначається як мінімальне значення між оголошеним буферним простором отримувача та оціненим рівнем перевантаження мережі. Відправник може мати до W непідтверджених пакетів у транзиті.

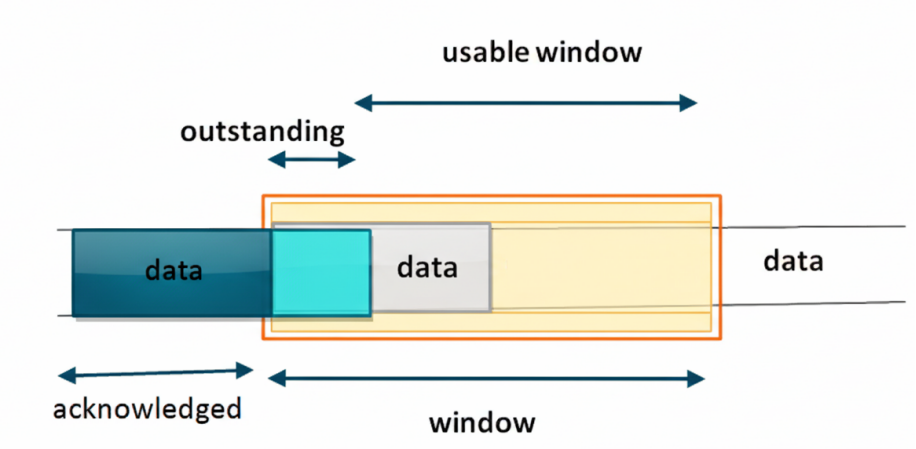

Рис. 3.1. Механізм управління вікном TCP

За нормальних умов, якщо процес-споживач на стороні отримувача працює повільніше, ніж відправник, буфери отримувача починають заповнюватися, що змушує його оголошувати progressively менші розміри вікна. У крайньому випадку, коли буферний простір вичерпується, отримувач оголошує нульовий розмір вікна.

При отриманні оголошення нульового розміру вікна відправник зобов'язаний призупинити всі таймери повторної передачі та перейти в режим наполегливості (persistence mode). Цей режим передбачає періодичне надсилання зондуючих пакетів (Zero Window Probes, ZWP), доки вікно отримувача не відкриється. Інтервал між зондами експоненційно збільшується до максимального значення в 1 хвилину. Оскільки доставка ZWP не гарантується, їх втрата не призводить до зменшення вікна перевантаження відправника. Зрештою, отримувач відповідає на ZWP ненульовим розміром вікна, і передача даних відновлюється.

Винятком є ситуація, коли отримувач зменшує оголошений розмір вікна, зсуваючи його правий край вліво. Це може призвести до раптового утворення негативного розміру корисного вікна, що здатне викликати некоректну поведінку відправника. Хоча така поведінка не рекомендована, протокол повинен коректно її обробляти. Відправнику дозволяється повторно передавати непідтверджені пакети, але не надсилати нові дані, і він має перейти в режим наполегливості.

3.1.2. Проблеми функціонування TCP у мобільних середовищах

Протокол TCP був розроблений для дротових статичних топологій, що характеризуються високим ступенем надійності. Тому він функціонує на базовому припущенні, що будь-яка втрата пакета є наслідком мережевого перевантаження. Однак у мобільних середовищах втрати частіше спричинені:

- Високим коефіцієнтом бітових помилок (BER) у бездротових каналах.
- Тимчасовими роз'єднаннями, зумовленими завмиранням сигналу, помилками каналу або переміщенням мобільного вузла між зонами покриття.

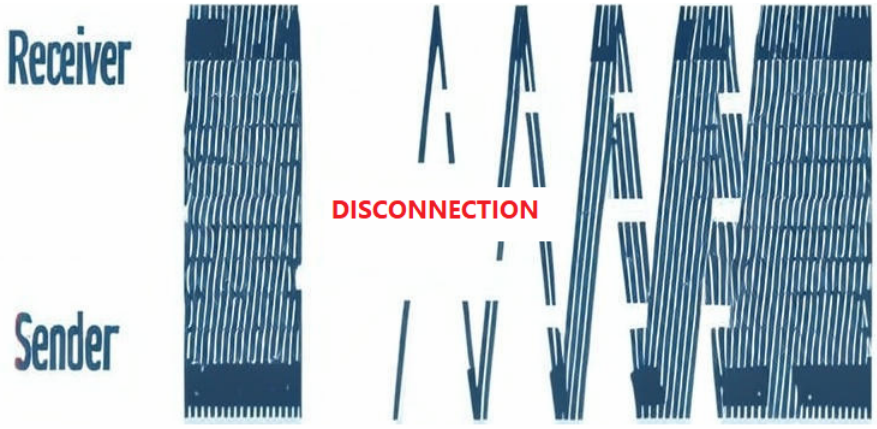

Рис. 3.2. Механізм повільного старту в TCP

Концепція мобільності передбачає, що відкриті з'єднання (FTP, Telnet тощо) повинні зберігатися безперервно, незважаючи на переміщення користувача та зміну базової IP-адреси. Стандартна реалізація TCP, зіткнувшись із втратою хоча б одного пакета, помилково інтерпретує її як

перевантаження і різко знижує швидкість передачі, зменшуючи вікно перевантаження до мінімуму. У поєднанні з механізмом повільного старту це призводить до невиправданого обмеження пропускної здатності, навіть якщо роз'єднання було короткочасним (рис. 3.2).

Було запропоновано декілька підходів для вирішення цих недоліків:

1. Проміжний агент на базовій станції кешує пакети, що прямують до мобільного вузла, і локально повторно передає їх у разі втрати в бездротовому каналі.

2. Indirect TCP (I-TCP) - розділяє TCP-з'єднання на два сегменти на базовій станції: один для дротової мережі та інший (потенційно з використанням іншого протоколу) для бездротової.

3. MTCP. Аналогічний до I-TCP, також розділяє з'єднання, використовуючи спеціалізований протокол для бездротового сегмента.

Інші методи включають затримку дубльованих підтверджень, щоб дати час локальним механізмам відновлення відпрацювати.

При оцінці схем покращення TCP слід враховувати наступні ключові фактори:

1. Сумісність з існуючою інфраструктурою.

Ідеальне рішення не повинно вимагати модифікацій проміжних маршрутизаторів або відправника. Підходи, що розділяють з'єднання (I-TCP, MTCP), вимагають значних змін на базовій станції.

2. Обробка зашифрованого трафіку.

З поширенням технологій безпеки (наприклад, IPsec в IPv6), проміжні вузли не зможуть аналізувати TCP-заголовки, що робить неефективними рішення типу Snoop, I-TCP та MTCP.

3. Асиметричні маршрути.

У випадках, коли дані та підтвердження йдуть різними шляхами, схеми, що покладаються на проміжного агента, функціонуватимуть некоректно.

4. Дотримання наскрізної семантики.

I-TCP та MTCP порушують принцип наскрізного (end-to-end) TCP-з'єднання.

5. Проблема "вузького місця".

Проміжні агенти (базові станції) повинні буферизувати дані та виконувати додаткову обробку для кожного з'єднання, що може призвести до перевантаження. Крім того, передача стану з'єднання під час хендовера між базовими станціями створює значні накладні витрати.

3.1.3. Ключовий принцип Freeze-TCP

Ключовий принцип Freeze-TCP полягає у перенесенні відповідальності за сигналізацію про ймовірне роз'єднання на клієнтський вузол. Мобільний вузол здатний моніторити рівень сигналу та передбачати тимчасове роз'єднання. У такому випадку він може проактивно оголосити нульовий розмір вікна (Zero Window Advertisement, ZWA), щоб змусити відправника перейти в режим ZWP і запобігти зменшенню вікна перевантаження. Це рішення вимагає модифікації TCP-стека лише на стороні клієнта.

Обґрунтованим вибором для періоду попередження є час кругового затримання (RTT), що дозволяє ZWA-повідомленню гарантовано досягти відправника до моменту роз'єднання.

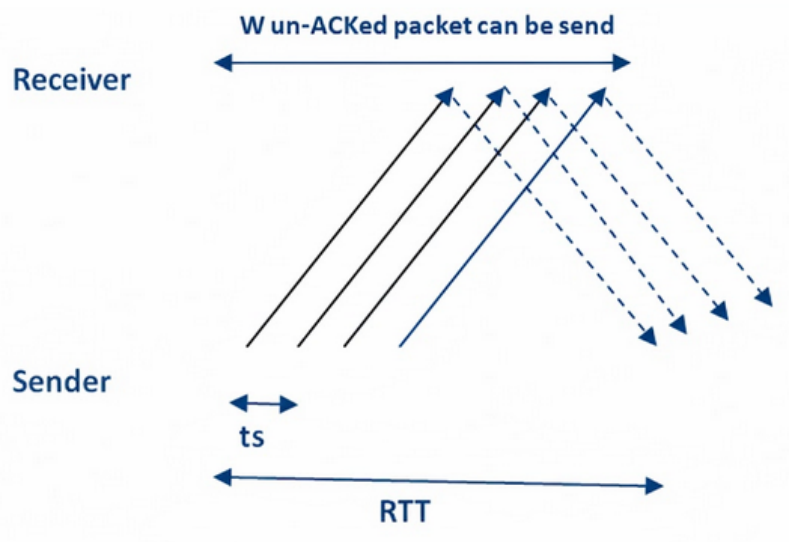

Рис. 3.3. Співвідношення між ts, RTT та W

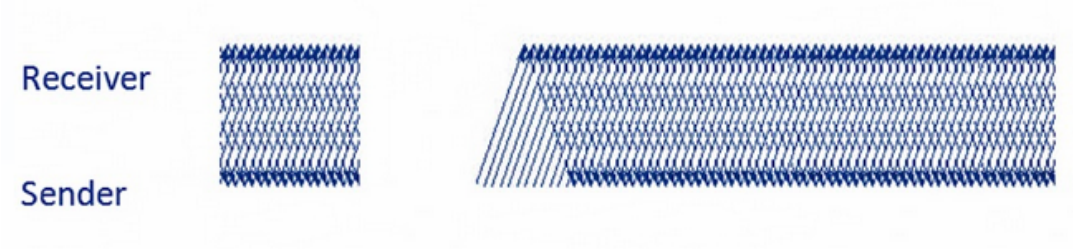

Рис. 3.4. Принцип роботи Freeze-TCP

Для уникнення простою після відновлення з'єднання (через експоненційне збільшення інтервалу ZWP), клієнт після повторного підключення надсилає три копії підтвердження для останнього отриманого сегмента (Triplicate Reconnection ACKs, TR-ACKs).

Аналіз продуктивності (рис. 3.16 та 3.17) показує, що для повного використання пропускної здатності каналу необхідно, щоб виконувалася умова:

$$W \cdot t_s \geq RTT$$

де W — розмір вікна, а ts — час передачі одного пакета.

При виконанні цієї умови, Freeze-TCP запобігає падінню вікна перевантаження. Приблизна кількість додаткових сегментів, переданих завдяки Freeze-TCP, описується виразом:

$$\text{Додаткові сегменти} \approx \frac{W^2}{8} + W \lg W - \frac{5W}{4} + 1$$

Цей вираз базується на моделі повільного старту та уникнення перевантаження стандартного TCP.

Freeze-TCP — це схема міграції з'єднання, яка дозволяє мобільному хосту "заморозити" TCP-з'єднання під час передачі обслуговування шляхом оголошення нульового вікна та "розморозити" його після завершення. Цей підхід зменшує втрати пакетів ціною потенційного збільшення затримки.

Важливо, що це наскрізна (end-to-end) схема, яка не вимагає участі проміжних вузлів. Freeze-TCP орієнтований виключно на міграцію з'єднання і може бути використаний у комплексі з іншими протоколами для реалізації повноцінної системи управління мобільністю.

3.2. Представлення підходу на основі транспортного протоколу M-TCP для забезпечення безперервності сервісу для stateful-застосунків

З метою реалізації кооперативної моделі для забезпечення безперервності сервісу було розроблено протокол міграційний TCP (M-TCP) — надійний транспортний протокол, орієнтований на з'єднання, який підтримує ефективну міграцію активних сесій. Протокол надає можливість серверам, що зберігають стан (stateful), безшовно відновлювати обслуговування на мігруючих з'єднаннях шляхом передачі визначеного обсягу стану, контрольованого на рівні застосунку. Хоча раніше пропонувалися рішення для дрібнозернистої міграції з'єднань з використанням специфіки протоколів прикладного рівня, таких як HTTP, наскільки відомо авторам, M-TCP є першим у своєму роді рішенням, що надає універсальну підтримку міграції через сумісний з TCP транспортний протокол.

3.2.1. Архітектура протоколу

Архітектура M-TCP базується на припущенні, що стан серверного застосунку може бути логічно розділений між з'єднаннями шляхом визначення дрібнозернистого стану, асоційованого з кожною сесією. Інтерфейс сервісу M-TCP, по суті, є контрактом між прикладним процесом сервера та транспортним протоколом. Відповідно до цього контракту, застосунок зобов'язаний виконувати наступні функції:

- Експортувати знімок стану (snapshot) на вихідному сервері в момент, коли цей стан узгоджений з потоком даних, надісланих/отриманих у рамках з'єднання.

- Імпортувати останній знімок стану на цільовому сервері після міграції для відновлення обслуговування клієнта.

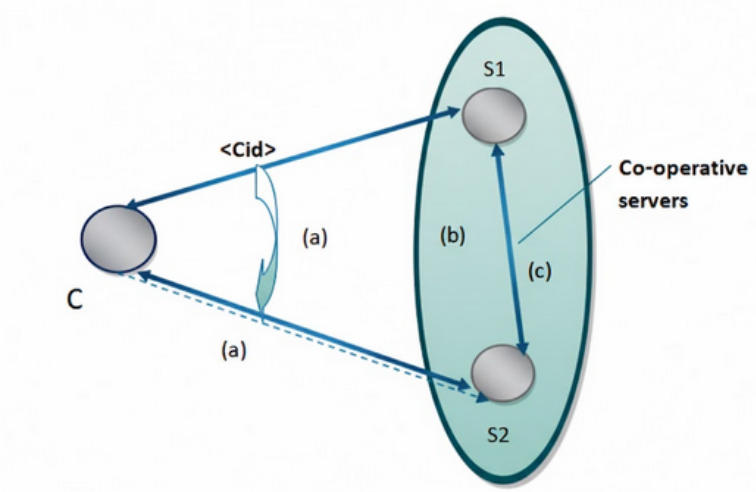

Рис. 3.5. Механізм міграції у протоколі M-TCP

Механізм міграції M-TCP (рис. 3.5) гарантує, що новий сервер відновлює обслуговування, зберігаючи семантику доставки «точно один раз» (exactly-once) протягом усього процесу міграції, без призупинення ("заморозки") чи іншого переривання трафіку. При цьому клієнтський застосунок не потребує жодних модифікацій.

Процес міграції виглядає наступним чином: клієнт взаємодіє із сервісом через з'єднання Cid до сервера S1. Під час встановлення з'єднання S1 надає адреси своїх кооперативних серверів разом із сертифікатами міграції. Клієнтська сторона M-TCP ініціює міграцію Cid, відкриваючи нове з'єднання до альтернативного сервера S2 та передаючи сертифікат у спеціалізованій опції. Для реконструкції з'єднання Cid на S2, M-TCP передає асоційований стан (стан протоколу та останній знімок) з S1.

Залежно від стратегії реалізації, передача стану може бути:

- Реактивною (лінивою), що ініціюється за запитом (on-demand) у момент міграції.

- Проактивною (завчасна), що виконується в очікуванні міграції (наприклад, при створенні нового знімка стану).

На рисунку 3.5 ілюстровано реактивний варіант передачі: S2 надсилає запит (b) до S1 і отримує стан (c). Після успішного відновлення мігруючої кінцевої точки на S2, клієнт C та сервер S2 завершують процедуру квитування (handshake), що фіналізує міграцію (d). Після цього серверний застосунок на S2 імпортує знімок стану і відновлює сервіс, використовуючи його як точку відновлення. Для повної синхронізації стану M-TCP веде журнал та передає з S1 дані, отримані та підтверджені з моменту останнього знімка, а також непідтверджені дані для повторної передачі з S2.

3.2.2. Сценарії застосування та реалізація

Прототип M-TCP було реалізовано в середовищі FreeBSD як розширення стека TCP/IP, повністю сумісне зі стандартним TCP. Архітектура M-TCP відокремлена від політик міграції, що дозволяє інтегрувати її з різними стратегіями. Визначено два класи сервісів, для яких застосування M-TCP є найбільш доцільним:

- застосунки, що використовують довготривалі з'єднання, такі як сервіси потокового мультимедіа або критичні процеси в ядрі Інтернету.

- критично важливі застосунки, що вимагають одночасно коректності та високої швидкості відгуку, наприклад, онлайн-банкінг.

Для демонстрації потенціалу M-TCP було реалізовано та оцінено два прикладних застосунки. Перший — універсальний сервер потокового мультимедіа, де міграція ініціюється, коли продуктивність на стороні клієнта падає нижче певного порогу. Результати показують, що M-TCP здатний підтримувати стабільно високу продуктивність шляхом динамічної міграції з'єднання між серверами. Другий застосунок — система віддаленого доступу до транзакційної бази даних на основі PostgreSQL. Отримана система

дозволяє клієнту розпочати послідовність транзакцій на одному frontend-сервері, а потім безшовно мігрувати та продовжити виконання на іншому. При цьому гарантується збереження семантики ACID та детерміноване виконання транзакцій протягом усього процесу міграції.

3.3. Фундаментальні аспекти та критерії оцінки схем управління мобільністю

Комплексні схеми управління мобільністю включають три фундаментальні компоненти: передачу обслуговування (handover), міграцію з'єднання та управління місцезнаходженням. Для порівняльного аналізу ефективності таких схем необхідно розробити систему критеріїв оцінки. До складу цих критеріїв можуть бути включені такі параметри, як затримка та втрата пакетів під час передачі обслуговування, відмовостійкість, вимоги до модифікації мережевої інфраструктури, тип підтримуваної мобільності, сумісність з різними версіями IP, безпека та масштабованість. У даній роботі зазначені критерії використовуються для класифікації та аналізу запропонованих архітектур мобільності. Управління мобільністю в комп'ютерних мережах визначається як процес, що забезпечує нерозривність з'єднання при зміні мобільним хостом (MH) точки підключення до мережі, що, як правило, супроводжується зміною його IP-адреси. Зміна IP-адреси породжує низку технічних проблем, пов'язаних із підтримкою безперервності потоку даних, мінімізацією втрат пакетів, забезпеченням безпеки та ідентифікацією нового місцезнаходження хоста.

3.3.1. Міграція з'єднання

Коли мобільний хост (MH) змінює свою підмережу, він отримує нову IP-адресу. Це породжує проблему збереження комунікації між ним та відповідним хостом (CN), оскільки MH тепер може бути асоційований з кількома IP-адресами. Міграція з'єднання є одним із можливих рішень, що

передбачає сповіщення CN про зміну адреси та перенесення активного з'єднання зі старої IP-адреси на нову. Для уникнення маршрутизації даних через застарілу адресу цей процес може вимагати тимчасового призупинення потоку даних. Для обробки перемикання з'єднання може бути залучений проміжний шлюз. Деякі сучасні протоколи підтримують множинні IP-адреси для одного MH з кількома інтерфейсами, що забезпечує плавну передачу обслуговування при зміні підмереж. Якщо MH та базові протоколи не підтримують множинні адреси, після отримання нової IP-адреси MH стає доступним виключно за нею. Це призводить до неможливості доставки пакетів, адресованих на стару IP-адресу, що спричиняє їх втрату, збільшення затримки та неефективне використання мережевих ресурсів. Архітектури мобільності повинні включати механізми для мінімізації цих негативних ефектів під час передачі обслуговування.

3.3.2. Вимоги до інфраструктури

Архітектура Інтернету на початкових етапах не передбачала підтримки мобільності. Внаслідок цього значна кількість запропонованих схем вимагає внесення змін до існуючої мережевої інфраструктури, наприклад, впровадження спеціалізованих шлюзів або проксі-серверів для забезпечення функціонування мобільних з'єднань.

Після зміни IP-адреси MH, відповідний хост (CN) повинен мати механізм для його локалізації. Менеджер місцезнаходження — це системний компонент, який відстежує актуальну IP-адресу MH і надає її будь-якому суб'єкту, що ініціює комунікацію з мобільним хостом.

3.4. Критерії оцінки архітектур управління мобільністю

Процес передачі обслуговування ініціюється, коли мобільний хост (MH), керуючись показниками рівня сигналу, приймає рішення про від'єднання від поточної підмережі та підключення до нової. У результаті MH

отримує нову IP-адресу. Дані, що знаходяться в процесі передачі на попередню IP-адресу, піддаються ризику втрати, що призводить до збільшення загальної затримки через необхідність їх повторної передачі. Процес передачі обслуговування може вимагати, щоб прикладні процеси на MH та відповідному хості (CN) були адаптовані до умов мобільності, що знижує рівень прозорості для застосунків. Крім того, міграція між підмережами може створювати конфлікти з існуючими політиками мережевої безпеки та вимагати розгортання додаткового апаратного чи програмного забезпечення в мережевій інфраструктурі.

3.4.1. Типи передачі обслуговування

Продуктивність схеми управління мобільністю значною мірою залежить від типу реалізованої передачі обслуговування, яка класифікується як жорстка (hard handoff) або м'яка (soft handoff). М'яка передача, також відома як безшовна, забезпечує плавний перехід, дозволяючи мобільному пристрою підтримувати комунікацію через декілька мережевих інтерфейсів одночасно протягом процесу міграції.

3.4.2. Масштабованість та відмовостійкість

Масштабованість характеризує здатність архітектури управління мобільністю ефективно обробляти велику кількість мобільних (MH) та відповідних (CN) хостів. Схема вважається масштабованою, якщо її продуктивність не деградує зі збільшенням розміру мережі. Відмовостійкість визначає здатність системи зберігати функціональність в умовах збоїв її компонентів. Наприклад, архітектура з єдиною точкою відмови (single point of failure) не є відмовостійкою.

3.4.3. Вимоги до модифікації протоколів

Схеми управління мобільністю, реалізовані на транспортному рівні, можуть вимагати модифікації існуючих транспортних протоколів або

впровадження нових протоколів та відповідних програмних інтерфейсів (API) на рівні застосунків.

3.4.4. Сумісність із політиками безпеки

Багато стандартних рішень безпеки, таких як пакетна фільтрація на вхід (ingress filtering) та міжмережеві екрани, обмежують або унеможливлюють маніпуляції із заголовками пакетів на проміжних вузлах. Це може створювати конфлікти з деякими схемами мобільності, які вимагають такої інспекції або модифікації пакетів.

3.4.5. Прозорість для застосунків

Схема управління мобільністю вважається прозорою для застосунків, якщо прикладний рівень не потребує інформації про процеси передачі обслуговування, що відбуваються на нижчих рівнях стека протоколів, і, відповідно, не вимагає модифікації коду застосунків.

3.4.6. Проблема втрати пакетів та затримки

Під час передачі обслуговування транзитні пакети можуть не бути доставлені до МН. Це не лише призводить до їх втрати та збільшення затримки, але й може помилково інтерпретуватися протоколами транспортного рівня (наприклад, TCP) як ознака мережевого перевантаження, що викликає невиправдане зниження швидкості передачі.

3.4.7. IP-різноманіття

Сучасні мобільні пристрої все частіше оснащуються декількома комунікаційними інтерфейсами. Під час передачі обслуговування МН може утилізувати переваги наявності декількох IP-адрес (IP-різноманіття), отриманих від різних підмереж через ці інтерфейси, для забезпечення більш надійного та плавного переходу.

3.4.8. Вимоги до модифікації інфраструктури

Реалізація схеми управління мобільністю може вимагати розгортання додаткових програмних агентів (наприклад, домашнього та іноземного агентів у Mobile IP) або спеціалізованого апаратного забезпечення в існуючій мережевій інфраструктурі, що може ускладнити її практичне впровадження та масштабування.

3.5. Порівняльний аналіз схем управління мобільністю на транспортному рівні

У цьому розділі представлено порівняльний аналіз ключових архітектур управління мобільністю, реалізованих на транспортному рівні. Кожна схема оцінюється за такими критеріями, як механізм міграції, тип передачі обслуговування, управління місцезнаходженням, відмовостійкість та вимоги до модифікації інфраструктури.

3.5.1. Особливості архітектури SIGMA

SIGMA є комплексною архітектурою управління мобільністю, що функціонує на транспортному рівні та підтримує м'яку передачу обслуговування на основі IP-різноманіття. Коли МН входить у зону перекриття двох підмереж, він отримує нову IP-адресу, зберігаючи стару як основну. При послабленні сигналу від початкової мережі, МН перемикає свою основну адресу на нову, забезпечуючи безшовний перехід. Управління місцезнаходженням реалізовано через динамічне оновлення DNS-записів, що обґрунтовано використанням DNS на початковому етапі більшості інтернет-сесій.

Це мінімізує втрати пакетів, однак відмова менеджера місцезнаходження (DNS-сервера) унеможливлює встановлення нових з'єднань. Схема не вимагає змін інфраструктури, але передбачає модифікацію стека протоколів.

3.5.2. Протокол MSOCKS

Протокол MSOCKS реалізує розділення TCP-з'єднання (TCP Splice) на проксі-сервері, трансформуючи одну сесію "хост-хост" у дві: "хост-проксі" та "проксі-хост". Міграція з'єднання відбувається шляхом встановлення нового каналу зв'язку між мобільним хостом (MH) та проксі при зміні підмережі, що відповідає механізму жорсткої передачі обслуговування. При цьому з'єднання між проксі та відповідним хостом (CN) залишається незмінним, забезпечуючи прозорість мобільності для CN. Управління місцезнаходженням централізоване на проксі, що обмежує мобільність його зоною покриття. Основним недоліком є наявність єдиної точки відмови: збій проксі-сервера призводить до повної відмови системи. Реалізація вимагає модифікації як мережевої інфраструктури, так і стека протоколів.

3.5.3. Архітектура Migrate TCP

Дана архітектура базується на механізмі міграції з'єднання з використанням ідентифікаційних токенів, що обмінюються між кінцевими вузлами на етапі встановлення сесії. Протокол реалізує жорстку передачу обслуговування, під час якої MH відновлює раніше встановлене з'єднання за допомогою токена. Аналогічно до SIGMA, для управління місцезнаходженням пропонується використовувати DNS. Ключовою перевагою є уникнення передачі даних під час міграції, що запобігає втраті пакетів. Схема не вимагає змін інфраструктури, проте потребує модифікації стека протоколів на CN.

3.5.4. Протоколи RCP та R²CP

RCP є протоколом, що реалізує парадигму керування на стороні отримувача, переносячи відповідальність за контроль перевантаження та надійність з відправника на отримувача. Це дозволяє більш ефективно управляти передачею даних у динамічних мережевих умовах. Протокол

підтримує м'яку передачу обслуговування, сумісний з політиками безпеки та утилізує IP-різноманіття. Його логічним розвитком є протокол R²CP.

R²CP є розширенням протоколу RCP, спеціально адаптованим для гетерогенних бездротових середовищ. Базуючись на принципі керування на стороні отримувача, R²CP додає підтримку множинних станів, що дозволяє одночасно використовувати декілька мережевих інтерфейсів. Це забезпечує ефективну м'яку передачу обслуговування та агрегацію пропускної здатності. Протокол сумісний з політиками безпеки, підтримує IP-різноманіття та не вимагає модифікації мережевої інфраструктури.

3.5.5. Схема міграції Freeze-TCP

Freeze-TCP є схемою міграції з'єднання, що дозволяє MH тимчасово "заморозити" існуючу TCP-сесію шляхом оголошення нульового розміру вікна. Це запобігає відправці нових даних з боку CN під час жорсткої передачі обслуговування. Після успішного підключення до нової мережі з'єднання "розморожується". Такий підхід мінімізує втрати пакетів, однак може збільшувати загальну затримку. Freeze-TCP є вузькоспеціалізованим рішенням для міграції і не охоплює управління місцезнаходженням, але може інтегруватися з іншими системами. Вимагає модифікації стека протоколів на кінцевих вузлах, але не зачіпає інфраструктуру.

3.6. Представлення таксономії архітектур мобільності на транспортному рівні

Архітектури управління мобільністю, розглянуті раніше, можуть бути класифіковані на основі їхнього фундаментального підходу до реалізації мобільності.

Пропонується таксономія, що включає чотири основні категорії, які узагальнено в таблиці 3.1 та детально описано нижче.

3.6.1. Протоколи, орієнтовані на передачу обслуговування

Схеми цієї категорії не є комплексними системами управління мобільністю, а є розширеннями транспортних протоколів, спрямованими на оптимізацію процесу передачі обслуговування (handover). Їх головна мета — мінімізація затримки та втрати даних під час переходу хоста між мережами. До цього класу належать R²CP, MMSP, mSCTP, які утилізують IP-різноманіття для реалізації безшовної передачі. Обмеженість цих рішень полягає у відсутності вбудованих компонентів, таких як управління місцезнаходженням.

3.6.2. Протоколи, орієнтовані на міграцію з'єднання

Архітектури цього класу базуються на механізмі міграції з'єднання, який передбачає тимчасове призупинення сесії на час передачі обслуговування з подальшим її відновленням. Це забезпечує нерозривність з'єднання між відповідним (CN) та мобільним (MH) хостами, однак не вирішує безпосередньо проблем оптимізації самого процесу хендовера. Прикладами є Freeze-TCP та TCP-R, які розширюють функціональність TCP, дозволяючи "заморожувати" та "розморожувати" з'єднання до та після міграції відповідно.

3.6.3. Архітектури на основі шлюзу

Даний клас схем реалізує мобільність шляхом впровадження спеціалізованого шлюзу в мережеву інфраструктуру. З'єднання між CN та MH розділяється на цьому шлюзі на два сегменти. Сегмент "шлюз-CN" залишається статичним, тоді як сегмент "MH-шлюз" може динамічно змінюватися при переміщенні хоста. Протоколи MSOCKS, I-TCP, M-TCP, M-UDP та BARWAN належать до цієї категорії і вимагають наявності проміжних сутностей для розділення з'єднання. Вони не надають комплексних рішень для управління місцезнаходженням.

3.6.4. Комплексні архітектури управління мобільністю

Схеми цієї категорії є повноцінними наскрізними (end-to-end) системами управління мобільністю, реалізованими на транспортному рівні. Вони інтегрують усі необхідні компоненти, включаючи механізми передачі обслуговування та управління місцезнаходженням. До цієї групи належать Migrate TCP та SIGMA.

Таблиця 3.1.

Класифікація архітектур мобільності на транспортному рівні

Клас	**Опис**	**Приклад**
Протокол передачі обслуговування	Транспортний протокол, який має функції для підтримки мобільності	R²CP, MMSP, mSCTP
Протокол міграції з'єднання	Транспортний протокол, який може мігрувати декілька з'єднань	Freeze TCP, TCP-R
Схема мобільності на основі шлюзу	Надає мобільність, розміщуючи інфраструктуру між CN та MH та розділяючи з'єднання	MSOCKS, I-TCP, M-TCP, M-UDP, BARWAN
Менеджер мобільності	Повні схеми мобільності з передачею обслуговування та управлінням розташуванням	Migrate TCP та SIGMA

3.7. Підсумкова оцінка архітектур управління мобільністю на транспортному рівні

На основі представленого аналізу проведено порівняльну оцінку розглянутих протоколів управління мобільністю на транспортному рівні за ключовими критеріями, такими як тип передачі обслуговування, рівень втрат пакетів та затримки, відмовостійкість, вимоги до модифікації інфраструктури та стека протоколів, а також підтримка IP-різноманіття.

Ключові висновки порівняння є наступними.

- Тип передачі обслуговування. Протоколи MSOCKS та M-TCP реалізують механізм жорсткого хендовера, тоді як RCP та R²CP підтримують більш досконалу м'яку (безшовну) передачу.

- Продуктивність (втрати/затримка). Архітектури SIGMA, RCP та R²CP демонструють мінімальний рівень втрат пакетів. На противагу цьому, в MSOCKS пакети, що знаходяться в транзиті, втрачаються під час міграції, а Freeze-TCP мінімізує втрати ціною повного призупинення передачі даних.

- Відмовостійкість. Протоколи RCP та R²CP характеризуються високою відмовостійкістю. Системи, що залежать від централізованих компонентів, є більш вразливими: відмова проксі-сервера в MSOCKS призводить до повного розриву з'єднання, а збій менеджера місцезнаходження в SIGMA унеможливлює встановлення нових сесій.

- Вимоги до розгортання. MSOCKS та RCP вимагають модифікації мережевої інфраструктури, тоді як інші розглянуті протоколи можуть функціонувати без таких змін.

- Підтримка IP-різноманіття. Ця функціональність, що є ключовою для сучасних мобільних пристроїв, реалізована в SIGMA, RCP та R²CP.

Узагальнені результати порівняльного аналізу за всіма розглянутими критеріями детально представлені в таблиці 3.2.

Таблиця 3.2.

Порівняння протоколів за різними критеріями

Критерій	**MSOCKS**	**SIGMA**	**Migrate TCP**	**Freeze TCP**	**RCP**	**R²CP**
Тип передачі обслуговування	Жорстка	М'яка	М'яка	Жорстка	М'яка	М'яка
Втрата пакетів	Низька	Дуже низька	Дуже низька	Висока	Низька	Дуже низька
Затримка	Низька	Дуже низька	Дуже низька	Висока	Низька	Дуже низька

Критерій	MSOCKS	SIGMA	Migrate TCP	Freeze TCP	RCP	R²CP
Масштабованість	Низька	Висока	Висока	Висока	Висока	Висока
Стійкість до збоїв	Низька	Висока	Висока	Висока	Висока	Висока
Прозорість застосунку	Так	Так	Так	Так	Так	Так
Підтримка IP-різноманітності	Ні	Так	Ні	Ні	Так	Так
Зміна інфраструктури	Так	Ні	Ні	Ні	Так	Ні
Зміна протоколу	Так	Так	Так	Так	Так	Так

Отже, було проведено комплексне дослідження та порівняльний аналіз протоколів управління мобільністю на транспортному рівні. На основі розроблених критеріїв було виконано класифікацію та оцінку ефективності розглянутих архітектур.

Встановлено, що кожна архітектура характеризується унікальним набором переваг та обмежень, відтак вибір оптимального рішення зумовлений специфічними вимогами застосунку та особливостями мережевої інфраструктури. Зокрема, протоколи SIGMA та R²CP демонструють найвищу ефективність у сценаріях, що вимагають м'якої (безшовної) передачі обслуговування та мінімізації втрат пакетів. Натомість рішення на кшталт MSOCKS або Freeze-TCP можуть бути доцільними за умов, де допустимі відповідні модифікації інфраструктури або протокольного стека.

Висновки до розділу

У третьому розділі представлено методи та архітектури управління мобільністю на транспортному рівні, а також здійснено порівняння підходів Freeze-TCP, M-TCP, SIGMA, RCP та інших схем. Проаналізовано проблеми роботи TCP у мобільних середовищах, визначено шляхи їх усунення за допомогою наскрізних механізмів адаптації. Обґрунтовано переваги транспортного підходу до мобільності над мережевими рішеннями з погляду

прозорості, надійності та мінімізації затримок. Сформовано критерії оцінки архітектур мобільності – від вимог до інфраструктури до підтримки безпеки й відмовостійкості. Підсумковий аналіз дозволив узагальнити характеристики основних протоколів та побудувати таксономію транспортних схем мобільності, що відображає тенденції розвитку сучасних протоколів і перспективи їх використання в системах нового покоління.

ВИСНОВКИ

У результаті виконання магістерської роботи на тему «Порівняльний аналіз транспортних рівнів мобільних протоколів» було здійснено комплексне дослідження теоретичних, методологічних та практичних аспектів забезпечення мобільності в мережах на транспортному рівні. Робота спрямована на систематизацію знань про архітектури, механізми та критерії ефективності сучасних транспортних протоколів мобільності, а також на порівняльну оцінку їх можливостей у контексті забезпечення безперервності з'єднань, оптимізації передачі даних і підтримки гетерогенних середовищ зв'язку.

На основі проведеного аналізу визначено, що традиційні підходи до управління мобільністю, зосереджені на мережевому рівні (зокрема Mobile IP та його похідні), не завжди здатні забезпечити необхідний рівень адаптивності та продуктивності в умовах високої динаміки мережевих підключень і зростаючих вимог до якості сервісу. У цьому контексті транспортний рівень виступає більш гнучким середовищем для реалізації механізмів мобільності завдяки своїй близькості до прикладних процесів і можливості враховувати специфіку конкретних застосунків.

У роботі досліджено архітектуру, принципи функціонування та ефективність низки протоколів транспортного рівня — MSOCKS, SIGMA, RCP, R²CP, M-TCP, Freeze-TCP. Для кожного з них визначено ключові функціональні характеристики, переваги та недоліки, зокрема в аспектах управління з'єднаннями, контролю перевантаження, забезпечення надійності та підтримки безшовної передачі обслуговування (handover). Особливу увагу приділено питанням масштабованості, відмовостійкості, прозорості для застосунків і відповідності вимогам безпеки.

Проведений порівняльний аналіз продемонстрував, що:

- SIGMA забезпечує високу гнучкість і низькі затримки під час handover завдяки використанню множинних IP-адрес;

- MSOCKS орієнтований на проксі-архітектуру, що забезпечує сумісність із наявними застосунками, проте знижує ефективність у масштабних середовищах;

- RCP і R²CP характеризуються покращеними механізмами контролю перевантаження та здатністю до адаптації в гетерогенних мережах;

- Freeze-TCP і M-TCP представляють наскрізні підходи до збереження стану з'єднань у разі переривань, що робить їх ефективними для мобільних середовищ із високою варіативністю каналів зв'язку.

Сформовано таксономію транспортних протоколів мобільності, що класифікує їх за принципами архітектури (орієнтовані на передачу обслуговування, на міграцію з'єднань, на шлюзові рішення та комплексні схеми). Така систематизація дозволяє визначити оптимальні підходи для різних сценаріїв застосування — від мобільних IoT-пристроїв до високопродуктивних мультимедійних сервісів.

Наукова новизна отриманих результатів полягає у вдосконаленні підходів до порівняльної оцінки транспортних протоколів мобільності з урахуванням критеріїв адаптивності, прозорості, надійності та ресурсної ефективності. Практичне значення роботи полягає у можливості використання сформованих висновків і класифікаційних моделей при проектуванні сучасних систем передачі даних, розробці архітектур для мобільних мереж нового покоління (5G/6G), а також у створенні прототипів транспортних протоколів із підтримкою багатоінтерфейсної мобільності.

У підсумку, проведене дослідження підтверджує, що транспортний рівень має значний потенціал для подальшого розвитку механізмів мобільності, здатних забезпечити високу якість обслуговування, безперервність сеансів і ефективне використання мережевих ресурсів у динамічних мобільних середовищах.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. RCP, experimental packet-switched data transmission service. – https://rogerdmoore.ca/blog/rcp
2. Goff, T., Ponec, J., F. F. Kuo, & J. F. C. (2000). Freeze-TCP: a true end-to-end TCP enhancement for mobile environments. Proceedings of IEEE INFOCOM 2000, 3, 1537-1545.
3. Snoeren, A. C., Balakrishnan, H., & Kaashoek, M. F. (2001). Fine-grained failover using connection migration. Proceedings of the 3rd USENIX Symposium on Internet Technologies and Systems (USITS '01).
4. Balakrishnan, H., Padmanabhan, V. N., Seshan, S., & Katz, R. H. (1997). A comparison of mechanisms for improving TCP performance over wireless links. IEEE/ACM Transactions on Networking, 5(6), 756-769.
5. Bakre, A. J., & Badrinath, B. R. (1995). I-TCP: Indirect TCP for mobile hosts. Proceedings of the 15th International Conference on Distributed Computing Systems, 136-143.
6. Maltz, D. A., & Bhagwat, P. (1998). MSOCKS: An architecture for transport layer mobility. Proceedings of IEEE INFOCOM '98, 3, 1037-1045.
7. Fikouras, N. A., et al. (2002). SIGMA: a seamless mobility architecture for connection-oriented transport protocols. Technical Report, Columbia University.
8. Yang, Y., & Kravets, R. (2005). R²CP: a receiver-driven and router-assisted transport protocol for wireless networks. Proceedings of the 11th annual international conference on Mobile computing and networking (MobiCom '05), 154-167.
9. Perkins, C. (Ed.). (2002). IP Mobility Support for IPv4. RFC 3344, IETF.
10. Stewart, R., et al. (2007). Stream Control Transmission Protocol. RFC 4960, IETF.

11. Hsieh, H. Y., & Sivakumar, R. (2003). A transport layer approach for achieving richer mobility in the Internet. IEEE Transactions on Mobile Computing, 2(3), 213-227.
12. Caceres, R., & Iftode, L. (1994). Improving the performance of reliable transport protocols in mobile computing environments. IEEE Journal on Selected Areas in Communications, 13(5), 850-857.
13. Akyildiz, I. F., Xie, J., & Mohanty, S. (2004). A survey of mobility management in next-generation all-IP-based wireless systems. IEEE Wireless Communications, 11(4), 16-28.
14. Brown, K., & Singh, S. (1997). M-TCP: TCP for mobile cellular networks. ACM SIGCOMM Computer Communication Review, 27(5), 19-43.
15. Fu, S., Atiquzzaman, M., & Ma, L. (2006). A survey of transport layer protocols for wireless networks. IEEE Communications Surveys & Tutorials, 8(3), 48-61.
16. Yavatkar, R., & Bhagwat, P. (1994). Improving end-to-end performance of TCP over mobile internetworks. Proceedings of the Workshop on Mobile Computing Systems and Applications.
17. Jacobson, V. (1988). Congestion avoidance and control. ACM SIGCOMM Computer Communication Review, 18(4), 314-329.
18. Fall, K., & Floyd, S. (1996). Simulation-based comparisons of Tahoe, Reno and SACK TCP. ACM SIGCOMM Computer Communication Review, 26(3), 5-21.
19. Lee, Y. K., et al. (2003). mSCTP: a multi-homed SCTP for mobile hosts. ACM SIGCOMM Computer Communication Review, 33(5), 33-46.
20. Snoeren, A. C., & Balakrishnan, H. (2000). An end-to-end approach to host mobility. Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom '00), 155-166.
21. Brewer, E. A., et al. (1998). A network architecture for heterogeneous mobile computing. IEEE Personal Communications, 5(5), 8-24.

22. Held, A., & Pralay, M. (2002). Migratory TCP: Connection migration for service continuity in the internet. Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops.
23. Chen, W., et al. (2007). MMSP: A multi-path multi-stream transport protocol for mobile Internet. Proceedings of IEEE INFOCOM 2007, 1860-1868.
24. Valko, A. G. (1999). Cellular IP: a new approach to Internet host mobility. ACM SIGCOMM Computer Communication Review, 29(1), 50-65.
25. Ramjee, R., et al. (1999). HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks. Proceedings of the International Conference on Network Protocols.
26. Ghosh, A., Wolter, D. R., Andrews, J. G., & Chen, R. (2010). Broadband wireless access with WiMAX/802.16: current performance benchmarks and future potential. IEEE Communications Magazine, 48(2), 129-136.
27. Ford, A., Raiciu, C., Handley, M., & Barre, S. (2011). Architectural guidelines for multipath TCP development. RFC 6182, IETF.
28. Chakravorty, R., Cartwright, J., & Pratt, I. (2002). Practical experience with TCP over GPRS. Proceedings of the IEEE GLOBECOM.
29. Wu, C. S., & Chen, G. Y. (1999). A seamless handoff approach for mobile IP. IEEE Personal Communications, 6(3), 32-39.
30. Xylomenos, G., Polyzos, G. C., et al. (2001). TCP performance issues over wireless links. IEEE Communications Magazine, 39(4), 52-58.
31. Casetti, C., Gerla, M., Mascolo, S., Sanadidi, M. Y., & Wang, R. (2002). TCP Westwood: End-to-end congestion control for wired/wireless networks. IEEE/ACM Transactions on Networking, 10(4), 467-479.
32. Bar-Noy, A., Kessler, I., & Sidi, M. (1995). Mobile users: To update or not to update? Wireless Networks, 1(2), 175-185.
33. Papademetriou, A., et al. (2010). The design of the mobility support in SCTP. Internet-Draft, IETF.

34. Sun, X., & Sou, K. C. (2002). Mobile-TCP: A new TCP protocol for mobile communications. Proceedings of the IEEE International Conference on Communications.
35. Lee, J. H., & Kim, J. H. (2004). An end-to-end seamless handoff scheme for mobile IP based on connection migration. Proceedings of the IEEE Vehicular Technology Conference.
36. Stemm, M., & Katz, R. H. (1998). Vertical handoffs in wireless overlay networks. Mobile Networks and Applications, 3(3), 335-350.
37. Banga, G., Druschel, P., & Mogul, J. C. (1999). Better operating system features for faster network servers. Proceedings of the Workshop on Hot Topics in Operating Systems.
38. Rizzo, L. (1997). A reliable multicast data distribution protocol based on software FEC. Technical Report, University of Pisa.
39. Haddad, W., & Madhukumar, A. S. (2005). A survey on transport layer protocols for heterogeneous wireless networks. Proceedings of the International Conference on Information Technology: Coding and Computing.