

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
ТЕЛЕКОМУНІКАЦІЙ**

## **Пояснювальна записка**

до магістерської кваліфікаційної роботи

на тему: **“МЕТОДИ ОЦІНЮВАННЯ ПАРАМЕТРІВ МЕРЕЖІ ПЕРЕДАЧІ  
РІЗНОРІДНОГО МЕРЕЖНОГО ТРАФІКУ”**

Виконав: студент 6 курсу, групи ТСДМ-63  
спеціальності

172 Телекомунікації та радіотехніка

(шифр і назва спеціальності)

Фесенко П.О.

(прізвище та ініціали)

Керівник

Горбенко В.М.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтроль

(прізвище та ініціали)

Київ - 2019

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
ТЕЛЕКОМУНІКАЦІЙ

Кафедра Телекомунікаційних систем та мереж

Ступінь вищої освіти Магістр

Спеціальність 172 Телекомунікації та радіотехніка

(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

телекомунікаційних систем та мереж

В.Ф. Заїка

“ ”

\_\_\_\_\_ 2019 року

**З А В Д А Н Н Я**

**НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Фесенку Павлу Олександровичу

1. Тема роботи: “Методи оцінювання параметрів мережі передачі різнорідного мережного трафіку”,

керівник роботи Горбенко Володимир Михайлович, к.в.н., доцент,  
затверджені наказом вищого навчального закладу від 14.11.2019 №518.

2. Строк подання студентом роботи 20.12.2019 р.

3. Вихідні дані до роботи:

1. Безпроводові мережі.
2. Методи та засоби підтримки безпечного функціонування мережі.
3. Методи оцінювання показників продуктивності мережі з урахуванням завад
4. Науково-технічна література.

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

1. Аналітичний огляд і постановка задачі дослідження .
2. Розробка методів оцінки ключових параметрів безпроводової мережі при різних статистиках мережного трафіку.
3. Метод урахування взаємного впливу термінальних вузлів безпроводової мережі.
4. Методи оцінювання показників продуктивності мережі з урахуванням завад

5. Перелік графічного матеріалу (назва слайдів презентації):

1. Мета роботи;
2. Актуальність теми;
3. Безпроводові мережі з різними структурами;
4. Етапи діагностики мережі;
5. Методи оцінки КПЕ для аналізу комп'ютерних мереж;
6. Метод урахування взаємного впливу термінальних вузлів безпроводової мережі;
7. Методи оцінювання показників продуктивності мереж з урахуванням завад;
8. Результати розрахунків параметрів мережі з використанням комп'ютерної моделі;
9. Висновки.

6. Дата видачі завдання 11.09.2019

---

### КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	27.09.19	Викон.
2.	Аналітичний огляд і постановка задачі дослідження	15.10.19	Викон.
3.	Розробка методів оцінки ключових параметрів безпроводової мережі при різних статистиках мережного трафіку	31.10.19	Викон.
4.	Метод урахування взаємного впливу термінальних вузлів безпроводової мережі	15.11.19	Викон.
5.	Методи оцінювання показників продуктивності мережі з урахуванням завад	29.11.19	Викон.
6.	Висновки, вступ, реферат	10.12.19	Викон.
7.	Розробка презентації	18.12.19	Викон.

**Студент**

**Фесенко П.О.**

(підпис)

(прізвище та ініціали)

**Керівник роботи**

**Горбенко В.М.**

(підпис)

(прізвище та ініціали)

## РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 76 сторінок, 17 рисунків, 2 таблиці, 40 джерел.

*Об'єкт дослідження* – процес управління навантаженням на комп'ютерну мережу з різномірним трафіком.

*Предмет дослідження* – безпроводова комп'ютерна мережа з різномірним трафіком (мова, дані, відео), обладнанням комутації та керування, різними архітектурами і топологіями.

*Мета роботи* – дослідження принципів і методів управління навантаженням на комп'ютерну мережу з різномірним трафіком.

*Методи дослідження* – теорія масового обслуговування, методи цифрової обробки інформації та імітаційного моделювання.

У магістерській атестаційній роботі вирішені наступні основні задачі: проаналізований сучасний стан і перспективи розвитку безпроводових комп'ютерних мереж і методів оцінювання характеристик каналів передачі; розроблені математичні моделі безпроводових мереж як великих систем, що працюють за наявності зовнішніх завад; розроблені модифіковані методи оцінювання ключових параметрів безпроводової мережі з урахуванням самоподібної природи мережного трафіку; вдосконалено метод розрахунку поточного коефіцієнту використання мережі та контролю степеню самоподібності для запобігання неприпустимому перевантаженню мережі із-за колізій шляхом управління інтенсивністю мережного трафіку.

БЕЗПРОВОДОВА КОМП'ЮТЕРНА МЕРЕЖА, СПОТВОРЕННЯ, ТРАКТ, БЕЗПРОВОДОВІ МЕРЕЖІ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ, КЗІ, ОБЛАДНАННЯ КОМУТАЦІЇ, КЕРУВАННЯ, АРХІТЕКТУРА, ТОПОЛОГІЯ, МОДЕЛЬ, МЕТОДИ, БЕЗПЕКА.



## ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	10
1 АНАЛІТИЧНИЙ ОГЛЯД І ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ.....	13
1.1. Загальна проблема моніторингу та аналізу комп'ютерних мереж .....	13
1.2. Методи ідентифікації параметрів безпроводових мереж з різними структурами .....	19
1.3. Методи отримання інформації про сигнали та завади у мережі.....	22
2 ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ КЛЮЧОВИХ ПАРАМЕТРІВ БЕЗПРОВОДОВОЇ МЕРЕЖІ ПРИ РІЗНИХ СТАТИСТИКАХ МЕРЕЖНОГО ТРАФІКУ .....	28
2.1. Теоретичні засади застосування системи ключових показників ефективності для аналізу комп'ютерних мереж .....	28
2.2. Метод визначення середнього часу обслуговування пакету у мережі .....	31
3 МЕТОД УРАХУВАННЯ ВЗАЄМНОГО ВПЛИВУ ТЕРМІНАЛЬНИХ ВУЗЛІВ БЕЗПРОВОДОВОЇ МЕРЕЖІ.....	39
3.1. Ієрархічна модель безпроводової мережі.....	39
3.2. Метод оцінки середнього часу затримки пакету й імовірності відмови обслуговування.....	43
3.4. Методи врахування неоднорідності вхідних пакетів .....	45
4 МЕТОДИ ОЦІНЮВАННЯ ПОКАЗНИКІВ ПРОДУКТИВНОСТІ МЕРЕЖІ З УРАХУВАННЯМ ЗАВАД.....	56
4.1. Методика моделювання і аналізу результатів .....	56
4.2. Результати розрахунків параметрів мережі з використанням комп'ютерної моделі .....	63
4.3. Оцінка впливу завад на характеристики мережі.....	65
4.4. Розробка методу аналізу колізій у мережі з різнорідним трафіком .....	67
ВИСНОВКИ .....	71
ПЕРЕЛІК ПОСИЛАНЬ .....	73

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

АС	автономний сегмент;
АЧХ	амплітудно-частотна характеристика;
БЛМ	безпроводова локальна мережа
ГЧЗ	груповий час затримки
ВК	вузол комутації;
КПЕ	ключовий показник ефективності;
МСКП	критерій мінімуму середньоквадратичної помилки;
РВХ	розподіли з “важкими хвостами”;
СК	система керування;
ТАУ	теорія автоматичного керування.
ФЧХ	фазочастотна характеристика
ARED	Adaptive Random Early Detection, адаптивний алгоритм випадкового раннього виявлення;
CBQ	Class-Based Queuing, черга, основана на класах;
CMSIE	Common Management Information Service Element, елемент системи керування, що забезпечує доступ до керуючої інформації, яка зберігається в керованих об'єктах;
DiffServ	Differentiated Services, модель диференційованого обслуговування;
MPLS	Multiprotocol Label Switching, технологія багатопроTOCOLЬНОЇ комутації по мітках;
OSPF	Open Shortest Path First, протокол першочергового виявлення найкоротших маршрутів;
P-RED	PACKET-RED, модифікація алгоритму RED, яка працює з групою комірок;
RED	Random Early Detection, алгоритм випадкового раннього виявлення;

RMON	Remote Monitoring, протокол дистанційного моніторинга комп'ютерних мереж, розширення SNMP;
RSVP	Resource Reservation Protocol, протокол резервування мережних ресурсів;
SAP	Service Access Point, точка доступу до сервісу;
SIFS	Short InterFrame Space, короткий міжкадровий інтервал
SNMP	Simple Network Management Protocol, простий протокол керування мережами;
TCP	Transmission Control Protocol, протокол керування передачею даних;
UDP	User Datagram Protocol, протокол призначених для користувача даних;
VoIP	Voice over IP, система зв'язку, що забезпечує передачу мовного сигналу по IP-мережам;
VPN	Virtual Private Network, віртуальна приватна мережа

## ВСТУП

**Актуальність теми.** Сьогоденність вражає стрімким розвитком різноманітних комунікації, причому практично магістральним напрямом став процес удосконалення його технологічних підґрунть. Підвищення швидкості обміну інформацією та якості її перетворення в кінцевому підсумку визначає успішність соціального та державного розвитку конкретного суспільства. Не стане помилкою твердження, що становим хребтом цих змін стали розгалужені комп'ютерні мережі. Іноді складається враження, що розмаїття мережевих технологій стає надмірним, але саме в цьому полягають можливості удосконалення як методів передавання, так і перероблення інформаційних потоків. До того ж значно загострюється проблема обґрунтованого вибору систем фізичних каналів зв'язку, їх концептуальних архітектур та мережевих топологій.

«Комп'ютерна мережа - система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа - це система зв'язку через кабельне чи бездротове середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило - різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали» [1].

Все це розмаїття пов'язується за допомогою сучасних апаратно програмних засобів, які забезпечують управління, аналіз, моніторинг, кризову діагностику мережі як у поточному часі, так і забезпечує ретроспективний аналіз ефективності діючої системи та знаходження шляхів її покращення і регулярної модернізації. Темпи змін та удосконалення мереж є вражаючими, але можна констатувати, що дуже часто вони мають, так би мовити, «силовий характер» - відбувається просто зміна обладнання на нове міцніше, в той час як явно не вичерпані можливості вже існуючих апаратних платформ, систем, алгоритмів, не до кінця вирішені

проблеми взаємодії пристроїв, не знайдені оптимальні організації та конфігурації системи, не погоджені належним чином питання роботи клієнтів.

Причому, фахівцям достатньо добре відомо, що в даний час використовується не більш 1% сумарної «міжнародної» смуги пропускання. У той же час регулярні втрати пакетів на внутрішніх і транзитних мережах досягають 30%. Втрата вже 10% пакетів помітно позначається на продуктивності мережі, а при втраті 50% пакетів мережна служба стає фактично даремною.

Як це не дивно, незважаючи на явну претензію на ефективність, існуючі системи управління, які у більшості випадків функціонально надмірні, тим не менш, як правило, не дозволяють будувати реалістично прогнозовану можливу поведінку комп'ютерної мережі та і її окремих маршрутів, а особливо розгалужених об'єднань мереж. У кращому разі достатньо повно забезпечуються питання моніторингу роботи мереж. І це при тому, що на порядок денний наполегливо висуваються завдання розробки і реалізації комплексних систем реального управління комп'ютерними мережами, а також прогнозування, визначення т.зв. «вузьких місць» і своєчасного прийняття мір з їх «розширки» і т.п. Сьогодні проєктанти, виробники обладнання, ті хто його встановлює та експлуатують обладнання, вельми зацікавлені у оптимальному вирішенні питань знаходження ефективних методів керування трафіком.

Ні для кого не секрет, що всі ці питання ще більш ускладнюються при вирішенні їх у межах бездротових мереж, що напряму обумовлено специфікою ефірного простору, багатьма різномірними завадами, подолання яких потребує додаткових зусиль. Не можна також не згадати труднощів, що породжуються необхідностями модифікації математичного апарату.

Таким чином, можна упевнено стверджувати, що питання розвитку, удосконалення, оптимізації підходів до здійснення аналізу, забезпечення моніторингу, контролю і діагностики, і в кінцевому підсумку в рішення основних питань керування безпроводною мережею – стоять на сьогоденному порядку дня.

**Метою магістерської роботи є дослідження методів оцінювання параметрів мережі передачі різномірного мережного трафіку.**

**Об'єктом дослідження** є процес функціонування безпроводової комп'ютерної мережі з різномірним телекомунікаційним мережевим трафіком.

**Предмет дослідження.** Методи оцінювання параметрів безпроводової комп'ютерної мережі з різномірним телекомунікаційним мережевим трафіком.

**Методи дослідження.** У магістерській роботі застосовувалися теорія імовірності і математичної статистики, теорія масового обслуговування, методи цифрової обробки інформації, моделювання і розрахунки на ЕОМ.

**Апробація результатів магістерської роботи.** Основні результати магістерської атестаційної роботи доповідалися на конференціях Державного університету телекомунікацій та опубліковано в науковому журналі “Наукові записки Українського науково-дослідного інституту зв'язку”.

# 1. АНАЛІТИЧНИЙ ОГЛЯД І ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

## 1.1. Загальна проблема моніторингу та аналізу комп'ютерних мереж

Технологія моніторингу і аналізу закладається у процесі проектування комп'ютерних мереж. Вона є невід'ємною частиною загальної проблеми забезпечення сталого функціонування мережі, зокрема, якості сервісу (*Quality of Service, QoS*). Задача проектування мережі включає три етапи: вибір топології мережі, вибір технологій, на основі яких буде здійснюватися практична реалізація, і вибір обладнання. У реальних ситуаціях, наприклад, при створенні безпроводових мереж, вибір топології диктується специфікою використання радіоканалу. Найбільш прийнятними є топології “зірка” та комбінація топологій “кільце”, а також “загальна шина”. Вони, по суті, визначаються варіантами архітектури безпроводової мережі: незалежна конфігурація (*Ad Hoc*) та конфігурація з інфраструктурою (структурована мережа [1]). Незважаючи на те, що відмінності між цими архітектурами незначні, вони помітно впливають на такі показники, як кількість користувачів, що можуть підключатися до мережі, радіус мережі, завадостійкість мережі тощо.

У свою чергу, серед технологій, що вибираються, перевага, як правило, віддається одній з багатьох. Це умовні логічно, оскільки змішування різнорідних технологій у межах одного автономного сегмента мережі, безумовно, буде приводити до неузгодженості техніко-експлуатаційних характеристик, викликатиме необхідність підтримки великої кількості протоколів мережного обміну, розв'язання конфліктів між різнорідними протоколами та інтерфейсами тощо. Як наслідок, матиме місце нераціональне використання мережного ресурсу та зниження продуктивності мережі.

Таким чином, проблема вибору обладнання набуває вирішального значення. Від цього залежать ключові показники ефективності функціонування мережі, так звані *Key Performance Indicators, KPIs* [2, 47,48].



Ключовими параметрами є затримка передачі, пропускна спроможність, втрати пакетів і рівень безпеки. Ці параметри роблять найбільший вплив на результуючу якість сервісу.

Ключові параметри *KPIs* можна розбити на такі групи, які мають відносно самостійне значення для оцінювання характеристик мережі [3]:

- механізми забезпечення продуктивності (довгострокової, короткочасної, миттєвої);
- засоби аналізу, моніторингу та загального керування мережами;
- засоби керування надійністю обладнання для забезпечення безвідмовної роботи мережі;
- ергономічні параметри (зручність керування, експлуатації, обслуговування та користування).

У даній роботі розглядається система ключових показників ефективності для комп'ютерної мережі як великої системи із затримками сигнальної і управляючої інформації. При оптимізації характеристик мережі необхідно враховувати параметри, від яких залежить якість сервісу, і взаємозв'язок між цими параметрами.

Технологія аналізу, моніторингу і діагностики представляє собою набір діагностичних засобів і методику їх використання, які дозволяють дати об'єктивну оцінку якості роботи апаратних засобів та прикладних програм в мережі і обґрунтувати рекомендації по поліпшенню їх роботи. Для досягнення поставленої мети необхідно вирішувати наступні задачі:

- аналіз вимог до обладнання та прикладного програмного забезпечення (ПО) залежно від умов угоди про рівень обслуговування (*SLA, Service Level Agreement*) і об'єктивна оцінка швидкодії прикладних програм;
- поточний контроль швидкодії обладнання та прикладних програм в процесі їх експлуатації;
- контроль функціонування обладнання та прикладних програм в різних умовах експлуатації мережних компонентів.

Будь-який призначений для користувача апаратно-програмний засіб можна



розглядати як деякий генератор транзакцій, яким є:

- реальне обладнання з набором характеристик, які повинні підтримуватися у межах допусків;
- призначений для користувача програмний додаток, написаний з підтримкою прикладного програмного інтерфейсу (*API, Applied Program Interface*);
- тестові програми, що циклічно виконують деяку дію, поточна продуктивність виконання якого дає інформацію про стан мережі.

Через *API* генератори транзакцій взаємодіють з так званими агентськими додатками, в задачу яких входить збір інформації про час проходження тієї або іншої транзакції.

Інформація про якість конкретної транзакції міститься в профайлі – текстовому файлі, що складений за принципом *ini*-файлів *Windows* і містить набір умов, на підставі яких робиться висновок про стан мережі. Профайл створюється на основі результатів теоретичного аналізу і довготривалого тестування мережі, що працює в ідеальних умовах.

До показників, що вводяться в локальний файл або базу даних, додаються інші результати аналізу стану системи в цілому – інформація від управляючих протоколів, мережних аналізаторів і систем управління. Вони вводяться в єдину базу даних з відображенням в єдиній тимчасовій шкалі. Незадовільний час проходження тієї або іншої транзакції може бути безпосередньо пов'язано з якимсь зміряним параметром – завантаженням процесора на сервері або клієнті, скачками завантаження мережі і ін. Якщо проблема не така очевидна, буде потрібний аналіз різномірних даних, для чого застосовується статистичний (кореляційний і регресійний) аналіз [4,5].

Мережа – це велика система, до складу якої входить безліч компонентів: кабельна інфраструктура, активне устаткування, мережна операційна система і багато що інше. Концепція кризової діагностики мережі припускає уміння ефективно оцінити, як працюють всі компоненти мережі з урахуванням їх взаємозв'язків і взаємовпливу. Основний недолік більшості програм модернізації

мережі – постійна заміна устаткування на більш продуктивне. При цьому значна частина проблем функціонування мережі криється зовсім не у вичерпанні ліміту пропускної спроможності, а в проблемах взаємодії апаратури, конфігурації, організації мережі і роботи користувачів.

Інший недолік – використання адміністраторами мережі однієї-двох часткових методик діагностики і моніторингу і, відповідно, необ'єктивне оцінювання стану мережі. Суть дослідження, що проводиться, полягає саме в реалізації системного підходу. Методика безперервної діагностики мережі полягає в розбитті процесу на наступні взаємозв'язані етапи.

1. На першому етапі виробляється діагностика на фізичному рівні для виключення помилок і правильної інтерпретації результатів подальшого тестування.

2. На другому етапі доцільно проводити діагностику термінальних вузлів мережі шляхом стресового тестування мережі в двох режимах:

– режим калібрування з навантаженням тільки на мережу для виявлення помилок апаратної і програмної реалізації;

– режим з навантаженням тільки на мережу для виявлення проблем взаємодії станцій, вузьких місць на сервері і в каналах зв'язку.

3. Завершальний етап кризової діагностики мережі – діагностика прикладного мережного програмного забезпечення.

Ефективність використання мережі в значній мірі визначається якістю управління в умовах перевантаження. Поки мережа завантажена незначно, число пакетів, що приймаються і оброблюються, рівне числу тих, що прийшли на вхід комутаційного вузла. Проте, коли в мережу поступає дуже великий об'єм даних, може виникнути перевантаження і робочі характеристики погіршуються. При надмірних завантаженнях пропускна спроможність каналу або мережі може стати нульовою [6]. Така ситуація приводить до колапсу мережі.

Частково це може бути пов'язано з недостатністю пам'яті для вхідних буферів, але навіть якщо маршрутизатор має нескінченну пам'ять, ефект перевантаження може виявитися ще важчим. Це зв'язано з часом очікування

обробки. Якщо воно перевищує тривалість тайм-ауту, з'являються повторно передані пакети, що приводить до зниження корисної пропускнує спроможності мережі. Причиною перевантаження може бути повільний процесор або «вузьке горло» – низька пропускнує спроможність окремої ділянки мережі. Просте підвищення швидкодії процесора або інтерфейсу не завжди вирішує проблему – вузьке місце, як правило, переноситься в інший фрагмент мережі.

Одним з поширених методів боротьби з перевантаженнями є управління із зворотним зв'язком. Механізм управління із зворотним зв'язком може поліпшити продуктивність мережі, скорочуючи втрати пакетів, і запобігти розповсюдженню перевантаження. У принципі можна послати повідомлення про перевантаження відправнику, проте при цьому переобтяжена ділянка мережі навантажується ще більше. Тому задача управління розв'язується на транспортному рівні засобами протоколу *TCP* [7]. При виявленні перевантаження швидкість передачі знижується шляхом зменшення розміру ковзного вікна.

По суті, має місце управління із зворотним зв'язком, що запізнюється. При неправильному обліку характеристик запізнювання система може втратити стійкість і перейти в незгасаючий коливальний режим, або коректування інтенсивності потоку здійснюватиметься надто пізно. Це приводить до погіршення продуктивності мережі, особливе для додатків реального часу. Компенсація затримки зворотного зв'язку може виконуватися методами прогнозу, наприклад, з використанням моделі авторегресії і ковзного середнього (АРКС) або шляхом усереднювання параметрів вікна. Другий варіант простіший, але, природно, забезпечує значно нижчу якість сервісу.

Позитивного результату також можна досягти шляхом варіації значень тайм-аутів, зміни політики повторної передачі пакетів. В деяких випадках позитивний результат може бути одержаний зміною схеми буферизації.

Управління із зворотним зв'язком широко використовується в архітектурі інтегрованих служб (*Integrated Service Architecture – ISA*) для підтримки служб з різними рівнями якості сервісу (*Quality of Service – QoS*) в Інтернет і в часткових об'єднаних мережах.

Крім того, необхідно враховувати, що на даний момент актуальним є питання проходження різних видів трафіку по широкосмугових мережах, наприклад, регіональних мережах або мережах мегаполісу (MAN) [2], у тому числі по безпроводових мережах. Кожен вид трафіку, що передається, має свої характеристики, які, як відомо, значно впливають на вимоги, що пред'являються до обладнання мережі. Тому дослідження статистичних характеристик трафіку є важливим для успішної роботи мережі.

Як показали дослідження останніх десятиліть, вхідний потік трафіку не завжди можна вважати простим [8–10]. Встановлено і експериментально підтверджено, що характер трафіку є фрактальним, або самоподібним. Також, в ході досліджень підтверджено, що самоподібність трафіку істотно впливає на характеристики мережі.

Оскільки по сучасних мережах передаються різні види трафіку, то для забезпечення необхідної якості обслуговування використання дисципліни черг *FIFO* (*First in First Out* – першим прибув, першим обслужений) не завжди буде оптимальним. У таких випадках використовуються пріоритети. Пріоритети можуть призначатися залежно від типу трафіку. Важливим є випадок призначення пріоритету на основі середнього часу обслуговування. Часто запитам з меншим очікуваним часом обслуговування дається більший пріоритет, ніж запитам з великим очікуваним часом обслуговування. При такій схемі продуктивність високопріоритетного трафіку збільшується. Також вищі пріоритети можуть призначатися трафіку, чутливому до затримок, наприклад, голосовому або відеотрафіку.

Затримки викликають необхідність в збільшенні буферної пам'яті пристроїв комутації і маршрутизації, оскільки вони не справляються з потоком пакетів вже при коефіцієнті використання мережі 50-60%. Велика кількість пакетів відкидається і передається повторно, що приводить до ще більшого перевантаження мережі. Тому необхідно розраховувати необхідні розміри буфера з урахуванням характеристик трафіку.

Методи розрахунку вимог до мереж нових поколінь (пропускної спроможності каналів, місткості буферів і ін.) засновані на марківських моделях і формулах Ерланга, які з успіхом використовувалися при проектуванні телефонних мереж, можуть давати невиправдано оптимістичні рішення і приводити до недооцінки навантаження.

## **1.2. Методи ідентифікації параметрів безпроводових мереж з різними структурами**

Отримання інформації про різні характеристики фізичних каналів передачі комп'ютерних мереж практично необхідне для поточного контролю якості систем передачі. Вирішальний вплив на якість передачі інформації по каналах передачі мають такі характеристики мереж, як затримка, число втрачених пакетів, продуктивність мережі і пов'язані з ними передавальна, пропускна спроможність та інтегральна характеристика якості сервісу. На практиці найбільший інтерес представляють затримка доставки та число втрачених пакетів як ключові чинники впливу на якість сервісу.

Окреме і дуже важливе місце у переліку ключових параметрів ефективності безпроводових мереж займають безпека передачі та захист даних. У зв'язку з принциповою відкритістю каналів зв'язку безпроводових мереж підтримання цих параметрів на належному рівні є нагальною проблемою.

Розглянемо проблеми безпеки безпроводових мереж на прикладі сегменту *SOHO* (від англ. *Small office/home office* – “малий офіс/домашній офіс”). *SOHO* відноситься до категорії бізнесу, який включає від 1 до 10 працюючих. Концепція віддаленої роботи з'явилася на початку 70-х років ХХ століття. Починаючи з середини 1990-х років, сукупність таких чинників, як персональні комп'ютери, цифрові технології передачі даних, прихід провайдерів з обладнанням останньої милі, а також цифровий голосовий зв'язок, створили можливість для ефективної колективної роботи без обов'язкової присутності всіх працівників в одній будівлі офісу. Децентралізація зменшує накладні витрати і потенційно забезпечує вищу



продуктивність, особливе у великих містах, де непродуктивний час на переміщення від будинку до робочого місця і назад досягає іноді 2-3 годин в день.

Потреба в передачі великих об'ємів різнорідних даних примусила компанії принципово змінити схеми побудови мереж – особливо в сегменті *SOHO*, де чисельність співробітників, а відповідно мережних користувачів, складає декілька десятків (до 100) осіб. Для захисту таких мереж зазвичай використовуються наступні технології.

*WPA* і *WPA 2 (WLAN IEEE 802.11x Protected Access)* – є оновленими програмами сертифікації пристроїв безпроводового зв'язку. Технологія *WPA* прийшла на заміну технології захисту безпроводових мереж *WEP*. Плюсами *WPA* є посилена безпека даних і посилений контроль доступу до бездротових мереж. Важливою характеристикою є сумісність між безліччю безпроводових пристроїв як на апаратному рівні, так і на програмному. На даний момент *WPA* і *WPA 2* розробляються і просуваються організацією *Wi-Fi Alliance*.

*WPA* має спрощений режим, який одержав назву *Pre-Shared Key (WPA - PSK)*. При застосуванні режиму *PSK* необхідно ввести один пароль для кожного окремого вузла безпроводової мережі (бездротові маршрутизатори, точки доступу, мости, клієнтські адаптери). Якщо паролі співпадають із записами в базі, користувач отримує дозвіл на доступ в мережу.

*Wired Equivalent Privacy (WEP)* – алгоритм для забезпечення безпеки мереж *WLAN IEEE 802.11x*. Використовується для забезпечення конфіденційності і захисту даних, що передаються авторизованими користувачами від прослуховування у безпроводовій мережі. Існує два різновиди *WEP*: *WEP-40* і *WEP-104*, що розрізняються тільки довжиною ключа. В даний час технологія *WEP* є застарілою, оскільки її зламування може бути здійснено всього за декілька хвилин. Проте, вона продовжує широко використовуватися. Для забезпечення належного рівня безпеки в мережах *WLAN IEEE 802.11x* рекомендується використовувати *WPA*. *WEP* часто неправильно називають *Wireless Encryption Protocol*.

*RADIUS* (англ. *Remote Authentication in Dial-In User Service*) – протокол

аутентифікації, авторизації і збору даних про використані ресурси, розроблений для передачі даних між центральною платформою та термінальним обладнанням.

У літературі знайшли відображення різні методи отримання поточної інформації про характеристики мережних і термінальних та вузлів каналів передачі. Традиційними є операції вимірювання і допускового контролю [11,12]. Відносно новим є напрям, орієнтований на ідентифікацію каналів передачі [13 – 18]. Всі три напрями мають спільність, що обумовлена загальною метою дій, які здійснюються над каналом – отримання інформації про його характеристики. Відмінності полягають в засобах, а також в можливій повноті досягнення цієї мети.

Слід зазначити, що відмінності між вимірюванням, контролем і ідентифікацією часто є умовними. Так ряд методів вимірювання може трактуватися також в сенсі контролю та ідентифікації.

Використовуване стосовно каналів передачі поняття ідентифікації декілька відрізняється від поширеного у області автоматичного управління [19] тим, що не потребує, у обов'язковому порядку, настройки моделі об'єкту в безпосередній формі за допомогою алгоритмів цілеспрямованого перебору коефіцієнтів моделі.

Для визначення стану справ в області оцінювання ключових параметрів ефективності безпроводових комп'ютерних мереж проаналізуємо основні принципи їх побудови, мережні топології та структури.

На рис. 1.1 показано архітектуру мережі, типову для більшості невеликих компаній, чий профіль діяльності не лежить в галузі комп'ютерних інформаційних технологій. Точка доступу й безпроводові сегменти знаходяться в одній внутрішній мережі з проводовими сегментами. Для захисту може використовуватися *WPA* або *WPA2 (IEEE 802.11i)* у режимі *Pre Shared Key*, але, як правило, з міркувань простоти застосування використовується *WEP*. Це найбільш дешеве рішення, потребує мінімум налаштувань, однак воно є найменш безпечним.

На рис. 1.2 показано архітектуру мережі з проводовим та безпроводовим сегментами, рознесеними в різні підмережі, та з фільтрацією транзитного трафіку. Потрібна установка додаткового обладнання (шлюз або MME). Захищеність мережі в цілому значно вище, однак захист безпроводового сегменту залишається на рівні мережі, схему якої зображено на рис. 1.1.

На рис. 1.3 зображено схему мережі з системою захисту безпроводового сегменту, яка реалізується на основі сервера аутентифікації (*RADIUS*). Рівень захисту безпроводового сегменту – максимальний. Потребує встановлення й налаштування додаткового обладнання, що не завжди є тривіальною задачею.

В схемі, зображеній на рис. 1.4, використовується віддалений сервер авторизації (власний або зовнішньої компанії). Управління та контроль доступу здійснюється через віртуальну приватну мережу (*VPN – Virtual Private Network*). Спосіб є зручним для сумісного використання єдиної бази даних різними безпроводовими мережами. Існує велика кількість компаній, які надають подібні послуги.

Рішення *WLAN IEEE802.11x* найчастіше зводяться до побудови з'єднань типу "точка-точка" або "центр-точки"; у кожній з цих схем існує безліч різновидів реалізацій.

### **1.3. Методи отримання інформації про сигнали та завади у мережі**

Вимірювання і контроль по інформаційному сигналу є традиційними для систем автоматичного управління [20], проте не знаходять застосування у області передачі через те, що має місце просторове рознесення входу і виходу каналів передачі, внаслідок чого виникає необхідність передавати в пункт вимірювання і контролю відсутній там сигнал в неспотвореному вигляді. Крім того, мають місце затримки сигнальної та керуючої інформації, що призводить до відповідних затримок у керуванні і, що більш небезпечно, може взагалі привести до втрати стійкості системи діагностики, моніторингу та керування в цілому.

Цей же принциповий момент перешкоджає практичному використуванню



ряду споріднених методів вимірювання ключових характеристик каналів обміну даними [21,22]. Дані методи полягають в необхідності вимірювання деякої характеристики вхідного інформаційного сигналу, передачі інформації про неї в приймальний пункт (вихід каналу), вимірюванні аналогічної або спорідненої характеристики вихідного сигналу і обчисленні за отриманими даними необхідних характеристик самого каналу. Проте, ця група методів історично розвивалася першою і з'явилася основою першого покоління вимірювальної техніки для апаратури передачі даних [23 – 27].

Відзначимо, що в більшості випадків для отримання інформації про характеристики каналів без перерви передачі у якості тестового використовується гармонійний вимірювальний сигнал.

При цьому, вимірювання параметрів сигналу на виході каналу з метою оцінки його характеристик здійснюється кореляційним методом. Гармонійний вимірювальний сигнал використовується переважно для вимірювання АЧХ каналів, але в окремих роботах, наприклад, в [28] пропонується використовувати його і для вимірювання і ГЧЗ, для чого вимірювальний сигнал піддається модуляції низькою частотою.

Багаточастотні вимірювальні сигнали для вимірювання частотних характеристик містять  $N$  частотних складових з відомими амплітудами і певними фазами. В результаті їх обробки значення АЧХ і ФЧХ визначаються в  $N$  точках частотної смуги.

У [29] розглядаються сигнали з дельта образною кореляційною функцією стосовно вимірювань на трактах багатоканальних систем передачі. Звертається увага на сигнали ЛЧМ. У [31] досліджується вплив частотних спотворень на кореляційні функції вимірювальних сигналів, що пройшли через канал.

Разом з тим розглядаються методи, які припускають застосування складних періодичних сигналів, у тому числі і шумоподобних.

Властивості шумоподобних сигналів достатньо добре вивчені з позицій передачі інформаційних повідомлень [24,25,30]. Проте, використання таких сигналів для цілей вимірювання і контролю характеристик каналів вивчене

недостатньо.

Далі розглянемо основні суміщені методи вимірювання і контролю, класифікуючи їх за способом обробки вимірювального сигналу. Класифікація методів суміщених кореляційних вимірювань характеристик каналів передачі також розглядалася в [31]. З урахуванням того, що комп'ютерні мережі є цифровими за визначенням, модифікуємо ці методи з використанням дискретизації за часом та квантування за рівнем [32].

Ці методи підрозділяються на такі, що забезпечують безпосереднє отримання інформації (прямі вимірювання) і опосередковане отримання інформації (складні непрямі вимірювання). Термін безпосередні є умовним, оскільки певні обчислювальні дії над вимірюваними величинами тут передбачаються.

Перший прямий метод [33,34] заснований на вимірюванні амплітуд і фаз частотних складових спектру вимірювального сигналу з урахуванням того, що передатна (системна) функція каналу  $H(z)$  рівна

$$H(z) = Y(z)/X(z) = |H(z)|\Phi(z), \quad (1.1)$$

де  $|H(z)|$  - модуль передатної функції каналу,  $\Phi(z)$  - аргумент передатної функції каналу, а  $Y(z)$  і  $X(z)$  - зображення на  $z$ -площині відповідно вихідного і вхідного сигналів. Припускається, що амплітуда вхідного сигналу незмінна і відома. Амплітуда вихідного дискретного гармонійного сигналу оцінюється кореляційним способом. Можлива оцінка тільки АЧХ каналу. Відмітимо, що АЧХ каналу обчислюється вздовж одиничного кола  $z$ -площини в інтервалі від  $-\pi/T_d$  до  $\pi/T_d$ , де  $T_d$  - період дискретизації.

Другий метод [32] дозволяє визначити АЧХ каналу по співвідношенню

$$\left| H(z)H^*(z^{-1}) \right| = F_y(z)/F_x(z) \quad (1.2)$$

де  $F_y(z) = |Y(z)Y^*(z^{-1})|$ ,  $F_x(z) = |X(z)X^*(z^{-1})|$  - спектральні щільності потужності вихідного та вхідного сигналів відповідно. Тут передбачається, що

спектральна щільність потужності вихідного сигналу підлягає вимірюванню, а спектральна щільність потужності вхідного сигналу відома наперед. Згідно третьому методу – методу взаємного спектру (ВС), частотні характеристики каналу визначаються по взаємному спектру вхідного і вихідного сигналів [32,33], згідно виразу

$$H(z) = F_{xy}(z) / F_x(z), \quad (1.3)$$

де  $F_{xy}(z)$ - взаємна спектральна щільність вхідного і вихідного сигналів,  $F_x(z)$ - спектральна щільність вхідного сигналу.

До непрямих методів визначення частотних характеристик відносяться такі, згідно яким, в результаті первинної обробки вимірювального сигналу, отримують часові характеристики каналу. Перш за все, це імпульсна характеристика, перехідна характеристика, взаємна кореляційна функція, що характеризує властивості, як вимірювального сигналу, так і каналу. Шуканий коефіцієнт передачі отримують в результаті подальших операцій над перерахованими функціями. Відомий метод визначення частотних характеристик, заснований на вимірюванні імпульсної характеристики каналу [36]. Метод припускає вимірювання реакції каналу  $h(n)$ ,  $n=0,1,2,K$  на короткий імпульс, який в теорії відображається дельта-символом Кронекера. За цим слідує дискретне перетворення Фур'є від імпульсної характеристики і визначення коефіцієнта передачі

$$H(k) = \frac{1}{N} \sum_{n=0}^{N-1} h(n) \exp\left(-\frac{j2\pi nk}{N}\right), \quad k = 0,1,2,K, K = N \quad (1.4)$$

Недоліком цього методу слід вважати ту обставину, що він не може бути віднесений до повністю суміщених, оскільки створює хоча і короткочасні, але достатньо потужні перешкоди передаванню. Модифікацією згаданого методу є визначення частотних характеристик, при якому вимірюється перехідна характеристика каналу  $g(n)$ . Згідно методу на вхід каналу впливають спеціальним сигналом, що відображається одиничною функцією включення, з

подальшим визначенням імпульсної характеристики по відомому співвідношенню

$$h(n) = g(n) - g(n-1). \quad (1.5)$$

Далі, отримана  $h(n)$  перетвориться по Фур'є аналогічно тому, як це передбачалося попереднім методом. Помітимо, що при проведенні операції диференціювання, можлива поява істотних викидів, що усуваються згладжуванням  $h(n)$  з використанням спеціальних вагових функцій (Дольф-Чебишева, Хеммінга, фон Ханна тощо).

Принципово можливе визначення характеристик каналу шляхом розв'язання рівняння дискретної згортки виду [32]

$$y(n) = \frac{1}{N-m+1} \sum_{m=0}^{N-m+1} x(n)h(n-m) = \frac{1}{N-m+1} \sum_{m=0}^{N-m+1} x(n-m)h(n) \quad (1.6)$$

$$\begin{aligned} y(n) &= x(0)g(n) + \frac{1}{N-m+1} \sum_{m=0}^{N-m+1} x'(n)g(n-m) = \\ &= x(0)g(n) + \frac{1}{N-m+1} \sum_{m=0}^{N-m+1} x'(n-m)g(n). \end{aligned} \quad (1.7)$$

В цьому випадку потрібне вимірювання вхідного  $x(n)$  і вихідного  $y(n)$  сигналів. Оскільки у даних, що передаються на фізичному рівні, є інформація про сигнал, то реалізація процесу вимірювання спрощується: відпадає необхідність в передачі якої-небудь інформації про нього на приймальну станцію мережі. Вельми цікавим представляється метод визначення характеристик каналу по змінній функції взаємної кореляції. Метод заснований на визначенні  $g(n)$  шляхом рішення рівняння згортки, що пов'язує  $R_{xy}(m)$  з  $h(m)$  і автокореляційною функцією  $R_x(m)$  вхідного сигналу [35]

$$R_{xy}(m) = \frac{1}{N-m+1} \sum_{n=0}^{N-m+1} h(n)R_x(n-m) \quad (1.8)$$

У ряді випадків рішення цього рівняння є простим, наприклад, коли  $R_x(m) \rightarrow \delta(m)$ . У [4,5] приводиться приклад кореляційного методу вимірювань,

що припускає ототожнення імпульсної реакції лінійної системи з взаємною кореляційною функцією вхідного і вихідного сигналів – метод взаємної кореляційної функції (ВКФ). Фактично це різновид попереднього методу

$$h(m) = R_{xy}(m) \quad (1.9)$$

Можливі застосування цього методу в автоматичі, ядерній фізиці і ряді інших областей. Метод є повністю суміщеним і орієнтований на застосування шумового або шумоподібного вимірювального сигналу низького рівня.

## 2. ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ КЛЮЧОВИХ ПАРАМЕТРІВ БЕЗПРОВОДОВОЇ МЕРЕЖІ ПРИ РІЗНИХ СТАТИСТИКАХ МЕРЕЖНОГО ТРАФІКУ

### 2.1. Теоретичні засади застосування системи ключових показників ефективності для аналізу комп'ютерних мереж

При оптимізації параметрів і структури комп'ютерних мереж до складу цільової функції входить велика кількість основних і додаткових параметрів, від яких залежить якість сервісу *QoS*.

Для вирішення задач поточного управління мережами необхідний системний підхід. Критерії оптимізації ключових параметрів функціонування мережі і поточного управління мережею є неоднозначними і суперечливими. Урахування цих суперечностей і пошук компромісних рішень можливий при використуванні статистичних методів, узгодження достовірності і детальної початкових даних з фізичним значенням вирішуваних задач [23].

Процеси зміни КПЕ, з одного боку, є істотно нестационарними, а, з іншою – тенденції їх змін вельми схожі. Тому представляє інтерес дослідження характеристик їх стохастичного взаємозв'язку. Цей інтерес має не тільки теоретичний, але і практичний характер. Як основні характеристики стохастичного взаємозв'язку використовується коефіцієнт множинної кореляції і множинна регресія [25,14]. Крім того, для автоматизації вимірювань і розрахунків необхідно вибрати метод апроксимації кривих повторюваності змін КПЕ. Найгнучкішим і точним методом є апроксимація поліномами по мінімуму середнього квадрата помилки [22,23].

Розглянемо задачу прогнозу  $k$ -ї змінної  $Y_k$ ,  $k = \overline{1, N}$  по  $M$  змінних  $X_m$ ,  $m = 1, 2, \dots, M$ ;  $m \neq k$ . У загальному випадку  $M \neq N$ . При  $m=1$  маємо рівняння лінійної або поліноміальної регресії незалежної змінної  $X_m$  на залежну змінну  $Y_k$ , при  $m>1$  маємо систему  $m$  рівнянь множинної регресії змінних  $X_1, X_2, \dots, X_m$  на  $Y_k$ .

(Мається на увазі функціональна, а не статистична залежність.) У даній задачі незалежні змінні  $X_1, X_2, \dots, X_m$  – це випадкові величини, які не обов'язково є статистично незалежними.

Змінну  $Y_k$  апроксимуємо функцією регресії, що містить оцінки КПЕ і невідомі коефіцієнти  $\{a_0, a_1, \dots, a_m\}$ . Рівняння моделі лінійної регресії незалежних змінних  $X_1, X_2, \dots, X_m$  на залежну змінну  $Y_k$  запишемо в наступному вигляді:

$$Y_k = a_{0k} + a_{1k}X_1 + \dots + a_{mk}X_m + \varepsilon, \quad (2.1)$$

де  $\varepsilon$  – помилка апроксимації.

Хай  $X_{1j} = X_1^j$ . Тоді можна записати рівняння поліноміальної регресії у вигляді

$$Y_k = a_{0k} + a_{1k}X_1 + a_{2k}X_1^2 + \dots + a_{mk}X_1^m + \varepsilon. \quad (2.2)$$

Параметри моделі регресії оцінюються по вибірці об'єму, узятій з деякої генеральної сукупності. Теоретично генеральна сукупність має нескінченний об'єм або є всім набором даних, який існує у принципі.

Вибірка формується таким чином. За наслідками тесту функціонування мережі фіксуємо першу вибірку незалежних змінних  $X_{11}, X_{12}, \dots, X_{1m}$  і розраховуємо залежну змінну  $Y_1$ . Потім фіксуємо другу вибірку незалежних змінних  $X_{21}, X_{22}, \dots, X_{2m}$  і розраховуємо залежну змінну  $Y_2$ . Продовжуємо процедуру до отримання  $N$  змінних  $Y_k$ ,  $k = \overline{1, N}$ . Одержуємо вибірку із  $N$  спостережень

$$\{Y_1 : X_{11}, X_{12}, \dots, X_{1m}\}, \{Y_2 : X_{21}, X_{22}, \dots, X_{2m}\}, \dots, \{Y_N : X_{N1}, X_{N2}, \dots, X_{Nm}\}.$$

Система рівнянь множинної лінійної регресії приймає вигляд

$$\left. \begin{aligned} Y_1 &= a_{01} + a_{11}X_{11} + \dots + a_{m1}X_{1m} + \varepsilon_1 \\ Y_2 &= a_{02} + a_{12}X_{21} + \dots + a_{m2}X_{2m} + \varepsilon_2 \\ &\quad \text{L} \\ Y_k &= a_{0k} + a_{1k}X_{k1} + \dots + a_{mk}X_{km} + \varepsilon_k \\ &\quad \text{L} \\ Y_N &= a_{0N} + a_{1N}X_{N1} + \dots + a_{mN}X_{Nm} + \varepsilon_N \end{aligned} \right\}, \quad (2.3)$$



де  $\{a_{0k}, a_{1k}, K, a_{mk}\}$ ,  $k = \overline{1, N}$  – невідомі коефіцієнти, а  $\varepsilon_k$ ,  $k = \overline{1, N}$  – випадкові помилки, які логічно вважати нормальними однаково розподіленими з параметрами  $\{0, \sigma_\varepsilon^2\}$ . Для отримання оцінок по методу якнайменших квадратів необхідно мінімізувати суму  $S_k$  квадратів відхилень в кожній крапці. Якнайкраще наближення відповідає мінімальній величині виразу

$$S_k = \sum_{k=1}^N (Y_k - a_{0k} - a_{1k} X_{k1} - K - a_{mk} X_{km})^2 \quad (2.4)$$

Величина  $S_k$  є мірою помилки, пов'язаною з прив'язкою наявних даних до вибраної моделі регресії. Мінімум  $S_k$  досягається диференціюванням останнього виразу по коефіцієнтах, прирівнюванням відповідних похідних нулю і рішенням системи рівнянь відносно  $\{a_{0k}, a_{1k}, K, a_{mk}\}$ . Одержуємо систему рівнянь для оцінки часткових коефіцієнтів регресії:

$$\left. \begin{aligned} \mathcal{H}_1 &= \alpha_{01} + \alpha_{11} X_{11} + K + \alpha_{m1} X_{1m} \\ \mathcal{H}_2 &= \alpha_{02} + \alpha_{12} X_{21} + K + \alpha_{m2} X_{2m} \\ &\quad L \\ \mathcal{H}_k &= \alpha_{0k} + \alpha_{1k} X_{k1} + K + \alpha_{mk} X_{km} \\ &\quad L \\ \mathcal{H}_N &= \alpha_{0N} + \alpha_{1N} X_{N1} + K + \alpha_{mN} X_{Nm} \end{aligned} \right\} \quad (2.5)$$

Тут  $\alpha_{0k}, \alpha_{1k}, K, \alpha_{mk}$   $\alpha_{0k}, \alpha_{1k}, K, \alpha_{mk}$  – оцінки для  $\{a_{0k}, a_{1k}, K, a_{mk}\}$ . Оцінки є незміщеними і ефективними, тобто мають мінімальну дисперсію для вибірки  $X_1, X_2, K, X_m$   $X_1, X_2, K, X_m$  серед всіх лінійних оцінок для прогнозу змінних  $Y_k$ ,  $k = \overline{1, N}$ . У табл. 2.1 приведені часткові коефіцієнти кореляції показників, що оцінюються, по яких надалі з використанням рівнянь (2.1 – 2.5) можна розраховувати часткові коефіцієнти регресії.

Між основними ключовими показниками виявляється сильна кореляція. Це пояснюється тим, що вони роблять значний вплив на вимоги до якості сервісу. Виняток становить електронна пошта, оскільки, на відміну від потокового аудіо, відео, *Web-сервісу* і передачі файлів по протоколу *FTP*, для неї не критичні ні



смуга пропускання каналу, ні затримка доставки. Проте необхідно відзначити, що параметр  $D_{sp}$  – рівень безпеки і захисту даних є критичним практично для всіх представлених додатків, оскільки навіть для таких видів еластичного трафіку, як електронна пошта, захист даних є невід'ємною вимогою забезпечення якості сервісу *QoS*.

Результати кореляційного аналізу служать також ключовим індикатором моніторингу і регулювання поточних даних і *Web-service*. Це необхідно для забезпечення безпечної передачі інформації по мережі, прогнозування і запобігання перевантаженням контрольованого мережного фрагмента. Таким чином, поточний моніторинг і управління рівнем безпеки в мережі, які є невід'ємною частиною задачі загального управління якістю сервісу, можна успішно здійснювати статистичними методами, зокрема, методом кореляційно-регресійного аналізу.

Крім того, необхідно відзначити, що повністю скомпільована програма розрахунків займає в пам'яті обчислювального пристрою від 80 до 500 кілобайт залежно від масштабу мережі і об'єму оброблюваної вибірки. Оскільки в даний час практично будь-який мережний вузол, по суті, є спеціалізованим обчислювачем або навіть багатопроцесорною системою, задача апаратурної реалізації запропонованого методу може розв'язуватися порівняно просто.

## **2.2. Метод визначення середнього часу обслуговування пакету у мережі**

Для оптимізації часу обслуговування пакетів у мережі з неоднорідною структурою (складеній мережі) необхідно виконувати балансування мережного навантаження. При цьому з'являється можливість уникнути перевантажень, коли велика кількість потоків мережного трафіку намагається пройти одним і тим же маршрутом, який на даний час є оптимальним за множиною критеріїв.

Балансування навантаження (*Load Balancing*) застосовується для оптимізації виконання розподілених (паралельних) обчислень за допомогою розподіленої

(паралельної) обчислювальної системи. Балансування навантаження припускає рівномірне навантаження обчислювальних вузлів (процесора багатопроцесорної ЕОМ або комп'ютера в мережі). При появі нових завдань програмне забезпечення, що реалізовує балансування, повинне ухвалити рішення про те, де (на якому обчислювальному вузлі) слід виконувати обчислення, пов'язані з цим новим завданням. Крім того, балансування припускає перенесення (*migration* – міграція) частини обчислень з найбільш завантажених обчислювальних вузлів на менш завантажені вузли.

Слід розрізняти декомпозицію задач і проблему відображення задач на обчислювальне середовище. Декомпозиція задачі є етапом процесу створення паралельної програми. Декомпозиція призначена для розділення додатку на модулі (задачі). Задачі виконуються на окремих процесорах. В результаті декомпозиції розподіленого додатку з'являється набір задач, які паралельно вирішують задачу. Ці задачі можуть бути незалежними або пов'язаними один з одним за допомогою обміну даними. Відображення (або "розподіл задач") є окремим етапом, що дозволяє розподілити завдання, одержані на етапі декомпозиції, між процесорами.

Отже, вважатимемо, що розподілений додаток є сукупністю логічних процесів, які взаємодіють один з одним, посилаючи один одному повідомлення. Логічні процеси розподіляються по різних обчислювальних вузлах і можуть функціонувати паралельно. При розподілі логічних процесорів по обчислювальних вузлах їх прагнуть розподіляти так, щоб навантаження обчислювальних вузлів було рівномірним.

Проте при виконанні розподіленого додатку виникає конфлікт між збалансованим розподілом об'єктів по процесорах і низькою швидкістю обмінів повідомленнями між процесорами. Якщо логічні процеси розподілені між процесорами таким чином, що витрати на комунікацію між ними зведені до нуля, то деякі процесори (комп'ютери) можуть простоювати, тоді як інші будуть переобтяжені. У іншому випадку, "добре збалансована" система зажадає великі витрати на комунікацію. Отже, стратегія балансування повинна бути такою, щоб

обчислювальні вузли були завантажені достатньо рівномірно, але і комунікаційне середовище не повинне бути переобтяжене.

Реалізація розподіленої системи імітації вимагає розробки алгоритмів синхронізації об'єктів (або процесів), що функціонують на різних вузлах ВС. Алгоритми синхронізації ми вже обговорювали раніше. Ефективність реалізації цих алгоритмів, у свою чергу, залежить від рівномірності розподілу (балансування) обчислювального навантаження по вузлах ВС під час функціонування розподіленої програмної системи, якої є, зокрема, розподілена система імітації.

З метою розробки методу визначення середнього значення часу обслуговування пакету на підставі марковської моделі поведінки мережі однорідних станцій, дослідимо БЛМ, що складається із  $N$  станцій. Припустимо, що в чергу кожній з яких поступає потік пакетів з однаковою інтенсивністю, і однаковим розподілом  $D(l_j)$  довжин пакетів  $l_j$ . Станції мережі працюють в розподіленому режимі управління  $DCF$ . Крім того, припустимо, що черга пакетів станції може містити не більш  $B$  пакетів, межі  $L$  і  $N_s = m$  – однакові для всіх станцій, а час розповсюдження сигналу – порівняно малий.

Основна мета розробки – знайти середнє значення часу обслуговування пакету, відлічуваного від моменту або надходження пакету в порожню чергу даної станції, або закінчення обслуговування попереднього пакету з цієї черги, і до моменту або отримання підтвердження  $ACK$ , або закінчення інтервалу  $EIFS$  після останньої невдалої спроби передачі, тобто у разі втрати пакету.

Називатимемо пакети, передача яких починається у момент надходження, переданими асинхронно, а всі інші – переданими синхронно.

Асинхронна передача має місце, якщо у момент приходу пакету станція була в стані простою, а канал був вільний впродовж захисних інтервалів, як мінімум,  $DIFS$  або  $EIFS$ . Таким чином, асинхронна передача відбувається тільки за відсутності синхронних передач інших станцій, а оскільки  $\lambda N \sigma \ll 1$ , то можна вважати, що за час одного слоту затримки в мережі може відбутися не більш ніж

одна асинхронна передача [35, 36]. Отже, асинхронна передача завжди успішна.

Для оцінки часу  $T$  побудуємо модель поведінки станції у вигляді ланцюга Маркова з дискретним цілочисельним часом, одиницею якого є віртуальний слот – проміжок часу між послідовною зміною лічильника затримки у кожній станції, що не знаходиться в стані простою.

Хай  $b(t)$  – стохастичний процес зміни лічильника затримки для даної станції, часи  $t$  і  $t+1$  відповідають початку двох послідовних віртуальних слотів, причому станція передає, коли  $b(t) = 0$ . У той же час,  $s(t)$  – стохастичний процес зміни стадії затримки  $0, \dots, m$ , до якого додано значення  $-1$  для ситуації, коли в черзі немає пакету.

Помітимо, що, виходячи з прийнятої моделі, ці інтервали не мають прямої відповідності реальному часу, і віртуальні слоти неоднорідні. Як вже було сказано, лічильник затримки «заморожується», якщо станція помічає передачу іншої станції. Тому реальний час, що пройшов між  $t$  і  $t+1$ , більше слота затримки  $a$ , за наявності передачі іншої станції. Таким чином, маємо 3 види віртуальних слотів:

- “порожній” слот, під час якого жодна станція не вела передачу;
- “успішний” слот, коли одна і лише одна станція вела передачу;
- “колізійний” слот, під час якого відбулася колізія.

Двовимірний процес  $\{s(t), b(t)\}$  описується ланцюгом Маркова. Стану простою станції відповідає стан  $(-1, 0)$ . Стани, коли станція не має пакету для передачі, але виконує процедуру затримки після вдалої передачі або відмови – це  $(-1, 1..W_0 - 1)$ . Нарешті, стани, коли станція має пакет і виконує процедуру затримки – це вся решта, де  $k = 0, \dots, W_i - 1$  характеризує значення лічильника затримки, а  $i = 0, \dots, m$  – стадію затримки.

Слідуючи [15], представимо поточний стан процесу обміну даними у мережі як елементарну частинку, а процес переходу з одного стану в інше – як процес випадкового блукання цієї частинки. Хай число екранів системи обміну даними рівне  $N$ , а стан  $s_0$  – віддзеркалення пакету від зовнішнього екрану. Стан  $s_{1i}$

– проходження пакету через  $i$ -й екран, а стан  $s_2$  – проходження всіх етапів і досягнення отримувача.

Переміщення частинки може походити із стану  $s_0$  через стани  $s_{1i}$  в стан  $s_2$  і назад. Очевидно, стан  $s_{1i}$  є якимсь ідеальним станом, імовірність якого  $p_{1i} = P(s = s_{1i})$  рівна нулю. Тому даний процес, строго кажучи, не є марківським [40,28]. Для формального приведення процесу до марківського введемо деякі додаткові стани  $s_{1i+\epsilon}$  і  $s_{1i-\epsilon}$ . Імовірності  $p_{1i+\epsilon} = P(s = s_{1i+\epsilon})$  і  $p_{1i-\epsilon} = P(s = s_{1i-\epsilon})$  цих станів (так звані фіктивні імовірності) є величинами другого порядку малості в порівнянні з імовірністю  $p_0 = P(s = s_0)$  і  $p_2 = P(s = s_2)$  станів  $s_0$  і  $s_2$  відповідно. Тут  $S_{1i\pm\epsilon}$  – мала околиця точки  $S_i$ .

Тоді процес можна розглядати як блукання частинки між пружними жорсткими екранами  $S_0$ ,  $S_{1i}$  і поглинаючим екраном  $S_2$  (рис.2.1). Наявність екранів означає наступне:

– якщо частинка потрапляє в точку  $S_0$ , то в наступний момент часу частинка з імовірністю  $r$  потрапить в точку  $S_{0+\epsilon}$  або з імовірністю  $1-r$  залишиться в точці  $S_0$ ;

якщо частинка потрапляє в точку  $S_2$ , то в наступний момент часу частинка з імовірністю  $q$  потрапить в точку  $S_{2-\epsilon}$  або з імовірністю  $1-q$  залишиться в точці  $S_2$ .

Враховуючи, що імовірність стану  $s_1$  рівна нулю, розглянемо можливі стани  $s_0$ ,  $s_{1-\epsilon}$ ,  $s_{1+\epsilon}$ ,  $s_2$ . На рис. 2.2 зображений розмічений граф станів системи. Проти кожної стрілки проставлена відповідна імовірність переходу.





Інтегруючи цю систему рівнянь за заданих початкових умов, одержуємо імовірність станів як функції часу. Початкові умови вибираються залежно від того, як був стан системи у момент початку відліку ( $t = 0$ ). Зокрема, для прикладу, якому відповідає графік на рис. 2.1, початкові умови такі: при  $t = 0$   $p_{11-\varepsilon} = 1$ ,  $p_0 = p_{11-\varepsilon} = p_2 = 0$ .

У свою чергу, імовірність переходів визначається відношенням миттєвої інтенсивності заявок на передачу  $\lambda_{\text{мгн}}$  до швидкості реакції мережі. Цю швидкість можна трактувати як інтенсивність потоку обслуговування заявок на передачу  $\mu$ . Для випадку незмінної на інтервалі спостереження інтенсивності посилок  $\lambda$  стаціонарне рішення системи рівнянь (2.3) тривіальне. Воно є експоненціальною функцією, параметри якої повністю визначаються співвідношенням  $\lambda/\mu$  і початковим станом системи.

Важливою модифікацією системи рівнянь для поставленої задачі є урахування змінної інтенсивності трафіку, що приводить до залежності значень  $r$ ,  $r_{1-\varepsilon}$ ,  $r_{1+\varepsilon}$ ,  $r_{2\varepsilon}$  та ін. від часу. У разі змінної інтенсивності трафіку одержуємо систему параметричних диференціальних рівнянь першого порядку, загальне рішення якої має наступний вигляд (приведемо рішення для імовірності  $p_0$ ):

$$p_0(t) = e^{\{-\int [1-2r(t)]dt\}} \int p_{1-\varepsilon}(t) r_{1-\varepsilon}(t) e^{\int r(t)dt} dt + C e^{\{-\int [1-2r(t)]dt\}}, \quad (2.7)$$

де  $C$  – константа, визначувана з початкових умов.

Таким чином, записавши модифіковану систему рівнянь Колмогорова типу (2.3) і відшукавши її сумісне рішення для імовірності станів у вигляді виразів типу (2.4), можна одержати кількісні оцінки ефективності обслуговування пакетів, що передаються, залежно від інтенсивності вхідного потоку і швидкості обробки в пристрої управління.

Елементи мережі періодично опитуються для перевірки їх стану. Елемент спрацьовує, якщо з'явиться достатньо інтенсивний сигнал, який перевищить пороговий рівень  $\beta_{0I}$ . Якщо спрацював один або декілька елементів, система

моніторингу переходить в режим підвищеної готовності. У цьому режимі можуть включатися додаткові ресурси мережі для детального аналізу стану.



### 3. МЕТОД УРАХУВАННЯ ВЗАЄМНОГО ВПЛИВУ ТЕРМІНАЛЬНИХ ВУЗЛІВ БЕЗПРОВОДОВОЇ МЕРЕЖІ

#### 3.1. Ієрархічна модель безпроводової мережі

У попередніх розділах розглянута робота БЛМ в умовах нормального навантаження. Підхід до моделювання, висвітлений раніше, заснований на допущенні про статистичну незалежність поведінки окремих станцій мережі. Таке допущення цілком застосовне у разі високого навантаження. Проте воно може привести до істотних погрішностей при оцінці продуктивності мереж, що працюють при нормальному навантаженні. Зокрема, якщо черга однієї станції не порожня, то висока імовірність, що за час віртуального слота в чергу іншої станції також поступить пакет. З урахуванням викладеного, пропонується підхід, що дозволяє врахувати взаємозалежність поведінки станцій мережі.

Нижче розглядається БЛМ з протоколом *IEEE 802.11*, що складається із  $N$  статистично однорідних станцій, в чергу кожній з яких поступає пуассонівський потік пакетів з інтенсивністю  $\lambda$ . Пакети однакові і передаються за допомогою базового методу; канал вважається ідеальним, а час розповсюдження сигналу між станціями – нехтуємо малим. Крім того, передбачається, що черга пакетів кожної станції може містити не більш  $M$  пакетів.

Мета аналізу – оцінити наступні показники продуктивності [35]:

- середнє значення  $\bar{T}_d$  часу затримки пакету, відлічуваного від моменту надходження пакету в чергу даної станції і до моменту закінчення його обслуговування, тобто після закінчення інтервалу *DIFS*, яким завершається успішна передача, або інтервалу *EIFS* у разі останньої невдалої спроби передачі, що приводить до втрати пакету;

- імовірність відмови в передачі пакету, що відбувається через або переповнювання черги станції, або закінчення числа  $N_s = R$  повторних передач.

Слідуючи підходу, запропонованому в [21, 22], розділяється весь час роботи

мережі на віртуальні слоти.

Віртуальні слоти не однакові, і кожний з них може представляти з себе:

– “порожній” слот відстрочення  $\sigma$ , в якому жодна із станцій не веде передачу;

– “успішний” слот, в якому тільки одна із станцій передає пакет синхронно;

– “асинхронний” слот, в якому одна із станцій передає пакет асинхронно;

– “колізійний” слот, в якому дві або більш станцій намагаються здійснити передачу.

Очевидно, імовірність цих слотів, що позначаються відповідно  $p_e(n)$ ,  $p_s(n)$ ,  $p_a(n)$ , и  $p_c(n)$ , залежить тільки від числа “активних” станцій  $n$ , черги яких не порожні на початку даного віртуального слота.

При описі роботи мережі процесом народження-загибелі з дискретним часом так, як це зображено на рис. 3.1, причому стан цього процесу описується сумарним числом  $l$  пакетів, що знаходяться в чергах станцій мережі, включаючи передані в даний момент пакет, а одиницею часу є віртуальний слот, на рис. 3.1 не показані так звані петлі, тобто переходи в той же самий стан (з  $l$  в  $l$ ).



Рисунок 3.1. Процес народження-загибелі петлі

Для визначення імовірності народження  $\lambda(l)$ , тобто збільшення  $l$  на 1 за слот, і загибелі  $\mu(l)$  – зменшення  $l$  на 1 за слот, введені наступні допущення.

1. Умова ординарності потоку. Протягом спроби передачі (включаючи завершальні її інтервали *DIFS* або *EIFS*) в черзі станцій може поступити не більш ніж один пакет.

2. По завершенні колізії відмова в подальшій передачі пакету може

відбутися не більше ніж на одній із станцій, залучених в колізію (імовірність одночасної відмови на двох і більш станціях є величиною другого порядку малості).

При  $l=0$  народження відбувається, коли одна із станцій передає асинхронно, і під час цієї успішної передачі, що дорівнює

$$t_s = \frac{l_{DATA}}{V} + t_H + t_{ACK} + SIFS + DIFS, \quad (3.1)$$

де  $l_{DATA}$  – довжина пакету, в чергу цієї або іншої станції поступає ще один пакет. Таким чином,

$$\lambda(0) = (1 - e^{-NA\sigma})(1 - e^{-NA t_s}). \quad (3.2)$$

При  $l > 0$  народження відбувається, коли новий пакет поступає в не переповнену чергу або під час порожнього слота, або під час асинхронної передачі, або протягом колізійного слота, в кінці якого не відбувається відмова в подальшій передачі пакету ні на одній із станцій, залучених в колізію. Загибель має місце, коли протягом “успішного” слота або колізії, що приводить до відмов в подальшій передачі пакету, не поступає новий пакет. Отже, при  $l > 0$

$$\begin{aligned} \lambda(l) = & \sum_{n=n_{\min}(l)}^{\min(N,l)} \gamma(n,l) \left\{ [1 - \beta_q^e(n,l)] p_c(n) (1 - e^{-nA\sigma}) + \right. \\ & \left. + [1 - \beta_q^f(n,l)] \left[ p_\alpha(n) (1 - e^{-NA t_s}) + p_c(n) [1 - \beta_m(n)] (1 - e^{-NA t_c}) \right] \right\} \\ & + [1 - \beta_q^f(n,l)] \left[ p_\alpha(n) (1 - e^{-NA t_s}) + p_c(n) [1 - \beta_m(n)] (1 - e^{-NA t_c}) \right] \end{aligned}$$

У цих формулах  $n_{\min}(n,l) = \lceil (l-1)/B \rceil + 1$ ;  $\lceil x \rceil$  – ціла частина числа  $x$ ;  $\gamma(n,l)$  – імовірність наявності  $n$  активних станцій. Стационарна імовірність  $p_{st}(l)$  станів даного процесу описується формулами:

$$p_{st}(l) = p_{st}(0) \prod_{i=1}^{M_l} \frac{\lambda(i-1)}{\mu(i)}, \quad p_{st}(0) = \frac{1}{1 + \sum_{j=1}^{NM} \prod_{i=1}^{M_j} \frac{\lambda(i-1)}{\mu(i)}}. \quad (3.3)$$

Для оцінки імовірностей  $\gamma(n,l)$  і  $\beta(n,l)$  прийемо наступне допущення:

Нехай сумарне число пакетів, що знаходяться в чергах станцій мережі, рівно  $l > 0$ . Тоді всі варіанти розміщення цих  $l$  пакетів по  $N$  чергах мережі мають однакову імовірність.

Використовуючи це припущення, знаходиться  $0 \leq l \leq NM$  і  $n_{\min}(l) \leq n \leq \min(N, l)$ :

$$\gamma(n, l) = \frac{1}{g[l, N, M]} C_n^N g[l - n, n, M - 1]; \quad \text{при } l < n + M - 1 \rightarrow \beta_q^f(n, l) = 0,$$

а при  $l \geq n + M - 1$

$$\beta_q^f(n, l) = \frac{1}{g[l - n, n, M - 1]} \sum_{k=k_{\min}(l, n)}^{K(l, n)} \frac{k}{N} C_k^n g[l - n - k(M - 1), n - k, M - 2].$$

Для знаходження імовірності слотів і імовірності відмови  $\beta_m(n)$  приймаються такі початкові умови: на початку даного віртуального слота число активних станцій дорівнює  $n$ . Тоді для будь-якої з цих станцій імовірність  $p_{ss}(n)$  початку синхронної передачі, а також імовірність відмови  $\beta_m(n)$  у разі колізії в цьому слоті співпадають з відповідними значеннями  $S_n$ , одержаними для мережі яка включає  $n$  постійно активних станцій на інтервалі спостереження. Інші  $N - n$  станцій в  $S_n$  можуть передавати тільки асинхронно за умови, що жодна з активних станцій не передає. Якщо пакет поступає в чергу будь-якої з  $N - n$  неактивних станцій у момент передачі будь-якої із станцій, то цей пакет втрачається.

У відповідності до прийнятої моделі одержується наступна імовірність передачі пакетів у слотах:

$$p_e(n) = [1 - p_{ss}(n)]^n e^{-(N-n)\sigma}, \quad p_a(n) = [1 - p_{ss}(n)]^n [1 - e^{-(N-n)\sigma}] \quad (3.5)$$

$$\begin{cases} p_s(n) = np_{ss}(n)[1 - p_{ss}(n)]^{n-1}; \\ p_c(n) = 1 - [1 - p_{ss}(n)]^n - np_{ss}(n)[1 - p_{ss}(n)]^{n-1}, \end{cases} \quad (3.6)$$

де  $p_{ss}(0) = 0$ .

Оскільки імовірність того, що поточна синхронна спроба невдала через колізію, рівна

$$\xi(n) = 1 - [1 - p_{ss}(n)]^{n-1}, \quad (3.7)$$

то імовірність того, що дана невдача –  $k$ -та поспіль, рівна  $\beta_m^0(n) = [\xi(n)]^{k-1}$ . Нехтуючи імовірністю колізії більш ніж двох станцій і імовірністю одночасних відмов на декількох станціях, виходить

$$\beta_m(n) = 2\beta_m^0(n). \quad (3.8)$$

Для визначення  $p_{ss}(n)$  слід послатися на [39], де  $p_{ss}(n)$  знаходиться шляхом рішення наступного рівняння:

$$p_{ss}(n) = \frac{2}{E[w] + 1}, \quad (3.9)$$

де  $E[w] = \left\{ \sum_{i=1}^R \xi^{i-1} W_i + \frac{\xi^R W_R - W_0}{1 - \xi} \right\} \frac{(1 - \xi)^2}{1 - \xi^R}$  – середнє значення довжини

конкурентного вікна у випадку  $R \leq m$ :

$$E[w] = \left\{ \sum_{i=1}^m \xi^{i-1} W_i + W_m \sum_{i=m}^{R-1} (i - m + 2) \xi^i + \frac{(R - m + 1) W_m \xi^R - W_0}{1 - \xi} \right\} \frac{(1 - \xi)^2}{1 - \xi^R}, \quad (3.10)$$

при  $R > m$ .

Таким чином, при досить великих значеннях довжини конкурентного вікна можна вважати, що імовірність  $p_{ss}(n)$  початку синхронної передачі є обернено пропорційною величиною середнього значення довжини конкурентного вікна передачі.

### 3.2. Метод оцінки середнього часу затримки пакету й імовірності відмови обслуговування

Виходячи з результатів вище приведеного аналізу, можна зробити висновок про вибір та обґрунтування моделі для досліджень. При використанні її для оцінки основних ключових показників ефективності: середнього часу затримки  $T_d$

і усередненої імовірності відмови  $P_{rej}$  через або переповнювання черги станції, або закінчення числа  $M$  повторних передач, по формулі Літтла виходить:

$$T_d = \frac{L}{\mu_q}, \quad (3.11)$$

де  $L$  – середнє значення загальної інтенсивності, а  $\mu_q$  – середнє число пакетів, прийнятих станціями в їх чергу за секунду. Тепер  $L$  можна обчислити по формулі:

$$L = \frac{1}{E[t_{vs}]} \sum_{l=0}^{NM} p_{st}(l) \sum_{n=n_{\min}(l)}^{\min(N,l)} \gamma(n,l) \left[ p_e(n) \bar{l}_e^n + p_a(n) \bar{l}_a^n + p_s(n) \bar{l}_s^n + p_c(n) \bar{l}_c^n \right], \quad (3.12)$$

де  $E[t_{vs}]$  – середня тривалість віртуального слота,

$$\bar{l}_e^n = l\sigma + \frac{1}{2} [1 - \beta_q^e(n,l)] N\Lambda\sigma^2; \quad \bar{l}_a^n = l \left( \frac{\sigma}{2} + t_s \right) + t_s + \frac{1}{2} [1 - \beta_q^f(n,l)] N\Lambda t_s^2;$$

$$\bar{l}_s^n = lt_s + \frac{1}{2} [1 - \beta_q^f(n,l)] N\Lambda t_s^2; \quad \bar{l}_c^n = lt_c + \frac{1}{2} [1 - \beta_q^f(n,l)] N\Lambda t_c^2 - \text{середні значення } l$$

протягом порожніх, асинхронних, успішних і колізійних слотів відповідно, причому кожне з цих значень помножене на середню тривалість відповідного слота і розраховане при даному  $n$ .

Інтенсивність надходження  $\Lambda_q$  визначається по формулі, аналогічній (3.9), із заміною  $\bar{l}^n$  з різними нижніми індексами на  $h_e^n = [1 - \beta_q^e(n,l)] N\Lambda\sigma$ ,  $h_a^n = 1 + [1 - \beta_q^f(n,l)] N\Lambda t_s$ ,  $h_s^n = [1 - \beta_q^f(n,l)] N\Lambda t_s$  і  $h_c^n = [1 - \beta_q^f(n,l)] N\Lambda t_c$  – середні кількості пакетів, прийнятих в черзі станцій протягом відповідно порожніх, асинхронних, успішних і колізійних слотів.

Тепер можна знайти усереднену імовірність відмови  $P_{rej}$ .

Оскільки середнє число пакетів, що поступають (але що необов'язково приймаються) в черзі станцій за слот, рівне  $N\Lambda E[t_{vs}]$ , те, обчислюючи середнє число пакетів, обслуговування яких завершується протягом даного слота, мається:

$$P_{rej} = 1 - \frac{1}{NE[t_{vs}]} \sum_{l=0}^{NM} P_{st}(l) \sum_{n=n_{\min}(l)}^{\min(N,l)} \gamma(N,l) [p_a(n) + p_s(n)]. \quad (3.13)$$

Отже, показники продуктивності обчислюються за наступною процедурою:

- а) для всіх  $l$  і  $n \leq \min(l, N)$  розраховуються імовірність  $\gamma(n, l)$  наявності  $n$  активних станцій і імовірність втрати  $\beta_q^e(n, l)$  и  $\beta_q^f(n, l)$ ;
- б) для всіх  $0 < n \leq N$  необхідно вирішити систему рівнянь (3.6 - 3.7), знаходячи  $p_{st}(n)$ , а потім – по формулі (3.5) – імовірність відмови  $\beta_m(n)$ ;
- в) для всіх  $0 < n \leq N$  розраховується імовірність слотів по формулах (3.2)...(3.3);
- г) для всіх  $l < NM$  розраховується стаціонарна імовірність  $p_{st}(l)$  по формулі (3.1);
- д) розраховуються показники продуктивності по формулах (3.8 - 3.10).

### 3.4. Методи врахування неоднорідності вхідних пакетів

Якщо в попередніх розділах розглядалися ситуації, коли довжина пакетів, що приходять, постійна і вона менше порогу  $RTS/CTS$ , то в цьому розділі будуть розглянуті зміни, що вносяться в модель для врахування неоднорідності пакетів, що приходять на станції, і можливості їх передачі з використанням механізму  $RTS/CTS$ .

Довжина пакету  $l_i$  може перевищувати поріг  $RTS/CTS$ , який позначений через  $L_{rts}$ . Нехай розподіл довжин  $D(l_i)$  однаковий для всіх станцій. Як і в попередньому розділі, можна припустити, що короткі кадри  $RTS$ ,  $CTS$  і  $ACK$  не спотворюються завадами, а пакет завдовжки  $l_i$  спотворюється з імовірністю  $q_i = 1 - (1 - BER)^{H_{MAC} + l_i}$ .

Визначаються можливі часи, що витрачаються на передачу пакету завдовжки  $l_i$ . При  $l_i \leq L_{rts}$  час успішної передачі рівний



$$t_s^i = \frac{l_i}{V} + t_H + t_{ACK} + SIFS + DIFS,$$

час передачі, що не вдалася через завади, –  $t_{CD}^i = \frac{l_i}{V} + t_H + EIFS$ , а час, що витрачається на передачу цього пакету при колізії –  $t_C^i = t_{CD}^i$ .

При  $l_i > L_{rts}$  є:

$$t_s^i = t_{RTS} + t_{CTS} + \frac{l_i}{V} + t_H + t_{ACK} + 3 \cdot SIFS + DIFS,$$

$$t_{CD}^i = t_{RTS} + t_{CTS} + \frac{l_i}{V} + t_H + 2SIFS + EIFS,$$

$$t_C^i = t_{RTS} + EIFS.$$

Як відмічено в [35, 48, 43] імовірність  $D^*(l_i)$  того, що спроба передачі, виконувана активною станцією мережі в довільно вибраному слоті, відноситься до пакету завдовжки  $l_i$ , відрізняється від початкового розподілу  $D(l_i)$ , з яким пакет поступає в чергу і виходить з неї. Ця відмінність пов'язана з тим, що чим довше пакет, тим більше імовірність його спотворення і тим більше (в середньому) спроб потрібно для його передачі. З урахуванням їх розподілів знаходимо середні тривалості асинхронного і “успішного” слотів:

$$t_s^a = \sum_i D(l_i) [(1 - q_i)t_s^i + q_i t_{CD}^i] + \frac{\sigma}{2}, \quad t_s^* = \sum_i D^*(l_i) [(1 - q_i)t_s^i + q_i t_{CD}^i].$$

Імовірності переходів в моделі на рнс. 3.2 набувають вигляду:

$$\left\{ \begin{array}{l} \bar{l}_a^n = l t_s^a + \frac{\sigma}{2} t_s^a + \frac{N\Lambda}{2} [1 - \beta_q^f(n, l)] \sum_i [(1 - q_i)(t_s^i)^2 + q_i (t_{CD}^i)^2] D(l_i); \\ \bar{l}_a^{n*} = l t_s^* + \frac{N\Lambda}{2} [1 - \beta_q^f(n, 1)] \sum_i [(1 - q_i)(t_s^i)^2 + q_i (t_{CD}^i)^2] D^*(l_i); \\ \bar{l}_c^n = l t_c + [1 - \beta_q^f(n, l)] \frac{N\Lambda}{2} \sum_{i,j} [\max\{t_c^i, t_c^j\}]^2 D^*(l_i) D^*(l_j); \\ h_a^n = 1 + [1 - \beta_q^f(n, l)] N\Lambda \left( t_s^a - \frac{\sigma}{2} \right). \end{array} \right.$$

У приведених формулах  $\beta_m^c(n, j)$  і  $\beta_m^d(n, j)$  означають імовірності відмови в подальшій передачі пакету завдовжки  $l_j$  через досягнення своїх граничних значень лічильниками  $n_s$  і  $n_d$  відповідно.

Решта компонентів (3.9) і аналогічної формули для  $\Lambda_q$ , відмінні від вже визначених в попередніх розділах, знаходяться таким чином:

$$\left\{ \begin{array}{l} \bar{l}_a^n = lt_s^a + \frac{\sigma}{2}t_s^a + \frac{N\Lambda}{2}[1 - \beta_q^f(n, l)] \sum_i [(1 - q_i)(t_s^i)^2 + q_i(t_{CD}^i)^2] D(l_i); \\ \bar{l}_a^{n*} = lt_s^* + \frac{N\Lambda}{2}[1 - \beta_q^f(n, 1)] \sum_i [(1 - q_i)(t_s^i)^2 + q_i(t_{CD}^i)^2] D^*(l_i); \\ \bar{l}_c^n = lt_c + [1 - \beta_q^f(n, l)] \frac{N\Lambda}{2} \sum_{i,j} [\max\{t_c^i, t_c^j\}]^2 D^*(l_i) D^*(l_j); \\ h_a^n = 1 + [1 - \beta_q^f(n, l)] N\Lambda \left( t_s^a - \frac{\sigma}{2} \right). \end{array} \right.$$

Для завершення побудови повної системи рівнянь, визначається імовірність початку синхронної передачі, розподіл спроб  $D^*(l_i)$  і імовірності відмови  $\beta_m^c(n, j)$  та  $\beta_m^d(n, j)$  для насиченої мережі  $S_n$ .

Знаходять вище вказану імовірність, використовуючи метод, запропонований в [31].

Далі розглядається процес передачі пакету завдовжки  $l_j$  деякою станцією, що починається у момент вибору пакету з черги і закінчується або його успішною передачею, або відмовою. Хай  $f(l_j)$  – середня кількість спроб передачі, зроблених цією станцією,  $\bar{w}(l_j)$  – середня кількість віртуальних слотів, в які станція утримується від передачі на інтервалі спостереження процесу, що розглядається. Інтервал  $\bar{w}(l_j)$  є сумарним часом відстрочення. Тоді

$$P_{st} = \frac{\sum_j f(l_j) D(l_j)}{\sum_j [f(l_j) + \bar{w}(l_j)] D(l_j)}.$$

Розпочинається з простішого випадку передачі коротких пакетів, тобто  $l_j \leq L_{RTS}$ , коли пакет передається за допомогою механізму основного доступу.

При цьому число спроб  $i$  обмежене величиною  $N_s$ , тому

$$f(l_j) = \sum_{i=1}^{N_s} i \Psi_{l_j}(i), \quad \bar{w}(l_j) = \sum_{i=1}^{N_s} \bar{W}_i \Psi_{l_j}(i), \quad (3.14)$$

де  $\Psi_{l_j}(i)$  – імовірність того, що відбувається рівно  $i$  спроб. Сумарний час відстрочення  $\bar{W}_i$  визначеної за умови  $i$  спроб, знаходиться за наступних формул:

$$\bar{W}_i = \begin{cases} \sum_{k=0}^{i-1} \frac{W_k - 1}{2} = W_{i-1} - \frac{W_0 + i}{2}, & 1 \leq i \leq m + 1; \\ \sum_{k=0}^m \frac{W_k - 1}{2} + \frac{W_m - 1}{2} (i - 1 - m) = W_m \frac{i - m + 1}{2} - \frac{W_0 + i}{2}, & i > m + 1. \end{cases}$$

Знаходження імовірності  $\psi_{l_j}(i)$ ,  $i = 1, \dots, N_s$ . Імовірність невдалої спроби рівна  $\hat{p}(l_j) = 1 - (1 - p)(1 - q(l_j))$ , де  $p = 1 - (1 - p_{st})^{N-1}$  – імовірність колізії поточної спроби, а  $q(l_j)$  – імовірність спотворення завадами. Тоді процес передачі пакету завершиться успішно на  $i$ -й спробі з імовірністю, або закінчиться відмовою після  $N_s$ -ї спроби з імовірністю  $p_{rej}(l_j) = [\hat{p}(l_j)]^{N_s}$ . Отже,

$$\psi_{l_j}(i) = \psi_{l_j}^S(i) = [1 - \hat{p}(l_j)] [\hat{p}(l_j)]^{i-1},$$

$$\psi_{l_j}(N_s) = \psi_{l_j}^S(N_s) + p_{rej}(l_j) = [\hat{p}(l_j)]^{N_s-1}.$$

Використовуючи формулу умовної імовірності, знаходиться:

$$\beta_m^c(l_j) = \beta_m^d(l_j) = [\hat{p}(l_j)]^{N_s-1}.$$

Тепер нехай  $l_j > L_{RTS}$ . В цьому випадку число передач кадру *DATA* обмежене величиною  $N_d$ , і кожній такій передачі може передувати  $0, \dots, N_{s-1}$

невдалих передач кадру  $RTS$ .

Хай в процесі передачі пакету завдовжки  $l_j$  відбувається рівно  $i_d$  і  $i_r$  повторних передач кадрів  $DATA$  і  $RTS$  відповідно. Позначаються імовірності невдалих передач кадрів  $DATA$  і  $RTS$  через  $q(l_j)$  та  $p_{RTS}$  відповідно. Тоді імовірність здійснення рівно  $i$  спроб рівна:

$$\psi_{l_j}(i) = \psi_{l_j}^s(i) + 1(i \geq N_s) \sum_{i_d=0}^{\min\{i, N_d\}-1} \zeta_{l_j}^r(i_d, i - i_d) + 1(1 \geq N_d) \zeta_{l_j}^d(i - i_d),$$

$$i = 1, \dots, N_s N_d,$$

$$\text{де } \psi_{l_j}^s(i) = \sum_{i_d=0}^{\min\{i, N_d\}-1} \zeta_{l_j}^s(i_d, i - i_d - 1) - \text{імовірність успішного завершення}$$

процесу на  $i$ -й спробі, а  $1(\ )$  – булев індикатор, рівний 1 при виконанні умови в дужках і рівний нулю в іншому випадку.

Середнє число спроб  $f(l_j)$  і середній сумарний час відстрочення  $\bar{w}(l_j)$  знаходяться з формул (3.11) заміною  $N_s$  на  $N_s N_d$ . Крім того, імовірність відмови для пакету завдовжки  $l_j$  рівна

$$p_{rej}(l_j) = \sum_{i_d}^{N_d-1} \sum_{i_r=N_s}^{N_s+i_r(N_s-1)} \zeta_{l_j}^r(i_d, i_r) + \sum_{i_r=0}^{N_d(N_s-1)} \zeta_{l_j}^d(i_r). \quad (3.15)$$

Використовуючи формулу умовної імовірності, знаходять:

$$\beta_m^c(l_j) = \frac{\sum_{i_d}^{N_d-1} \sum_{i_r=N_s}^{N_s+i_r(N_s-1)} \zeta_{l_j}^r(i_d, i_r)}{p}, \quad \beta_m^d(l_j) = \frac{\sum_{i_r=0}^{N_d(N_s-1)} \zeta_{l_j}^d(i_r)}{q(l_j)}.$$

Нарешті, розподіл спроб  $D^*(l_j)$  знаходиться по очевидній формулі:

$$D^*(l_j) = \frac{D(l_j) f_{l_j}}{\sum_h D(l_j) f_{l_h}}.$$

Наведені методики можна ефективно використовувати у безпроводових локальних мережах різного масштабу та призначення, які працюють при

високому мережному навантаженні (при так званому насиченні мережі). У спеціалізованих безпроводових мережах використовують саму різну архітектуру, технології і стандарти, тому такі мережі є гетерогенними за визначенням. Проте основою спеціалізованих безпроводових мереж, як правило, є мережі стандартів *IEEE 802.11*.

Вичерпний виклад принципів побудови мереж стандарту *IEEE 802.11* різних модифікацій, методів апаратної реалізації і оцінка продуктивності дані в роботі [1]. За основу аналізу часових характеристик роботи мережі узяті моделі рівномірного [13] або геометричного [14] розподілів імовірності відправки пакету кожною станцією мережі. Передбачається, що всі станції в мережі є статистично однорідними. Під цим мається на увазі однаковий розподіл імовірності довжини пакетів, вибраних кожною станцією з черги. У разі змішаної (гетерогенної) мережі пропонується кожному пристрою надавати в трафіку приблизно рівний часовий інтервал.

У спеціалізованих безпроводових мережах дані припущення виконуються не повною мірою. Трафік мережі, як правило, є різнорідним (мова, відео, дані) і самоподібним за своєю природою [15]. Його статистичні характеристики вже не можуть бути описані розподілами експоненціального сімейства. В цьому випадку використовуються розподіли з так званими «важкими хвостами» (Парето, Вейбулла, гамма- і бета-розподіли).

Для оцінювання характеристик продуктивності гетерогенних безпроводових мереж, в яких циркулює різнорідний самоподібний трафік, необхідно застосовувати непараметричні методи. Як нижній поріг продуктивності можна одержувати деякі асимптотичні порівняльні оцінки, наприклад, інформаційно-ентропійні міри даних розподілів імовірності [15,16].

Згідно моделям, запропонованим в [22,23], безперервний часовий інтервал, на якому відбувається передача даних, розбивається на віртуальні слоти. У кожному слоті може взагалі не бути пакету (жодна із станцій мережі не веде передачу), або один пакет (одна і лише одна станція веде передачу), або мати

місце колізія, коли передавати намагаються дві або більш станцій.

Хай на початку кожного слота  $t_k$   $j$ -а станція пробує відправити пакет. Імовірність спроби позначається  $p_{kj}$ . Якщо спроба виявилася невдалою, після деякого інтервалу відстрочення  $\tau_d(n_{tr})$  вона повторюється. Загальна тривалість інтервалу відстрочення не залежить від числа спроб передачі  $n_{tr} = 0, 1, 2, K$  аж до настання події успішної передачі. Величина  $\tau_d(n_{tr})$  вибирається з геометричного розподілу з параметром, тобто  $\tau_d(n_{tr}) = 0, 1, 2, K$  з відповідними імовірностями  $\tau_d(0), \tau_d(0)[1 - \tau_d(0)], \tau_d(0)[1 - \tau_d(0)]^2, \dots$

Шкала часу – дискретна, а кожен тип слота є цілим числом коротких (елементарних) інтервалів. Оскільки станція робить спробу передачі на початку слота, імовірність колізії і число повторних спроб не залежать від тривалості пакету. Як наголошувалося вище, найзагальнішою мірою для розподілів імовірності, що належать, принаймні, до одного типу (у даному випадку – до дискретного типу), є ентропія. Далі приведені порівняльні ентропійні характеристики модельних розподілів [37].

1. Геометричний розподіл нерозривно пов'язаний з біноміальним. Відмінність полягає у тому, що біноміальна випадкова величина визначає імовірність  $m$  успіхів у  $n$  випробуваннях, а геометрична - імовірність  $n$  успіхів у  $n$  випробувань до першого успіху (включаючи перший успіх).

2. Рівномірно розподілена на  $[-a, a]$  випадкова величина має щонайвищу ентропію серед всіх випадкових величин, розподілених на  $[-a, a]$ .

3. Показовий розподіл з параметром  $\lambda$  має найбільшу ентропію серед всіх розподілів, визначених на напівосі  $[0, \infty]$  з математичним очікуванням  $\lambda$ .

4. На всій прямій, серед всіх розподілів з фіксованим математичним очікуванням і дисперсією, найбільшою ентропією володіє нормальний розподіл.

Інформаційна ентропія геометричного розподілу

$$H_G(x) = -\log_2 p - \frac{q}{p} \log_2 q.$$

Диференціальна інформаційна ентропія гауссовського розподілу

$$H_N(x) = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(x-a)^2}{2\sigma^2}\right] \ln \left\{ \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(x-a)^2}{2\sigma^2}\right] \right\} dx = \log_2(\sigma\sqrt{2\pi e})$$

Ентропія дискретного джерела завжди позитивна. Диференціальна ентропія  $H(x)$  на відміну від ентропії джерел дискретних повідомлень може приймати позитивні, негативні і нульові значення, тобто може бути і негативною [10]. Диференціальна ентропія на відміну від звичної ентропії дискретного джерела не є мірою власної інформації, що міститься в ансамблі значень випадкової величини. Вона залежить від масштабу  $x$  і може приймати негативні значення, тому що інформаційний сенс має не абсолютне значення диференціальної ентропії, а різниця двох диференціальних ентропій, чим і пояснюється її назва.

Диференціальна ентропія не міняється при зміні всіх можливих значень випадкової величини на постійну величину. Дійсно, масштаб  $x$  при цьому не міняється, і справедлива рівність

$$h(x+C) = -\int_{-\infty}^{\infty} w(x+C) \log_2 w(x+C) d(x+C) = -\int_{-\infty}^{\infty} w(x) \log_2 w(x) dx.$$

З цього виходить, що не залежить від математичного очікування випадкової величини, оскільки змінюючи всі значення  $x$  на  $x+C$ , тим самим змінюється на  $C$  і її середнє, тобто математичне очікування.

Диференціальна ентропія адитивна, тобто для об'єднання  $x \cup y$  незалежних випадкових величин  $x$  і  $y$  справедлива рівність:

$$H(x \cup y) = H(x) + H(y).$$

Доказ цієї властивості аналогічно доказу властивості адитивності звичайної ентропії.

Для порівняння результатів моделей [20] і [21] слід розглянути інформаційні характеристики модельних розподілів [35,36].



У разі геометричного розподілу проводяться незалежні повторні випробування до появи "успіху". Для обчислення ентропії  $H_G(x)$  складається діаграма станів з імовірністю «успіху»  $p < 1$  і «неуспіху»  $q < 1$ . Очевидно,  $p + q = 1$ .

Система знаходиться в початковому стані  $s_0$ . Досягши успіху вона переходить в неповоротний (поглинаючий) стан  $s_f$  (рис. 3.3). Таким чином, випадковий процес є не транзитивним (не перехідним в попередній стан).

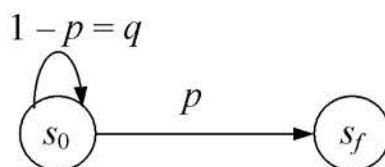


Рисунок 3.3. Стани системи

Граф переходів має наступний вигляд (рис. 3.4).

$s_+$  – перехідний стан при успіху випробування;  $s_-$  – перехідний стан при неуспіху випробування;  $H_{G_i}(x)$ ,  $i=1,2,K,n,K$  – ентропія розподілу досягши успіху на  $-y$  кроці.

Тоді поточна ентропія геометричного розподілу може бути розрахована по наступних формулах:

$$\begin{aligned}
 H_G(x) &= -p \log_2 p - pq \log_2(pq) - pq^2 \log_2(pq^2) - K - pq^{n-1} \log_2(pq^{n-1}) - K = \\
 &= -(1 + q + q^2 + K + q^{n-1} + K) p \log_2 p - pq(1 + 2q + 3q^2 + K + nq^{n-1}) \log_2 q; \\
 1 + q + q^2 + K + q^{n-1} + K &= \frac{1}{1-q};
 \end{aligned}$$

$$\begin{aligned}
& 1 + 2q + 3q^2 + K + nq^{n-1} + (n+1)q^n = \\
& = 1 + q + q^2 + K + q^{n-1} + K + q + 2q^2 + K + (n-1)q^{n-1} + nq^n K = \\
& = \frac{1}{1-q} + q(1 + 2q + 3q^2 + K + nq^{n-1}) = K = \frac{1}{1-q} + q\frac{1}{1-q} + q^2\frac{1}{1-q} + K = \frac{1}{(1-q)^2}.
\end{aligned}$$

$$H_G(x) = -\log_2 p - pq \frac{1}{(1-q)^2} \log_2 q = -\log_2 p - \frac{q}{p} \log_2 q.$$

Була розрахована залежність ентропії геометричного розподілу від імовірності  $p$  успішної передачі даних однієї із станцій (рис.3.5). Видно, що при завданні вищої імовірності успіху ентропія розподілу знижується, отже, потрібний ресурс для обміну даними зменшується.

Проте це досягається тільки при зменшенні імовірності колізій в мережі. Досягти цього можна, наприклад, ціною обмеження такого ключового показника ефективності, як максимальна тривалість пакетів, що передаються.

Для порівняння розрахована залежність диференціальної ентропії від середньоквадратичного відхилення інтервалу передачі від максимально допустимого (рис. 3.6). Спостерігається монотонне зростання ентропії, отже, зростання потрібного ресурсу обміну даними.

Для аналізу впливу фактору самоподібності мережного трафіку виведено вираз для поточної ентропії розподілу Парето як типового розподілу з «важкими хвостами», характерного для самоподібного трафіку:

$$H_P(x) = c \frac{\log_2 c}{\ln 2} \times \frac{x^{-c}}{-c-1} + (c-1) \left[ x^{-c} \log_2 x - \frac{x^{-c}}{c \ln 2} \right], \text{ де } c - \text{ параметр форми.}$$

На рис. 3.7 зображені графіки диференціальної ентропії розподілу Парето для параметрів форми  $c=0,5$  і  $c=1$ . Видно, що при зміні значень  $x$  ентропія спочатку убуває, а потім зростає, що пояснюється впливом «важкого хвоста» розподілу.

Слід відзначити, що при розрахунку ентропійних мір можна використовувати різні параметри модельних розподілів. При цьому порівняльні оцінки, засновані на ентропії, будуть достатньо універсальними і наочними.

На закінчення необхідно відзначити головну перевагу описаного методу: він дозволяє ефективно використовувати приведені методики в дослідженні бездротових локальних мереж, що працюють в насиченні (при високому навантаженні), для їх аналітичного моделювання при довільному (зокрема, нормальній) навантаженні.

## 4. МЕТОДИ ОЦІНЮВАННЯ ПОКАЗНИКІВ ПРОДУКТИВНОСТІ МЕРЕЖІ З УРАХУВАННЯМ ЗАВАД

### 4.1. Методика моделювання і аналізу результатів

Застосуємо розроблені вище аналітичні моделі для оцінки впливу параметрів трафіку, конфігурації мережі і інтенсивності завад на показники продуктивності, а також для обґрунтування раціонального вибору керованих параметрів протоколу.

В існуючих мережах можна виділити наступні методи технічного обслуговування: профілактичний, відновний і статистичний. Кожний з них має певні переваги і недоліки перед іншими, тому використовуються різні поєднання методів. Проте у зв'язку з підвищенням надійності вся більша перевага в сучасних мережах одержує статистичний метод обслуговування, суть якого полягає у тому, що ремонтно-відновні роботи починаються після того, як якість функціонування досягла критичного значення. Елементи мережі піддаються технічній діагностиці для отримання інформації про стан елементів мережі. При погіршенні якості функціонування вони, як правило, виводяться з робочої конфігурації для відновлення працездатності. Дана методика дозволяє виключити багато видів дефектів, які звичайно виникають при профілактичному обслуговуванні у зв'язку з демонтажем і іншими роботами, а в мережі і її елементах допустиме деяке число несправностей, що не приводять до припинення правильного функціонування завдяки наявності надмірності.

Доцільність застосування статистичного методу технічного обслуговування в бездротових мережах визначається в основному двома чинниками: розвиненою системою контролю і діагностики і використанням в елементах мережі високонадійної елементної бази.

Функціонування мережі відбувається в умовах постійної дії різного роду обурень. Це може приводити до перевантаження вузлів комутації і каналів зв'язку, виникнення помилок в повідомленнях, що передаються.

Ефективність і якість роботи будь-якої інформаційно-обчислювальної системи практично повністю визначають три найважливіші властивості – точність, надійність і достовірність доставки інформації. Спеціалізовані безпроводові мережі (мережі спеціального і критичного застосування) мають свою специфіку [11]. По-перше, до якості передачі інформації, циркулюючої в мережі, як правило, пред'являються особливі вимоги, зокрема, допустима імовірність помилок значно менше, ніж в звичних мережах. По-друге, часто безпосередній доступ до мережі для вирішення задач контролю, діагностики і усунення несправностей вузлів і елементів мережі утруднений або взагалі неможливий. Тому задача непрямой оцінки продуктивності спеціалізованих мереж залежно від їх завадозахищеності є актуальною.

Розглянемо спеціалізовану безпроводову мережу без інфраструктури (мережа *Ad Hoc*). Такі мережі широко застосовуються для вирішення обмеженого круга задач в умовах великих перепадів навантаження, наявності інтенсивних перешкод. При цьому потрібна гарантована якість обміну даними.

В умовах стабільно високого навантаження на мережу правомірним є допущення про статистичну незалежність процесів функціонування окремих вузлів [2]. Проте таке допущення може привести до істотних погрішностей при оцінці продуктивності мереж, що працюють в умовах змін навантаження в широких межах [25,26]. Зокрема, якщо черга заявок на  $i$ -й вузол велика (вхідний буфер зберігання заявок близький до заповнення), то висока імовірність, що на інтервалі доступу до  $i$ -го вузла на  $j$ -й вузол також поступить пакет. З урахуванням викладеного необхідно враховувати взаємозалежність процесів, що протікають в різних вузлах мережі.

Розглянемо мережу, що складається із  $N$  статистично однорідних вузлів, у вхідний буфер кожного з яких поступає потік пакетів з середньою інтенсивністю  $\lambda$ . Параметри пакетів однакові і постійні на інтервалі спостереження; канал вважається ідеальним, а час розповсюдження сигналу між вузлами – нехтує малим. Крім того, передбачається, що в буферній пам'яті кожного вузла може зберігатися не

більш  $R$  пакетів. Відмова в обслуговуванні відбувається за наступних умов:

- при повному заповненні вхідного буфера;
- при закінченні часу життя пакету;
- при вичерпанні спроб передачі пакету.

Така модель, не дивлячись на зовнішню простоту, цілком адекватно відображає реальну ситуацію обслуговування сумарних потоків, що приходять від різних джерел на один вузол-приймач. При підсумовуванні інтенсивностей окремих потоків з довільними розподілами імовірності результуюча щільність імовірності асимптотика сходиться до пуассонівської. Це пояснюється тим фактом, що пуассонівський розподіл відноситься до класу статистично стійких [44].

Необхідно оцінити наступні показники продуктивності:

- середнє значення  $\tau_d$  часу затримки пакету, відлічуваного від моменту надходження пакету в чергу даного вузла і до моменту закінчення його обслуговування, тобто після закінчення інтервалу, завершального успішну передачу, або інтервалу до моменту останньої невдалої спроби передачі, що приводить до втрати пакету;
- імовірність відмови в передачі пакету, що відбувається або переповнювання черги станції, або через досягнення максимального числа повторних передач.

Адекватною моделлю процесу обміну даними в мережі з взаємозв'язаними вузлами є процес загибелі і розмноження [40, 25], схема якого зображена на рис. 4.1. Стан цього процесу визначається сумарним числом  $R_{\Sigma}$  пакетів, що знаходяться в чергах станцій мережі, включаючи пакети, які передаються у нинішній момент. Періодом відліків є інтервал часу, що виділяється для кожного вузла. На рис. 4.1 не показані цикли, коли система залишається в тому ж самому стані, оскільки можна вважати, що імовірності таких подій для реально функціонуючих мереж можна вважати величинами другого порядку малості в порівнянні з імовірністю переходів із стану в стан [25].

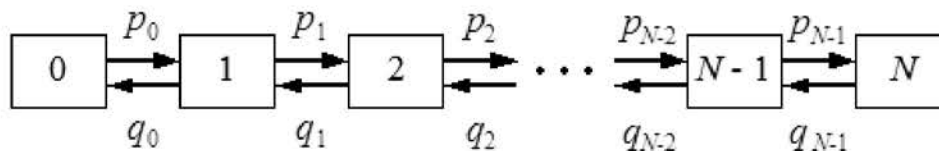


Рисунок 4.1. Граф процесу обміну даними

Для визначення імовірності розмноження, тобто збільшення  $R_{\Sigma}$  на одиницю і загибелі, тобто зменшення  $R_{\Sigma}$  на одиницю протягом виділеного інтервалу, введемо наступні допущення.

1. Протягом відведеного інтервалу часу передачі даних у вхідні буфери вузлів може поступити не більш один пакет.

2. При виникненні колізії, коли два або більш вузлів одночасно намагаються здійснити передачу, відмова в подальшій передачі пакету може відбутися не більше ніж на одному з вузлів, залучених в колізію (імовірність одночасної відмови на двох і більш вузлах нехтує мала).

При  $R_{\Sigma} = 0$  розмноження відбувається, коли один з вузлів успішно здійснює передачу в довільний момент часу, а під час цієї передачі в буфер даного або будь-якого іншого вузла поступає ще один пакет. Тривалість цієї успішної передачі рівна

$$t_S = t_H + t_D + t_{ACK} + \sum_i t_{di} = \frac{L_H + L_D + L_{ACK}}{V_{tr}} + \sum_i t_{di}, \quad (4.1)$$

де  $L_H, L_D$  – довжина заголовка і поля даних пакету відповідно;  $L_{ACK}$  – довжина кадру підтвердження (*ACKnowledgement*);  $t_{di}$  – захисні інтервали після передачі кадру підтвердження і успішної передачі власне пакету даних.

З урахуванням викладеного вища імовірність розмноження при  $R_{\Sigma} = 0$

$$p_0 = (1 - e^{-N\lambda t_e})(1 - e^{-N\lambda t_S}),$$

де  $t_e$  – середня тривалість порожнього інтервалу, на якому жоден вузол не здійснює передачу.



При  $R_\Sigma > 0$  розмноження відбувається за наступних умов:

- коли новий пакет знаходить вільне місце в буфері;
- при успішній передачі на інтервалі, наданого даному вузлу;
- при успішній довільній передачі;
- на інтервалі колізії, в кінці якого не відбувається відмова в подальшій передачі пакету ні на одній із станцій, залучених в колізію.

Загибель має місце, коли протягом успішної передачі слота або колізії, що приводить до відмови в подальшій передачі пакету, не поступає новий пакет.

Отже, при  $R_\Sigma > 0$

$$p_{R_\Sigma} = \sum_{n=n_{\min}(R_\Sigma)}^{\min(N, R_\Sigma)} \gamma(n, R_\Sigma) \left\{ [1 - \beta_q^e(n, R_\Sigma)] p_c(n) (1 - e^{-n\lambda_e}) + [1 - \beta_q^f(n, R_\Sigma)] [p_\alpha(n) (1 - e^{-N\lambda_s}) + p_c(n) [1 - \beta(n)] (1 - e^{-N\lambda_c})] \right\}. \quad (4.2)$$

Тут

$$n_{\min}(n, R_\Sigma) = \lceil (R_\Sigma - 1) / B \rceil + 1,$$

де  $\lceil x \rceil$  – ціла частина числа  $x$ ;  $\gamma(n, R_\Sigma)$  – імовірність наявності  $n$  активних станцій за умови, що сума довжини черг на початку інтервалу рівна  $R_\Sigma$ ;  $\beta_q^e(n, R_\Sigma)$  і  $\beta_q^f(n, R_\Sigma)$  – імовірність втрати через переповнювання буфера, в який поступає новий пакет, при даних  $n$  і  $R_\Sigma$ . Ця імовірність різна для порожнього інтервалу ( $\beta_q^e$ ) і для решти інтервалів, оскільки за визначенням протягом порожнього інтервалу пакети можуть поступати тільки в буфери активних станцій. Крім того, очевидно, що ця імовірність рівна 0 при  $R_\Sigma < n + B - 1$ ;  $\beta(n)$  – імовірність відмови через досягнення граничного числа  $M_r$  повторних передач при даному числі активних станцій; передбачається, що лічильник  $m_r$ ,  $m_r$  тільки однієї із станцій, що беруть участь в колізії, може досягти межі  $M_r$ ;  $t_c = \frac{L_D}{V} + t_u$  – час колізії, в яке входить захисний інтервал після останньої невдалої спроби передачі і, як

результат – втрати пакету.

Стационарні імовірності  $\pi(R_\Sigma)$  станів даного процесу описується виразами:

$$\pi(R_\Sigma) = \pi(0) \prod_{i=1}^N \frac{p_{i-1}}{q_i}; \quad \pi(0) = \frac{1}{1 + \sum_{j=1}^{NR} \prod_{i=1}^N \frac{p_{i-1}}{q_i}}. \quad (4.3)$$

Для оцінки імовірності  $\gamma(n, R_\Sigma)$  і  $\beta(n, R_\Sigma)$  прийнемо наступне допущення. Хай сумарне число  $R_\Sigma$  пакетів, що знаходяться в чергах станцій мережі, більше нуля. Тоді всі варіанти розміщення цих  $R_\Sigma$  пакетів по  $N$  буферах вузлів мережі мають однакову імовірність.

Використовуючи це припущення, знаходимо для випадку  $0 \leq R_\Sigma \leq NR$  і  $n_{\min}(R_\Sigma) \leq n \leq \min(N, R_\Sigma)$ :

$$\gamma(n, R_\Sigma) = \frac{1}{g[R_\Sigma, N, R]} C_n^N g[R_\Sigma - n, n, R - 1];$$

$$\beta_q^f(n, R_\Sigma) = \begin{cases} 0, & R_\Sigma < n + R - 1; \\ \beta_q^f(n, R_\Sigma) = \frac{1}{g[R_\Sigma - n, n, R - 1]} \sum_{k=k_{\min}(R_\Sigma, n)}^{K(1, n)} \frac{k}{N} C_k^n g[R_\Sigma - n - k(R - 1), n - k, R - 2], & R_\Sigma \geq n + R - 1. \end{cases} \quad (4.4)$$

Функція  $\beta_q^f(n, R_\Sigma)$  визначається аналогічно шляхом заміни  $\frac{k}{N}$  на  $\frac{k}{n}$  у виразі

(4.4). Тут  $C_n^N = \frac{N!}{(N - n)!n!}$ , а  $g[u, v, K]$  – число варіантів, якими можна розмістити

$u$  куль, що не розрізняються, по  $v$  урнах так, що в будь-якій урні було б не більш  $K$  куль [33];  $k_{\min}(R_\Sigma, n) = \max[1, R_\Sigma - n(R - 1)]$ , а  $k(R_\Sigma, n)$  – найбільше цілі,

не перевищуючі відносини  $\frac{R_\Sigma - n}{R - 1}$ . Функція  $g[u, v, K]$  обчислюється рекурсивно:

$$g[0, v, K] = 1 \quad \text{при} \quad \text{всіх} \quad \text{при} \quad u \leq K \quad \text{і} \quad g[u, 1, K] = 0 \quad \text{при} \quad u > K;$$

$$g[u, v, K] = \sum_{k=0}^{\min(u, K)} g[u - k, v - 1, K] \quad \text{при} \quad v \geq 2, \quad u > 0.$$

Для знаходження імовірності відмови  $\beta(n)$  в доступі до вузла прийнемо

таке припущення. Хай на початку даного часового інтервалу число активних станцій рівне  $n$ . Тоді для будь-якої з цих станцій імовірність  $\rho(n)$  початку дозволеної передачі, а також імовірність відмови  $\beta(n)$  у разі колізії в цьому інтервалі співпадають з відповідними значеннями, одержаними для мережі, що включає  $n$  постійно активних вузлів. Інші  $N - n$  вузлів в цій мережі можуть передавати тільки довільно за умови, що ні з одного з активних вузлів передача не відбувається. Якщо пакет поступає в буфер одного з  $N - n$  неактивних вузлів у момент передачі будь-якого з активних вузлів, то цей пакет втрачається.

Імовірність того, що поточна дозволена спроба невдала через колізію, рівна

$$\chi(n) = 1 - [1 - \tau(n)]^{n-1}, \quad (4.5)$$

а імовірність того, що дана невдача –  $m$ -а по рахунку, рівна  $\beta_m(n) = [\chi(n)]^{m-1}$ .

Слідуючи Д. Ліндлі [34], нехтуючи імовірністю колізії більш ніж двох станцій і імовірністю одночасної відмови на декількох станціях, одержуємо наступну імовірність відмови:

$$\beta(n) = 2\beta_m(n). \quad (4.6)$$

Значення  $\rho(n)$  знаходиться шляхом розв'язання системи рівнянь виду

$$\rho(n) = \frac{2}{E[\zeta] + 1}, \quad (4.7)$$

де  $E[\zeta] = \left\{ \sum_{i=1}^m \chi^{i-1} w_i + \frac{\chi^m w_m - w_0}{1 - \chi} \right\} \frac{(1 - \chi)^m}{1 - \chi^m}$  – середнє значення розміру

конкурентного інтервалу у випадку  $M_r \leq m$   $M_r \leq m$  і

$$E[w] = \left\{ \sum_{i=1}^m \chi^{i-1} w_i + w_m \sum_{i=m}^{M_r-1} (i - m + 2) \chi^i + \frac{(M_r - m + 1) w_m \chi^{M_r} - w_0}{1 - \chi} \right\} \frac{(1 - \chi)^2}{1 - \chi^{M_r}}$$

(4.8)

при  $M_r > m$ .

## 4.2. Результати розрахунків параметрів мережі з використанням комп'ютерної моделі

У якості ключового показника продуктивності вибрана імовірність відмови в загальному доступі. Для дослідження впливу завад на імовірність відмови з використанням математичної моделі, розробленої в попередньому розділі, вибране граничне число невдалих спроб передачі коротких пакетів. Довжина пакету постійна і не перевищує (в середньому) 0,1 довжини дозволеного інтервалу передачі. При таких початкових даних залежності впливу перешкод є найбільш наочними і носять узагальнений характер.

У табл. 4.1 приведені деякі чисельні параметри моделі.

На рис. 4.2 зображені розрахункові залежності імовірності відмови в доступі до вузла від величини відносної інтенсивності перешкод. Імовірність відмови зростає як при підвищенні інтенсивності потоку пакетів, так і при збільшенні інтенсивності завад.

Для порівняння приведемо залежності імовірності відмови в доступі до обслуговування при різних значеннях  $m$  (див. рис. 4.3).

При раціональному виборі числа спроб повторної передачі вдається понизити імовірність відмови. Особливо помітний вииграш має місце при малому сумарному навантаженні на мережу і малому відносному рівні завад.

Таким чином, необхідно вибирати параметри спеціалізованої бездротової мережі на основі результатів аналізу її архітектури. Зокрема, при визначенні кількості спроб передачі необхідно враховувати об'єм (число вузлів) мережі, навантаження на мережу і завадову обстановку в зоні дії мережі.

Піддамо аналізу оцінку точності моделей, яку проведемо для випадку ідеального каналу за відсутності завад шляхом порівняння результатів, одержаних аналітично і за допомогою імітаційного моделювання. На рис. 4.6 і 4.7 представлені деякі результати оцінки середнього часу обслуговування  $T_{\text{норм}}$  і середнього часу затримки  $T_{\text{МС}}$  при варіюванні інтенсивності надходження пакетів  $\lambda$  для випадків  $N=15$  і  $N=32$  з використанням  $RTS$ -границі  $L=576$

байт.

Результати, одержані як аналітично (суцільні лінії), так і імітаційно (штрихові лінії), демонструють порогообразний характер залежностей  $T(\lambda)$  і  $T_{MAC}(\lambda)$ : із збільшенням  $\lambda$  значення  $T$  і  $T_{MAC}$  спочатку поволі ростуть, що відповідає періоду нормального навантаження на мережу, а потім після короткого перехідного періоду, який тим коротше, чим більше число станцій  $N$ , стають рівним деяким граничним значенням, відповідним випадку високого навантаження.

Видно, що як при нормальній, так і при високому навантаженні аналітична модель досить точна: погрішності не перевищують 8%.

Великі розбіжності значень показників продуктивності, одержаних аналітично і імітаційно, спостерігаються тільки в короткий перехідний період: у аналітичних кривих поріг різкіший (майже вертикальний).

Застосуємо розроблений аналітичний метод для вибору *RTS/CTS*-границі  $L$ , при якій мінімізується показник  $T$ . На рис. 4.6 показані залежності оптимальної межі  $L_{opt}$  від інтенсивності  $\lambda$  при різних  $N$ .

Ці залежності також порогообразні: до деякого порогу мережа працює в режимі нормального навантаження, імовірність колізії мала і тому оптимальний механізм базового доступу, тобто  $L_{opt} = 2000$ , оскільки всі пакети не довщі 2000 байт. Після цього порогу, який тим різкіше, чим більше  $N$ , межа  $L_{opt}$  встановлюється рівною фіксованому значенню, залежному від  $N$ .

Результати застосування цього оптимізованого гібридного методу доступу порівняно з сценаріями, коли для всіх пакетів використовується або тільки механізм базового доступу (а), або тільки механізм *RTS/CTS* (б), показані на рис. 4.7.

З рис. 4.7 видно, що для будь-якої інтенсивності  $\lambda$  така оптимізація дозволяє лише трохи поліпшити значення  $T$  в порівнянні з мінімумом із значень, відповідним сценаріям (а) і (б). Це означає, що доцільно використовувати

наступну стратегію, використовуючи тільки розроблений аналітичний метод:

а) знайти оптимум  $L_{opt}(N)$  для режиму високого навантаження і відповідне йому значення  $T_{opt}(N)$ ;

б) вибрати поріг  $\lambda_i(N)$  якому відповідає значення  $T$ , менше  $T_{opt}$  на  $d\%$ ;

в) застосовувати механізм базового доступу при  $\lambda < \lambda_i(N)$  і гібридний механізм з границею  $L = L_{opt}(N)$  при  $\lambda \geq \lambda_i(N)$ .

Наприклад, виберемо  $d=5\%$ . Тоді при  $N=40$  маємо  $L_{opt}(N) = 453$ ,  $T_{opt}(N) = 68,2$  мс і  $\lambda_i(N) \approx 16$  с<sup>-1</sup>. Порівняємо значення  $T$ , одержані за допомогою імітаційної моделі при  $\lambda = \lambda_i(N)$ : для механізму базового доступу  $T = 63,9$  мс, а для гібридного механізму  $T = 62$  мс, тобто значення  $T$  при інтенсивності  $\lambda_i(N)$ , знайденої аналітично, практично співпадають з результатами моделювання, отже, ця інтенсивність  $T$  дійсно є пороговою.

### 4.3. Оцінка впливу завад на характеристики мережі

Розглянемо випадок, коли канал не ідеальний і завади погіршують продуктивність мережі. Одним із наслідків впливу завад є зростання імовірності відмови, яка відбувається з двох причин:

– збільшується середній час обслуговування пакету, що веде до збільшення імовірності переповнювання черги;

– росте імовірність невдалої передачі пакету через його спотворення, джерелами якого тепер є не тільки колізії, але і радіозавади, а, отже, збільшується і імовірність відмови в подальшій передачі пакету через досягнення граничного числа спроб.

Значення імовірності відмови має велике значення для роботи мережних протоколів транспортного рівня. Зокрема, в протоколі TCP відмова в передачі пакету, тобто неотримання пакету протягом тайм-ауту істотно знижує

продуктивність транспортного з'єднання зважаючи на:

- а) зниження (принаймні, в 2 рази) довжини вікна передачі;
- б) збільшення тайм-ауту.

У зв'язку з цим у якості ключового показника продуктивності, досліджуваного в даному розділі, вибрана імовірність відмови. Як вже було показано в розділі 1, граничні значення  $N_s$  та  $N_d$  числа невдалих спроб передачі коротких і довгих кадрів відповідно надають значний вплив на імовірність втрати пакету. Якщо вони малі, пакет з великою імовірністю втрачається через вичерпання допустимого числа спроб передачі. Їх велике значення може збільшувати середній час обслуговування пакету і, отже, привести до зростання імовірності втрати пакету через переповнювання черги. У даному розділі ми чисельно досліджуватимемо випадок, коли всі пакети передаються за допомогою механізму базового доступу. Тому як керований параметр, який ми оптимізуватимемо, виберемо граничне число невдалих спроб передачі коротких кадрів  $N_s = m$ . Це, зокрема, дозволить використовувати аналітичну модель, розроблену в розділі 2.

Отже, дослідимо вплив інтенсивності завад BER на імовірність відмови  $P_{rej}$ , варіюючи так само решту параметрів трафіку і конфігурації мережі.

При отриманні результатів цього дослідження, представлених на рис. 4.8 довжина пакету  $l$  передбачалася постійною. Значення параметрів протоколу залишаються ті ж, що і в попередньому пункті.

Щоб знайти оптимум, дослідимо залежність імовірності відмови від максимального числа  $m$  спроб передачі, рис. 4.8, міняючи  $m$  від 1 до 20. Видно, що при малому навантаженні має сенс вибирати максимальне значення  $m$ , а для високого навантаження оптимальний вибір параметра  $m$  дозволяє істотно понизити імовірність відмови – до декількох разів.



#### 4.4. Розробка методу аналізу колізій у мережі з різномірним трафіком

Розглянемо далі задачу оцінювання імовірності виникнення колізії в мережі. Оскільки безпроводові мережі стандарту *IEEE 802.11x* будуються, як правило, за технологією *CSMA/CA*, проблема обмеження коефіцієнта використання мережі є ще гострішою з причин, пов'язаних саме з принципами роботи, закладеними в цій технології.

Як наголошувалося вище, при збільшенні коефіцієнта використання мережі – відношення пропускної спроможності до інтенсивності трафіку – все більша частина ресурсу витрачається на обробку колізій. При прагненні  $k_{исп}$  до одиниці прагнутиме до одиниці імовірність колізій і, відповідно, поява все нових і нових затримок передачі. Намагаючись обробляти колізії, мережа перестане пропускати корисну інформацію і працюватиме «на себе». При обґрунтуванні гранично допустимого коефіцієнта використання мережі необхідно враховувати ризик виникнення такої ситуації.

Хай до мережі підключено  $N$  комп'ютерів, які видають потоки пакетів з інтенсивностями  $\lambda_n(t)$ ,  $n = \overline{1, N}$ . Вважатимемо, що пакети, видавані  $n$ -м комп'ютером, мають тривалість  $\tau_n$ . Щоб не зв'язувати себе необхідністю точного обліку моменту появи кожного пакету, припустимо, що вони відбуваються у випадкові моменти часу з однаковим розподілом імовірності, і на кінцевому відрізку часу  $T \gg \tau_n$  утворюють потік Ерланга  $k$ -го порядку. Як відомо [40], задаючись порядком потоку Ерланга, можна одержати будь-який ступінь післядії: від повної взаємної незалежності між моментами появи подій при до детермінованого функціонального зв'язку при  $k \rightarrow \infty$ .

Хай в точці  $t_j$ , що знаходиться усередині інтервалу аналізу  $T$ , з'явився пакет  $f_j$  з тривалістю  $\tau_j$ . Імовірність появи цього пакету позначимо  $P(t_j)$ . Виведемо вираз для умовної щільності імовірності часткового перекриття пакету  $f_j$  іншим пакетом  $f_i$  з тривалістю  $\tau_i$ . Можливі положення пакетів зображені на рис. 4.9.

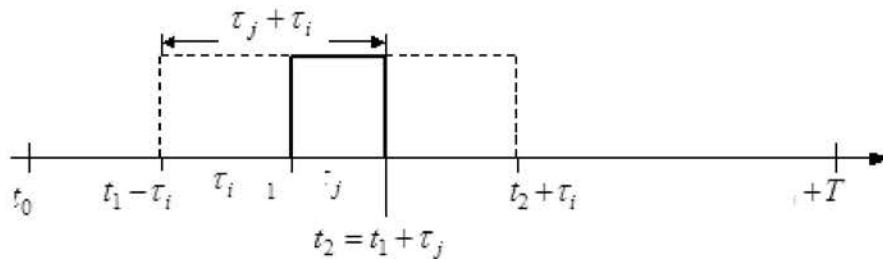


Рисунок 4.9. Можливі положення сигнальних слотів на часовій вісі

Вважатимемо, що перекриття відбувається вже при зіткненні пакетів. Тоді необхідно обчислити сумісну імовірність  $P(t_i, t_j)$  того, що пакет  $f_i$  потрапить в інтервал  $[t_1 - \tau_i, t_1 + \tau_j]$  за умови, що пакет  $f_j$  починається в точці  $t_1$ . З урахуванням часових співвідношень (див. рис. 4.10) ця імовірність визначається як

$$P(t_i, t_j) = P(t_1 - \tau_i \leq t \leq t_1 + \tau_j / t_1 = t_j) \quad (4.9)$$

Логічно припустити, що процеси появи в мережі пакетів, видаваних різними джерелами, взаємно незалежні, а моменти появи пакету  $f_j$  на інтервалі  $[t_0, t_0 + T]$  мають однакові імовірнісні характеристики. Тоді

$$P(t_i, t_j) = P(t_1 - \tau_i \leq t \leq t_1 + \tau_j / t_1 = t_j) = P(t_1 - \tau_i \leq t \leq t_1 + \tau_j) P(t_1), \quad (4.10)$$

$$\text{де } P(t_1) = P(0 \leq t_j < t_j + \tau_j \leq T) = \tau_j / T.$$

(4.11) імовірність того, що пакет  $f_j$  «накриє» інтервал тривалістю в якій-небудь точці  $t_j$ .

Покладемо, що у момент часу  $t_1 - \tau_i$  пакет  $f_i$  не спостерігається. Обчислимо імовірність  $P(t_1 - \tau_i \leq t_i \leq t_1 + \tau_j)$  появи  $i$ -го пакету за відрізок часу, використовуючи вирази для закону Ерланга  $k$ -го порядку [42], в яких для урахування нестационарності введемо змінну інтенсивність потоку  $\lambda_i(t)$ :

$$P(t_1 - \tau_i \leq t \leq t_1 + \tau_j) = \frac{\lambda_i(t_1 - \tau_i) (\lambda_i(t_1 - \tau_i + t) t)^{k-1}}{(k-1)!} \exp\left(-\int_{t_1 - \tau_i}^{t_1 + \tau_j} \lambda_i(t) dt\right). \quad (4.12)$$

Якщо вважати інтенсивність потоку  $\lambda_i(t)$  поволі змінною величиною, то можна з прийнятною точністю усереднити її на інтервалі інтегрування  $[t_1 - \tau_i, t_1 + \tau_j]$ :  $\lambda_i(t) \approx \lambda_{i\text{сеп}}$ .

Тоді вираз (4.12) спрощується:

$$P(t_1 - \tau_i \leq t \leq t_1 + \tau_j) = \frac{\lambda_{i\text{сеп}} (\lambda_{i\text{сеп}} t)^{k-1}}{(k-1)!} \exp(-\lambda_{i\text{сеп}}). \quad (4.13)$$

Після нескладних, але громіздких перетворень вираз (4.13) перетвориться для випадку самоподібного трафіку по аналогії з виразом (4.12):

$$P(t_1 - \tau_i \leq t \leq t_1 + \tau_j) = \frac{\lambda_{i\text{сеп}}^{1/2(1-H)} (\lambda_{i\text{сеп}}^{1/2(1-H)} t)^{k-1}}{(k-1)!} \exp[-\lambda_{i\text{сеп}} H/(1-H)], \quad (4.14)$$

де  $H$  - параметр Херста.

По формулах (4.12 – 4.14) розраховані залежності корисної пропускної спроможності мережі від коефіцієнта використання (рис. 4.10) для Пуассоновського трафіку і самоподібного трафіку з різними параметрами Херста. Під ідеальним трафіком ми розуміємо відсутність колізій. Видно, що продуктивність мережі помітно убуває вже при коефіцієнті використання, перевищуючому значення 0,3...0,4 (особливо для самоподібного трафіку).

Таким чином, коефіцієнт використання мережі не може бути дуже близький до одиниці, інакше корисна пропускна спроможність мережі різко впаде. Мережа або повторно передаватиме загублені пакети і квитанції, або оброблятиме колізії, тобто буде працювати «на себе». У жодному випадку не можна допускати неконтрольоване перевантаження мережі, тому що відновлення параметрів заявленої продуктивності мережі йде набагато повільніше, ніж їх падіння. Мережні фахівці говорять, що «мережа швидко лягає, але поволі встає». Такі ситуації тим більше недопустимі для систем критичного застосування. Тому для управління ресурсами і підтримки пропускної спроможності мережі в цілому на необхідному рівні необхідно перерозподіляти навантаження на окремі сегменти вже при появі найперших симптомів перевантаження, поки вона ще

контрольована [39].

При виявленні зростання коефіцієнту використання мережі треба включати механізми управління мережею при досягненні критичних коефіцієнтів використання, в залежності від степеню самоподібності трафіку.

## ВИСНОВКИ

У ході підготовки магістерської кваліфікаційної роботи здійснювався пошук методів: підйому пропускнуєї спроможності, підвищення завадостійкості, забезпечення якості передачі інформації, а також надійності функціонування безпроводних інформаційних систем – з постійними, змінними та випадковими параметрами; були отримані такі результати:

1. Створено аналітичну модель радіомережі з використанням протоколу IEEE 802/11, котра дозволила оцінювати продуктивність останньої як у режимі довільного навантаження так і враховувати особливості проявів протоколу в ідеальному каналі.

2. Дана аналітична модель модифікувалася під завдання забезпечення врахування впливу різноманітних перешкод і аналізу радіомереж, що побудовані з використанням різнотипових пристроїв. Вона також дозволила оцінювати продуктивність мережі в режимі довільного навантаження, причому враховує основні особливості протоколу та вплив різноманітних перешкод в радіоканалі та взаємовплив різних станцій, що діють у мережі. Таким чином, модель оцінює продуктивність комп'ютерної мережі при будь-якому режимі навантаження, враховуючи особливості згаданого вище протоколу, причому при взаємній залежності робочих станцій.

3. З використанням названих раніше аналітичних методів та в процесі імітаційного моделювання виконане цифрове порівняння продуктивності локальної мережі, що організована за протоколом IEEE 802.11. Дана оцінка доводить, що точність розрахунків, яка досягається є достатньою, а аналітичні моделі є ефективними.

4. Також вдалося виконати оцінку ефективності бездротових комп'ютерних мереж та виявлена явна кореляція ряду основних і додаткових показників ефективності комп'ютерних мереж. Даний аналіз системи ключових параметрів та їх застосування в інтересах управління якістю сервісу дозволяє стверджувати, що використовуючи статистичні методи можна встановити певні залежності між ключовими параметрами мережі, а останнє відкриває шлях до

створення системи керування якістю сервісу.

5. Були виявлені алгоритми оптимізації такого параметру протоколу, як поріг RST/CTS. Також було показано, що ці алгоритми можна покласти у підґрунтя створення системи автоматичного або хоча б напівавтоматичного налаштування протоколу та його продуктивності – а це шлях до досягнення оптимальних показників. При цьому стало зрозумілим, що потрібно обов'язково враховувати архітектуру мережі, статистику розподілів пакетів, наявність та інтенсивність перешкод, інтенсивність трафіку та ряд інших чинників.

6. Вдалось показати можливість використання інформаційно-ентропійних мір для оцінки продуктивності безпроводових комп'ютерних мереж. Виконання розрахунків звичної або диференціальної ентропії для модельних варіантів інтенсивності різноманітного мережевого трафіку дає широку картину узагальнених порівняльних характеристик функціонування мереж.

Підсумовуючи, є підстави вважати, що в магістерській роботі виконана розробка аналітичних методів і певне моделювання функціонування безпроводових комп'ютерних мереж побудованих на базі протоколу IEEE 802.11. Дослідження виконувались в умовах довільного навантаження за різноманітною статистикою трафіку, при цьому оцінювалася продуктивність мереж та питання оптимізації параметрів функціонування останніх. На цій підставі були розробленими певні заходи, що дозволять підвищити якість управління системами комп'ютерних мереж та модернізувати мережеві протоколи.

Таким чином, для оцінювання продуктивності комп'ютерних мереж, в тому разі безпроводних, потрібно різними методами виявляти функціональні а також статистичні зв'язки між характеристиками трафіку і характеристиками мережі. Саме на цьому напрямі, вочевидь, слід зосереджувати зусилля подальших досліджень.

Основними результатами роботи є розробка математичних моделей бездротових мереж з різноманітним подібним трафіком, а також методів оцінки характеристик процесів доступу в мережу.

**ПЕРЕЛІК ПОСИЛАНЬ**

1. Вишне夫斯基 В.М. Энциклопедия WiMAX. Путь к 4G / В.М. Вишне夫斯基, С.Л. Портной, И.В. Шахнович. – М.: Техносфера, 2009. – 472 с.
2. Филимонов А.Ю. Построение мультисервисных сетей Ethernet / А.Ю. Филимонов. – СПб.: БХВ-Петербург, 2007. – 592 с.
3. Столлингс В. Беспроводные линии связи и сети / В. Столлингс; пер. с англ. – М.: Вильямс, 2003. – 640 с.
4. Ярославцев А.Ф. Моделирование процессов передачи мультимедийного трафика в IP сети [Электронный ресурс] / А.Ф. Ярославцев // 2008. – Режим доступа: <http://nts.sibsubtis.ru/arc.php>. (дата звернення 02.12.2019)
5. Волков Л.Н. Системы цифровой радиосвязи: базовые методы и характеристики / Л.Н. Волков, М.С. Немировский, Ю.С. Шинаков. – М.: Эко-Трендз, 2005. – 392 с.
6. Торошанко Я.І. Ключові параметри ефективності безпроводових телекомунікаційних мереж та методи їх ідентифікації / Я.І. Торошанко, В.П. Грушевська, В.С. Шматко, М.С. Височіненко // Наукові записки Українського науково-дослідного інституту зв'язку. - 2014. - №3. - С. 28-33.
7. IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems: IEEE Std IEEE 802.16™ – 2009; Rev. of IEEE Std 802.16-2004. – N.-Y.: IEEE, 2009. – 68 p.
8. Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису: ДСТУ ISO/IEC 9798-3-2002. – Увед. 2003-01-01. – К.: Держспоживстандарт України, 2002. – 47 с.
9. Про електронний цифровий підпис [Електронний ресурс]: закон України від 22 травня 2003 р. № 852-IV / Верховна Рада України. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/852-15>. (дата звернення 02.12.2019)
10. Про електронні документи та електронний документообіг [Електронний ресурс]: закон України від 22 травня 2003 р. № 851-IV / Верховна Рада України. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/851-15>. (дата звернення



02.12.2019)

11. Безверщенко Е.В. Интеллектуальные технологии моделирования мультимедийного трафика / Е.В. Безверщенко, Е.А. Зубарева, Е.В. Шевцова // Интеллектуальні технології лінгвістичного аналізу: I міжнар. наук.-техн. конф., 6-8 жовтня 2008 р.: тези допов. – К.: НАУ, 2008. – С. 11.

12. Шевцова Є.В. Підвищення ефективності функціонування комп'ютерних мереж за рахунок удосконалення способів управління трафіком / Є.В. Шевцова, О.О. Зубарева // Комп'ютерні системи та мережні технології (CSNT-2011): IV міжнар. наук.-техн. конф., 14-16 червня 2011 р.: тези допов. – К.: НАУ, 2011. – С. 66.

13. Котельников В.А. Теория потенциальной помехоустойчивости / В.А. Котельников. – М.: Госэнергоиздат, 1956. – 153 с.

14. Про затвердження Плану використання радіочастотного ресурсу України [Електронний ресурс]: постанова Кабінету Міністрів України від 9 червня 2006 р. № 815 / Верховна Рада України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/815-2006-п>. (дата звернення 02.12.2019)

15. Аунг Мьо Маунг. Исследование и разработка алгоритмов планирования и приоритетного управления доступом в сетях WiMAX: дис. ... канд. техн. наук: 05.13.01 / Аунг Мьо Маунг. – М., 2010. – 148 с.

16. Про радіочастотний ресурс України [Електронний ресурс]: закон України від 1 червня 2000 р. № 1770-III / Верховна Рада України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1770-14>. (дата звернення 02.12.2019)

17. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2001. – 672 с.

18. Andrews J. Fundamentals of WIMAX: Understanding Broadband Wireless Networking / Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed. – [N. a.]: Prentice Hall, 2007. – 496 p.

19. Principles of Communication System Simulation with Wireless Applications / W.H. Tranter, K.S. Shanmugam, T.S. Rappaport, K.L. Kosbar. – [N. a.]: Prentice Hall, 2004. – 800 p.

20. ITU-T Recommendation Y.2001 (12/2004). General overview of NGN [Electronic resource] // December 2004. – Mode of access: <http://www.itu.int/itu->

t/recommendations/index.aspx?ser=Y.

21. Broadband Wireless Networks / [Вишне夫斯基 В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.]. – М.: Техносфера, 2005. – 592 с.

22. Стеклов В.К. Проектирование телекоммуникационных сетей / В.К. Стеклов, М.С. Беркман. – К.: Техніка, 2002. – 792 с.

23. ITU-T Recommendation E.800 (09/2008). Definitions of terms related to quality of service [Electronic resource] // September 2008. – Mode of access: <http://www.itu.int/itu-t/recommendations/index.aspx?ser=E>. (дата звернення 02.12.2019)

24. Олифер В.Г. Новые технологии и оборудование IP-сетей / В.Г. Олифер, Н.А. Олифер. – СПб.: БХВ-Петербург, 2000. – 512 с.

25. Слепов Н.Н. Современные технологии цифровых оптоволоконных сетей связи (ATM, PDH, SDH, SONET и WDM) / Н.Н. Слепов. – М.: Радио и связь, 2000. – 468 с.

26. ITU-T Recommendation Q.825 (1998). Specification of TMN applications at the Q3 interface: Call detail recording [Electronic resource] // 1998. – Mode of access: <http://www.itu.int/itu-t/recommendations/index.aspx?ser=Q>. (дата звернення 02.12.2019)

27. ITU-T Recommendation G.1010 (11/2001). End-user multimedia QoS categories [Electronic resource] // November 2001. – Mode of access: <http://www.itu.int/itu-t/recommendations/index.aspx?ser=G>. (дата звернення 02.12.2019)

28. RFC 2474 «Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers» [Electronic resource] / Internet Engineering Task Force, 1998. – Mode of access: <http://www.rfc-editor.org/info/rfc2474>. (дата звернення 02.12.2019)

29. RFC 2475 «An Architecture for Differentiated Services» [Electronic resource] / Internet Engineering Task Force, 1998. – Mode of access: <http://www.rfc-editor.org/info/rfc2475>. (дата звернення 02.12.2019)

30. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.

31. Джонс К.Дж. Анти – хакер. Средства защиты компьютерных сетей.

Справочник профессионала / К.Дж. Джонс, М. Шема, Б.С. Джонсон. – М.: СП ЭКОМ, 2003. – 688 с.

32. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения: ГОСТ Р 53110-2008. – Введ. 2009-10-01. – М.: Ростехрегулирования, 2009. – 22 с.

33. RFC 5758 «Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA» [Electronic resource] / Internet Engineering Task Force, 2010. – Mode of access: <http://www.rfc-editor.org/info/rfc5758>. (дата звернения 02.12.2019)

34. RFC 2459 «Internet X.509 Public Key Infrastructure Certificate and CRL Profile» [Electronic resource] / Internet Engineering Task Force, 1999. – Mode of access: <http://www.rfc-editor.org/info/rfc2459>. (дата звернения 02.12.2019)

35. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: ГОСТ Р 34.10-2001. – Введ. 2002-06-01. – М.: Ростехрегулирования, 2002. – 22 с.

36. RFC 5639 «Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation» [Electronic resource] // March 2010. – Mode of access: <http://www.rfc-editor.org/info/rfc5639>. (дата звернения 02.12.2019)

37. RFC 5480 «Elliptic Curve Cryptography Subject Public Key Information» [Electronic resource] / Internet Engineering Task Force, 2009. – Mode of access: <http://www.rfc-editor.org/info/rfc5480>. (дата звернения 02.12.2019)

38. Pat. 7986786 US, Int.Cl. (2006.01) H04L 9/00. Methods and systems for utilizing cryptographic functions for a cryptographic co-processor / Wael M. Ibrahim, Graeme J. Proudler, Liqun Chen, Manuel Novoa; assign. Hewlet-Packard Development Company. – № 11/565 075; filed 30.11.2006; date of pat. 26.07.2011.

39. Pat. 7372960 US, Int.Cl. (2006.01) H04L 9/00. Methods and apparatus for performing finite field calculations / Robert J. Lambert; assign. Certicom Corp. – № 10/058 212; filed 29.01.2002; date of pat. 13.05.2008.

40. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы / А.А. Чернов. – М.: Дашков и Ко, 2003. – 232 с.