Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Засоби та методи оцінювання характеристик якості безпровідних локальних мереж**

Виконав(ла): студент(ка) 6 курсу, групи СНм-61
спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

Лялик М.Д.
(підпис) (прізвище та ініціали)

Керівник Матійчук Л.П.
(підпис) (прізвище та ініціали)

Нормоконтроль Никитюк В.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри Боднарчук І. О.
(підпис) (прізвище та ініціали)

Рецензент Жаровський Р.О.
(підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 124 «Комп'ютерні науки»
(шифр і назва спеціальності)

студенту Лялик Микола Дмитрович
(прізвище, ім'я, по батькові)

1. Тема роботи Засоби та методи оцінювання характеристик якості безпровідних локальних мереж

Керівник роботи Матійчук Любомир Павлович, к.е.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*24*» *листопада* 2023 року № *4/7-1099*.

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Наукові публікації, електронні ресурси, підручники , посібники з тематики дослідження, щодо безпровідних локальних мереж.

4. Зміст роботи (перелік питань, які потрібно розробити) Вступ. 1.Технології та архітектура безпровідникових локальних мереж. 2. Особливості оцінок ефективності та математична модель оцінки продуктивності безпровідникових локальних мереж при довільному навантажені. 3. Реалізація програмного забезпечення для моделювання ефективності без провідникової локальної мережі. 4. Охорона праці та безпека в надзвичайних ситуаціях. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема 2. Мета та завдання дослідження. 3. Об'єкт та предмет дослідження. 4. Аналіз програмно-технічних засобів оцінки ефективності безпровідних локальних мереж. 5. Аналіз відомих аналітичних методів оцінки ефективності безпровідних локальних мереж. 6. Схема розподіленого управління DCF (Distributed Coordination Function). 7. Математична модель оцінки продуктивності безпровідних мереж при довільному навантаженні. 8. Математична модель оцінки ефективності безпровідних мереж при довільному навантажені (продовження). 9. Основні показники ефективності безпровідних локальних мереж, які оцінюються запропонованою моделлю. 10.Архітектура розробленого додатку. 11. Архітектура розробленого додатку. 12. Java аплет для моделювання функціонування безпровідної мережі. 13. Експериментальні дослідження з моделлю. 14. Висновки. 15. Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин Віктор Степанович		
Безпека в надзвичайних ситуаціях	Клепчик Василь Михайлович		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2023	*Виконано*
2.	Підбір наукових джерел щодо безпровідних локальних	26.11.2023-28.11.2023	*Виконано*
	мереж		
3.	Переклад та опрацювання наукових джерел щодо	29.11.2023-1.12.2023	*Виконано*
	безпровідних локальних мереж		
4.	Виконання дослідження щодо засобів та методів	2.12.2023-4.12.2023	*Виконано*
	оцінювання характеристик якості безпровідних локальних мереж		
5.	Оформлення розділу «Технології та архітектура	5.12.2023-7.12.2023	*Виконано*
	безпровідникових локальних мереж»		
6.	Оформлення розділу «Особливості оцінок	8.12.2023-10.12.2023	*Виконано*
	ефективності та математична модель оцінки		
	продуктивності безпровідникових локальних мереж		
	при довільному навантаженні»		
7.	Оформлення розділу «Реалізація програмного	11.12.2023-13.12.2023	*Виконано*
	забезпечення для моделювання ефективності без		
	провідникової локальної мережі»		
8.	Виконання завдання до підрозділу «Охорона праці»	14.12.2023-15.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.12.2023-17.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	18.12.2023-19.12.2023	*Виконано*
11.	Нормоконтроль	19.12.2023-20.12.2023	*Виконано*
12.	Перевірка на плагіат	21.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	26.12.2023	

Студент _____ Лялик М.Д.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Засоби та методи оцінювання характеристик якості безпровідних локальних мереж // Кваліфікаційна робота освітнього рівня «Магістр» // Лялик Микола Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм-61 // Тернопіль, 2023 // С.65, рис. –19, табл. –1, додат. –1, бібліогр. –51.

Ключові слова: Wi-Fi, WLAN, модель, інформаційна безпека. електромагнітна сумісність, цифрова обробка сигналів, перешкоди, моделі.

Кваліфікаційна робота присвячена розробці методів оцінювання характеристик якості безпровідних локальних мереж. В першому розділі проведено аналіз відомих програмно-технічних засобів для оцінки продуктивності локальних безпровідних мереж, встановлено їх основні переваги та недоліки. Проаналізовано аналітичні методи оцінки ефективності безпровідних локальних мереж.

В другому розділі кваліфікаційної роботи розроблена і застосована модель маркова з дискретним часом, що описує поведінку станції мережі. На відміну від відомих рішень, модель враховує такі особливості протоколу, які у режимі нормального навантаження, як 1) перехід в стан відстрочки після будь-якої передачі пакета і 2) можливість негайної, асинхронної передачі пакету, який прийшов в порожню чергу.

В третьому розділі кваліфікаційної роботи розроблено Java аплет, який дозволяє моделювати роботу безпровідної локальної мережі з метою оцінки її ефективності. Даний додаток забезпечує можливість отримання даних для їх подальшої модельної обробки, а також дозволяє застосовувати перевірку адекватності.

ANNOTATION

Means and methods for quality characteristics assessment of wireless local area networks// The educational level "Master" qualification work // Mykola Dmytrovych Lyalyk // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNm-61group // Ternopil, 2023 // P.65, fig. –19, tables -1, annexes –1, ref. -51.

Keywords: Wi-Fi, WLAN, model, information security. electromagnetic compatibility, digital signal processing, interference, models.

The qualification work is devoted to the development of methods for assessing the quality characteristics of wireless local networks. In the first section, an analysis of known software and technical tools for assessing the performance of local wireless networks was carried out, and its main advantages and disadvantages were established. Analytical methods for assessing the effectiveness of wireless local networks are analyzed.

In the second section of the qualification work, a discrete-time Markov model describing the behavior of a network station was developed and applied. In contrast to known solutions, the model takes into account such features of the protocol, which are in normal load mode, such as 1) transition to the delay state after any packet transmission and 2) the possibility of immediate, asynchronous transmission of a packet that arrived in an empty queue.

In the third section of the qualification work, a Java applet was developed that allows you to simulate the operation of a wireless local network in order to evaluate its effectiveness. This application provides the possibility of obtaining data for their further model processing, and also allows you to apply the adequacy check.

ЗМІСТ

ВСТУП

Актуальність теми. Безпровідні мережі забезпечують якісний обмін і передачу даних між локальними комп'ютерними мережами, коли неможливо або утруднено використання традиційних кабельних технологій.

Безпровідний зв'язок ефективно використовується для забезпечення стійкого каналу зв'язку між тими сегментами локальних мереж, які неможливо з'єднати класичним кабельним з'єднанням.

Також до безпровідних технологій доцільно вдаватись в разі невигідності прокладки кабелю, наприклад, при створенні тимчасових комп'ютерних мереж, оскільки така реалізація дозволяє в мінімальні терміни скрутити мережу без додаткового демонтажу кабельних трас.

Розробці моделі оцінки продуктивності безпровідних локальних мереж при довільному навантажені, а також веб-застосунку для моделювання функціонування такої мережі і присвячена дана кваліфікаційна робота.

Мета і задачі дослідження – побудова моделі оцінки продуктивності безпровідних локальних мереж при довільному навантажені. Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

- Аналіз архітектури безпровідних локальних мереж, виділення основних переваг та недоліків їх функціонування.

- Проведення порівняння основних програмно-технічних засобів оцінки ефективності функціонування безпровідних локальних мереж.

- Аналіз аналітичних методі оцінки ефективності.

- Розробка моделі оцінки ефективності функціонування безпровідної локальної мережі при довільному навантажені.

- Практична реалізація веб-додатку для моделювання ефективності безпровідних локальних мереж.

- Апробація розроблених методів та засобів.

Об’єкт дослідження – безпровідні локальні мережі.

Предмет дослідження – сукупність теоретичних, методологічних, методичних і практичних положень, що визначають процеси дослідження ефективності функціонування безпровідних мереж.

Наукова новизна одержаних результатів кваліфікаційної роботи: отримано математичну модель оцінки ефективності локальної безпровідної мережі при довільному навантажені, яка на відміну від відомих рішень враховує такі особливості протоколу у режимі нормального навантаження, як 1) перехід в стан відстрочки після будь-якої передачі пакета; 2) можливість негайної, асинхронної передачі пакету, який прийшов в порожню чергу.

Практичне значення одержаних результатів: в процесі виконання роботи реалізована веб-застосунок у вигляді Java аплету, який дозволяє моделювати роботу безпровідної мережі та проводить легування основних характеристик її функціонування.

Апробація результатів кваліфікаційної роботи. Основні результати проведених досліджень обговорювались на XI науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2023 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 51 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 65 сторінки, містить 19 рисунків та 1 таблицю.

1. ТЕХНОЛОГІЇ ТА АРХІТЕКТУРА БЕЗПРОВІДНИХ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Аналіз архітектури безпровідних локальних мереж

Під час дослідження ефективності функціонування безпровідних локальних мереж необхідно детальніше зупинитися на компонентах їх архітектури.

В архітектурі IEEE 802.11 містяться окремі компоненти, котрі покликані взаємодіяти один з одним, створюючи безпровідну LAN, яка підтримує в робочому стані мобільність станцій (station – STA) прозоро щодо вищих рівнів. Архітектура та її властивості а також послуги 802.11b зазначені стандартом 802.11. Специфікації 802.11b здійснюють вплив тільки на фізичний рівень, збільшуючи при цьому швидкість передачі даних і більш стійке їх сполучення.

Базова система послуг (Basic Service Set - BSS) являється головним блоком, з яких побудована WLAN IEEE 802.11. Згідно рисунку 1.1 продемонстровано дві BSS, кожна з яких включає по дві станції, які є складовими BSS.

Слід вважати, що їх внутрішні еліпси подані на рисунку 1.1 відображають області охоплень, а всередині цих станції, які включені до даної BSS, можуть комунікувати між собою. Якщо вони будуть перемщені за своєю BSS, то вони не будуть комунікувати з іншими членами BSS.

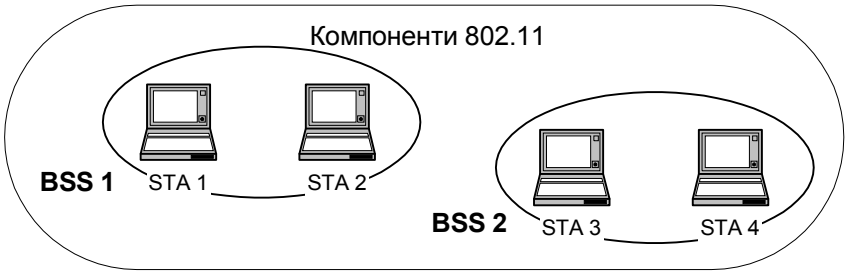

Рисунок 1.1 - Базова система послуг

Незалежна базова система послуг (Independent BSS – IBBS) є головним в типології LAN стандарту IEEE 802.11. Навіть найменша LAN може складатися

з тільки двох станцій. На рис. кожна з BSS 1 та BSS 2 – це IBSS. Робота в такому режимі можлива, за умови що станції здатні комунікувати одна з одною безпосередньо. Такий тип побудови мережі часто формується без будьякого планування, його зазвичай вважають одноразовою (ad hoc) мережею.

З'єднання між станцією та BSS динамічне – станція може вмикатися, вимикатися, залишати межі області охоплення і повертатися в неї. Щоб стати членом інфраструктури BSS, станція мусить стати "асоційованою". Ця асоціація динамічна і включає використання послуг розподільчої системи (Distribution System Service – DSS), описаної нижче.

Концепція розподільчої системи полягає в наступному. Обмеження Фізичного рівня (PHY) визначають максимальну відстань між станціями, яка ще може обслуговуватися. Для певних мереж ця відстань достатня, для інших вона повинна бути збільшена. Тоді, замість незалежного існування, BSS може виступати як компонента розширеної форми мережі, побудованої з багатьох BSS. Архітектурна компонента, яка вживається для взаємосполучення багатьох BSS, називається розподільчою системою (Distribution System - DS).

Стандарт IEEE 802.11 логічно відділяє безпровідне середовище (Wireless Medium - WM) від середовища розподільчої системи (Distribution SystemMedium - DSM). Кожне логічне середовище вживається для різних завдань, з різними компонентами архітектури мережі. Логічні середовища можуть бути фізично однаковими або різними. Розуміння того, що різні середовища логічно відмінні є ключовим лоя розуміння гнучкості архітектури. Архітектура LAN IEEE 802.11 визначена незалежно від фізичних характеристик будь-якого конкретного впровадження. Розподільча система уможливлює підтримку мобільних пристроїв, забезпечуючи логічні послуги, необхідні для обслуговування відображення адрес на призначення і, тим самим, об'єднання багатьох BSS.

Крім станції, IEEE 802.11 визначає пункт доступу (Access Point – AP), який діє як міст між безпровідною мережею та розподільчою системою. Пункт доступу – це станція, яка забезпечує доступ до DS, надаючи послуги

розподільчої системи додатково до своїх дій як станції. Пункт доступу звичайно складається із радіо, кабельного мережевого інтерфейсу (наприклад, для 802.3) і програмного забезпечення для бріджінгу (операцій мостів), сумісного із стандартом 802.1 для бріджінгу. Пункт доступу діє як базова станція для безпровідної мережі, агрегуючи доступ до кабельної мережі для багатьох безпровідних станцій. Кінцевими станціями 802.11, наприклад, можуть бути карти мережевого інтерфейсу IEEE 802.11, або телефонні апарати, базовані на 802.11. На рисунку 1.2 показані компоненти архітектури IEEE 802.11, які включають пункти доступу (AP) та розподільчу систему (DS).

Дані переміщаються між BSS і DS через пункти доступу. Пункти доступу мають власні адреси (як станції); адреси, які використовуються AP для комунікації через безпровідне середовище (WM) і через середовище розподільчої системи (DSM), не обов'язково ті самі.

Розподільчі системи і базові системи послуг дозволяють створювати безпровідні мережі довільного розміру і складності. Стандарт IEEE 802.11 називає такий тип мережі розширеною системою послуг (Extended Service Set – ESS). Ключова концепція полягає у тому, що мережа ESS виглядає на підрівні LLC так само, як IBSS.

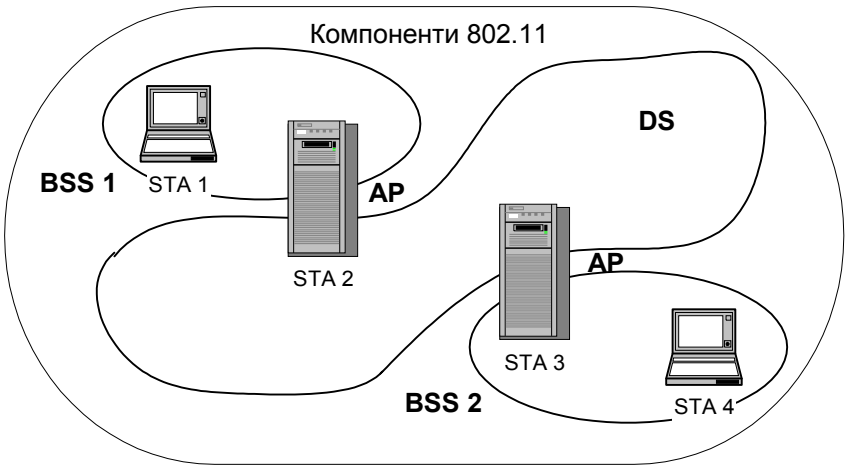

Рисунок 1.2 - Розподільча система і пункти доступу

Станції всередині ESS можуть комунікуватися і мобільні станції можуть переміщатися з однієї BSS до іншої (у межах однієї ESS) прозоро щодо LLC.

IEEE 802.11 не робить жодних припущень щодо фізичного розташування базових систем послуг (рисунок 1.3). Можливі усі вказані варіанти:

- різні BSS частково перекриваються; це широко вживається для організації неперервного покриття певного фізичного простору;

- різні BSS можуть бути фізично ізольованими; логічно нема обмежень на відстані між BSS;

- різні BSS можуть бути фізично суміжними; це може робитися для підвищення надійності;

- одна (або більше) мереж IBSS або ESS можуть фізично існувати у тому самому просторі, що й одна (або більше) мереж ESS.

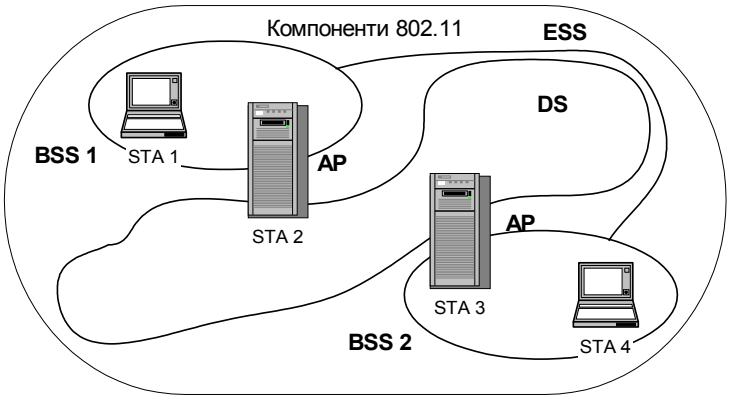

Рисунок 1.3 - Розширена система послуг

Щоб забезпечити інтеграцію в архітектуру IEEE 802.11 з традиційними кабельними мережами, було добавлено ще одну архітектурну компоненту – портал. Портал є ще одним пунктом, за допомогою якого блок даних послуг MAC (Mac Service Data Unit – MSDU) потрапляє з інтегрованої LAN іншого стандарту (не IEEE 802.11) до розподільчої системи LAN IEEE 802.11. Приклад наведений на рисунку 1.4.

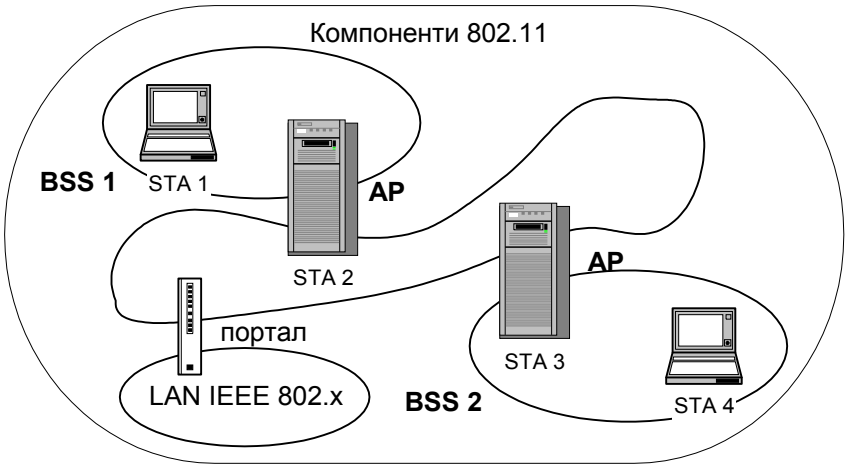

Рисунок 1.4 - Сполучення з іншими локальними мережами, відмінними від IEEE 802.11.

Портал здійснює логічну інтеграцію між архітектурою LAN IEEE 802.11 та чинною кабельною LAN. Можливі пристрої, які поєднують функції AP і порталу, це можливе, коли у розподільчу систему впроваджені компоненти з кабельної LAN. [14].

Архітектура IEEE 802.11 допускає можливість, що розподільча система не ідентична з чинною кабельною LAN. Розподільча система може бути утворена на основі багатьох різних технологій включно з локальними мережами IEEE 802. Стандарт також не обмежує DS до базування на Канальному або Мережевому рівні, а також не обмежує її до централізованості або розподіленості за своєю природою. Також стандарт не визначає подробиць впровадження DS, натомість, IEEE 802.11 описує послуги, пов’язані з різними компонентами архітектури. Існують дві категорії послуг у цьому стандарті – послуги станцій (Station Service – SS) і послуги розподільчої системи (Distribution System Service – DSS). Обидві категорії послуг використовуються на підрівні MAC.

Послуги станцій наявні в кожній станції IEEE 802.11, включно з AP. До цих послуг належать:

- автентифікація;

- деавтентифікація;

- конфіденційність (приватність – privacy);

- доручення блоків даних послуг MAC (MSDU).

Послуги розподільчої системи (показані стрілками між AP на рисунку 1.5) використовуються, щоб перетинати логічні межі середовищ і адресних просторів. Фізичне втілення різних послуг може бути і може не бути розташоване всередині фізичного пункту доступу. Послуги розподільчої системи забезпечуються самою DS і доступні через станції, які також забезпечують DSS. Станцією, яка здійснює доступ до DSS, є пункт доступу. До послуг розподільчої системи належать:

- асоціаціювання;

- деасоціаціювання;

- поширення;

- інтеграція;

- реасоціаціювання.

Послуги розподільчої системи визначені для використання об’єктами підрівня MAC.

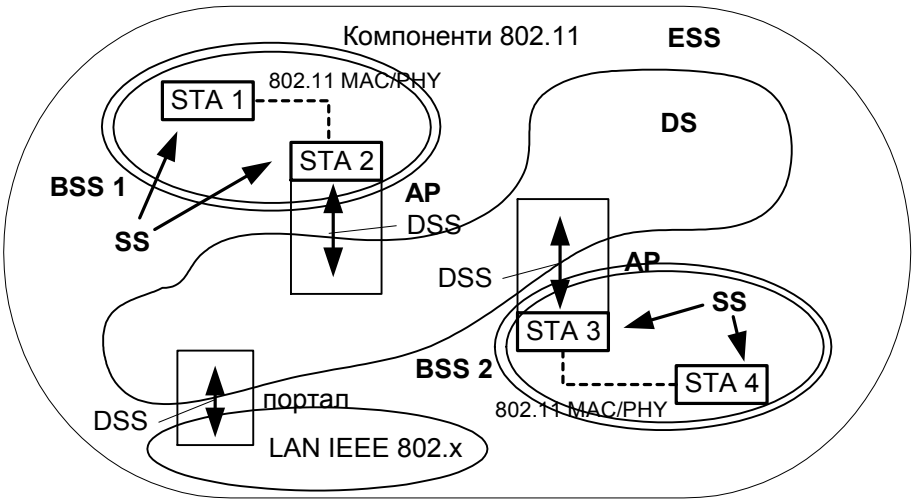

Рисунок 1.5 - Повна архітектура IEEE 802.11

Численні логічні адресні простори. Архітектура IEEE 802.11 дозволяє безпровідному середовищу, середовищу розподільчої системи і інтегрованій кабельній мережі використовувати різні адресні простори. Даний стандарт використовує і специфікує тільки адресний простір безпровідного середовища. Як кожен PHY IEEE 802.11 оперує в одному окремому середовищі – у WM, так

і MAC IEEE 802.11 оперує в окремому адресному просторі, який відноситься до безпровідного середовища (“адреси WM”). Стандарт IEEE 802.11 використовує 48-бітові адресний простір IEEE 802, тому ці адреси сумісні з адресним простором, вживаним у сімействі LAN IEEE 802. [11].

Однак архітектура IEEE 802.11 дозволяє розрізняти три логічні адресні простори - безпровідного середовища, середовища розподільчої системи і інтегрованої кабельної мережі. Приклад численних логічних алресних просторів – один, у якому впровадження DS використовує адресацію Мережевого рівня. У цьому випадку адресний простір WM і адресний простір DS будуть різними.

1.2 Основні проблеми функціонування безпровідних мереж

За рахунок особливостей функціонування безпровідних мереж зумовлюють додаткові проблеми, і як наслідок впливають на їх доступність, продуктивність, безпеку і вартість експлуатації. Для грамотного вирішення цих проблем потрібні спеціальні інструментарії підтримки та експлуатації, спеціальні механізми адміністрування і моніторингу, не реалізовані в традиційному інструментарії управління безпровідними мережами [7].

Активність у неробочий час. До бездротових мереж можна підключитися в будь-якому місці в зоні їх покриття і в будь-який час. Виходячи із зазначеного ряд фірм та організацій обмежують доступ до бездротових мереж тільки в робочий час.

Швидкості. Пристрої, які характеризуються низькою швидкістю, відповідно мають більшу зону покриття. Вони надають додаткову можливість віддаленого злому. Якщо в офісній мережі, де всі працюють на швидкостях 24/36/54 Мб /с, раптом з'являється з'єднання на 1 або 2 Мб/с, це може бути сигналом, що хтось намагається пробитися в мережу з вулиці.

Перешкоди. Якість роботи безпровідникової мережі залежить від багатьох факторів. Найбільш яскравим прикладом є перешкоди, значно знижують

пропускну здатність і кількість підтримуваних клієнтів, аж до повної неможливості використання мережі. Джерелом перешкод може бути будь-який пристрій, що випромінює сигнал достатньої потужності в тому ж частотному діапазоні. З іншого боку, зловмисники можуть використовувати перешкоди для організації DoS-атаки на мережу [7].

Крім перешкод, існують інші аспекти, що впливають на якість зв'язку у безпровідникових мережах - невірно конфігурований клієнт або збій антени можуть створювати проблеми як на фізичному, так і на канальному рівні, приводячи до погіршення якості обслуговування інших клієнтів мережі.

Поширеність безпровідникових технологій у наш час ставить під загрозу і ті мережі, де вони вже застосовуються, і ті, де ніколи не повинні використовуватися. Традиційні засоби захисту безсилі проти принципово нових класів безпровідникових загроз. При цьому ситуація ускладнюється тим, що необхідно захищати також і своїх користувачів (які можуть знаходитися і далеко від офісу), не порушуючи при цьому функціонування мереж сусідів, яким би підозрілим воно не виглядало. Тим не менше, існують методи захисту від подібних загроз як безпровідникових, так і провідникових мереж і користувачів, що дозволяють впевнено і безпечно розгортати і використовувати безпровідникові мережі [8].

1.3. Ефективність локальних безпровідних мереж та аналіз програмно-технічних засобів їх оцінки

Дуже часто користувачі скаржаться на поганий відгук безпровідникової мережі. Як встановити, де і чому відбувається падіння продуктивності? Для дослідження або, в ідеальному випадку, повного запобігання подібним проблемам необхідні адекватні методи аналізу і спеціалізовані інструменти.

При аналізі продуктивності йдеться не стільки про те, як збільшити швидкість передачі ще на декілька біт в секунду, скільки про те, як забезпечити “здоров’я” безпровідникової локальної мережі. Якщо вона сконфігурована

коректно і зовнішні негативні дії відсутні, зокрема джерела перешкод або радіоканали, що перекриваються, це позитивно відбивається на продуктивності.

Причина поганого відгуку може полягати в суміжних, провідникових сегментах мережі, каналах глобальних мереж, або навіть її слід шукати на рівні додатків (переобтяжений сервер).

Перш ніж проводити аналіз конкретного випадку падіння продуктивності робочої мережі, спочатку рекомендується виконати пасивний моніторинг ситуації в мережі за допомогою протокольного аналізатора. Технології для моніторингу за допомогою протокольних аналізаторів для бездротових мереж надають відомості про те, скільки активних бездротових вузлів ділять між собою наявну смугу пропускання, яка типова ефективна швидкість передачі даних (рисунок 1.6) і чи високий рівень помилок або повторень.

В середовищі 802.11g на продуктивність клієнтів 11g в переобтяжених мережах негативно можуть впливати як активні, так і пасивні клієнти 11b.

У такому разі усунути проблеми можливо лише із значними витратами, помістивши клієнтів відповідного типа WLAN в окремий бездротовий осередок.

Схожа дія на передачу спостерігається також в бездротових осередках з однотипними клієнтами (наприклад, на базі 802.11a), коли окремі станції розташовані на краю осередку і передають дані з низькою швидкістю. Залежно від конкретної ситуації позитивний ефект досягається шляхом переміщення точки доступу для кращого покриття реальної робочої області. Крім того, зони покриття можна розширити шляхом установки нових точок доступу.

Часто “пожирачами” пропускної спроможності в бездротових інфраструктурах опиняються сеанси передачі даних між вузлами WLAN в межах одного і того ж осередку, коли кожен пакет даних двічі перетинає радіоефір: від відправника до точки доступу і від точки доступу до одержувача [9].

Так звана “карта вузлів″, або “матриця пар”, в аналізаторі WLAN вкаже на активних взаємодіючих партнерів в осередку і дозволить швидко розкрити причину падіння продуктивності. Більшість сучасних точок доступу при необхідності здатного пригнічувати комунікацію між рівноправними вузлами в межах осередку.

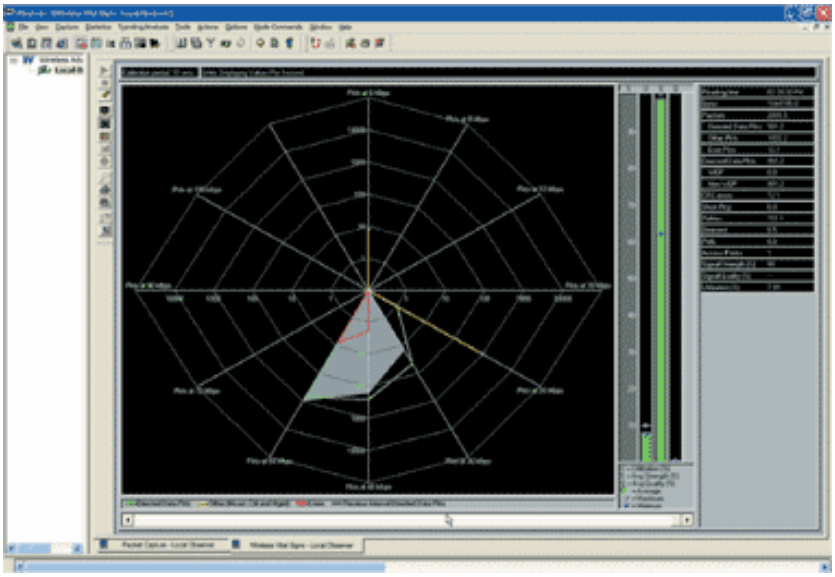

Рисунок 1.6 - Observer 8.3 від Network Instruments з її Wireless Vital Signs

Використання нестандартних режимів роботи, наприклад “турборежим” 802.11a на базі набору мікросхем від Atheros (вони застосовуються в продуктах компаній Lancom Systems, Proxim і Netgear), в ідеальному випадку хоч і підвищує пропускну спроможність осередку, але ускладнює пошук помилок.

Перші тести в лабораторії LANline підтвердили збільшення швидкості передачі в “турборежимі” до 60% (номінальна пропускна спроможність 108 Мбіт/с) в порівнянні із стандартом 802.11a (номінальна пропускна спроможність 54 Мбит/с).

З трьох представлених минулого разу протокольних аналізаторів - Observer 8.3 (від Network Instruments), Airopeek NX 2.01 (Wildpackets) і Wireless Sniffer 4.75 (Network Associates) - тільки Observer “бачить” пакети, що пересилаються в турборежимі.

Розширення набору мікросхем від Atheros на самому нижньому рівні мультиплексування з ортогональним розділенням частоти (Orthogonal Division

Frequency Multiplexing, ODFM) передбачає об’єднання двох каналів (”турбоканали” 42, 50 або 58), при цьому передача здійснюється по двох суміжних каналах стандарту IEEE (40/44, 48/52 і 56/60). Точки доступу перед активуванням “турбоканала” перевіряють зайнятість ефіру в цілях дотримання вимог місцевих регулюючих органів. Якщо ж для власної роботи точки доступу без підтримки турборежиму вибирають канал в безпосередній близькості від вже активного турбоканалу, то два осередки заважатимуть один одному, оскільки такі точки доступу не в змозі розпізнати активний турбоканал.

В перших тестах із-за конфліктів між каналами з боку 802.11a спостерігалося падіння швидкості передачі до 50%. За допомогою Observer ідентифікація накладення каналів такого типу за допомогою Channel Surfing більше не представляється проблемою. Решта аналізаторів WLAN хоч і зафіксувала підвищений рівень помилок, але не вказала можливих причин.

В більшості випадків проблеми з продуктивністю в мережі виявляються лише спорадично, і відтворити їх по опису користувачів не завжди вдається. Подібною властивістю відрізняються і бездротові локальні мережі. Перед введенням в нормальний режим експлуатації знову-таки потрібно перевірити характеристики продуктивності, але обійтися одним тільки аналізатором WLAN вже не вдасться.

Необхідно згенерувати націлений мережевий трафік і на нім зміряти швидкість передачі. Важливо, щоб створення трафіку по можливості не залежало від немережевих чинників - навантаження на сервер або на клієнта. Таким чином, потрібні спеціалізовані інструменти для вимірювання пропускної спроможності мережі.

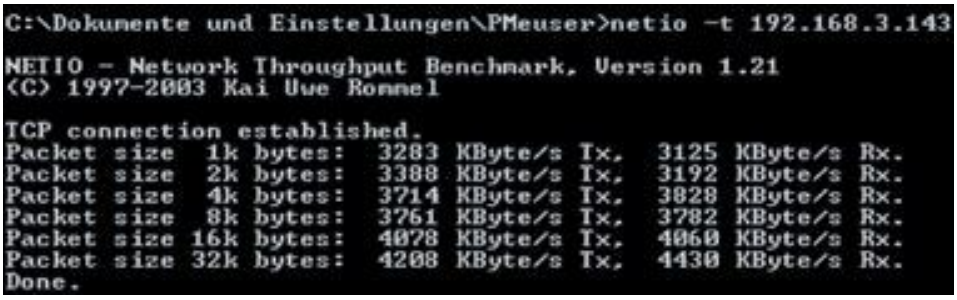

Рисунок 1.7 - Виклик з командного рядка і результати вимірювань Netio (в даному випадку в турборежимі 11a на 108 Мбіт/с на основі компонентів від Lancom).

Популярним і безкоштовним (за умови некомерційного використання) засобом вимірювання пропускної спроможності мережі є Netio від Кая Уве Роммеля (рисунок 1.7). Остання версія 1.21 цієї простої програми на базі командного рядка доступна у вигляді початкового коду за адресою: http://freshmeat.net/projects/netio/ для платформ Win32 (i386), Linux (i386) і OS/2.

Netio по вибору генерує трафік TCP або UDP між двома мережевими вузлами і дозволяє задавати величину блоку від 1 до 32 Кбайт. Передача даних на прикладному рівні відбувається поперемінно в обох напрямах. Якщо один вузол розташований в локальній мережі, а другий - в бездротовій, то в результаті можна отримати ефективну швидкість передачі для прямого (від локальної до бездротової мережі) і зворотного (від бездротової до локальної мережі) потоку.

Як показали різні тести точок доступу, між передачею в прямому і зворотному напрямах можуть спостерігатися істотні відмінності, наявність яких може, наприклад, указувати на помилки у вбудованому програмному забезпеченні точки доступу.

Вибір тестового трафіку - на базі TCP або UDP - визначається використовуваними додатками і типом їх передачі. Найбільш популярний TCP (у разі HTTP, FTP, SMB, Lotus Notes і т. д.), але і вимірювання на базі UDP мають сенс, коли потрібно добитися оптимальних значень для мультимедійних потокових додатків або мережевої файлової системи NFS на базі UDP [10].

У разі UDP внутрішні протокольні механізми для управління потоком даних (Data Flow Control, DFC) не задіюються, унаслідок чого можна розраховувати на вищу фактичну швидкість передачі. Якщо співвідношення між TCP і UDP не відповідає очікуваному, то це указує на можливу помилку в мережевих компонентах.

Коли за допомогою вимірювання пропускної спроможності мережі передбачається виявити джерела помилок в складних розподілених системах WLAN, Netio мало чим зможе допомогти.

Паралельні комунікаційні процеси між декількома мережевими вузлами не можна запускати синхронно (наприклад, паралельну передачу даних за стандартом 802.11g із швидкістю 11 і 54 Мбит/с), а крім того, немає можливості впливати на об'єм і тривалість передачі даних. Зміна різних комунікаційних партнерів в різних місцях мережевої топології для локалізації джерел помилок вимагає реконфігурациі на рівні командного рядка, на що йде багато часу.

Для вирішення подібних завдань компанія Netiq випустила комерційний продукт Chariot. Він складається з так званих "кінцевих точок продуктивності" для всіх широко поширених операційних систем (Windows ME/NT/2000/XP, Linux або Sun Solaris Sparc/x86) і центральної консолі для управління вимірюваннями [10].

При вимірюванні пропускної спроможності інстальовані "кінцеві точки продуктивності" по всій мережі можуть об'єднуватися в комунікаційні пари в будь-якій комбінації. Кожній парі без обмежень призначається використовуваний комунікаційний протокол (TCP, UDP, RTP, зокрема у варіантах для IPv6, а також SPX, IPX і APPC) і призначений для користувача протокол, що спирається на нього.

Chariot за бажанням моделює комунікаційні процеси таких додатків, як Microsoft SQL, Lotus Notes або Netshow Streaming, за допомогою власної мови сценаріїв і тим самим допомагає відтворити реальну ситуацію в мережі.

Для аналізу продуктивності бездротової мережі призначені вже майже стандартизовані вимірювання за допомогою простого сценарію Throughput - при стандартних параметрах він генерує порівнянний з Netio мережевий трафік. Вимірювання проводяться або для чітко певного об'єму даних, або в обмеженому тимчасовому інтервалі - при лабораторному тестуванні LANline його тривалість складала 1 хв. Обумовлені середовищем передачі відхилення переважно згладжуються; крім того, заразом можна провести запис пакетів з аналізатора WLAN для подальшого детального аналізу.

Як результати вимірювань видаються не тільки одні цифри (середнє значення ефективної пропускної спроможності, кількість транкзакций залежно від додатку, час реакції і переданий об'єм даних) - зміна абсолютних значень з часом представлена також в графічному вигляді (див. рис. 1.8).

Різкі відхилення значень легко виявляються, і при необхідності вимірювання можна повторити. Таким чином можна швидко побачити вплив різних чинників на реальну пропускну спроможність. Наприклад, з початком передачі даних клієнта 802.11b в тому ж осередку, яким користуються клієнти 802.11g, крива пропускної спроможності клієнтів g різко йде вниз. Chariot полегшує моделювання подібної ситуації завдяки тому, що комунікаційні пари можуть починати передачу даних із затримкою, що довільно задається, в рамках одного сеансу вимірювань.

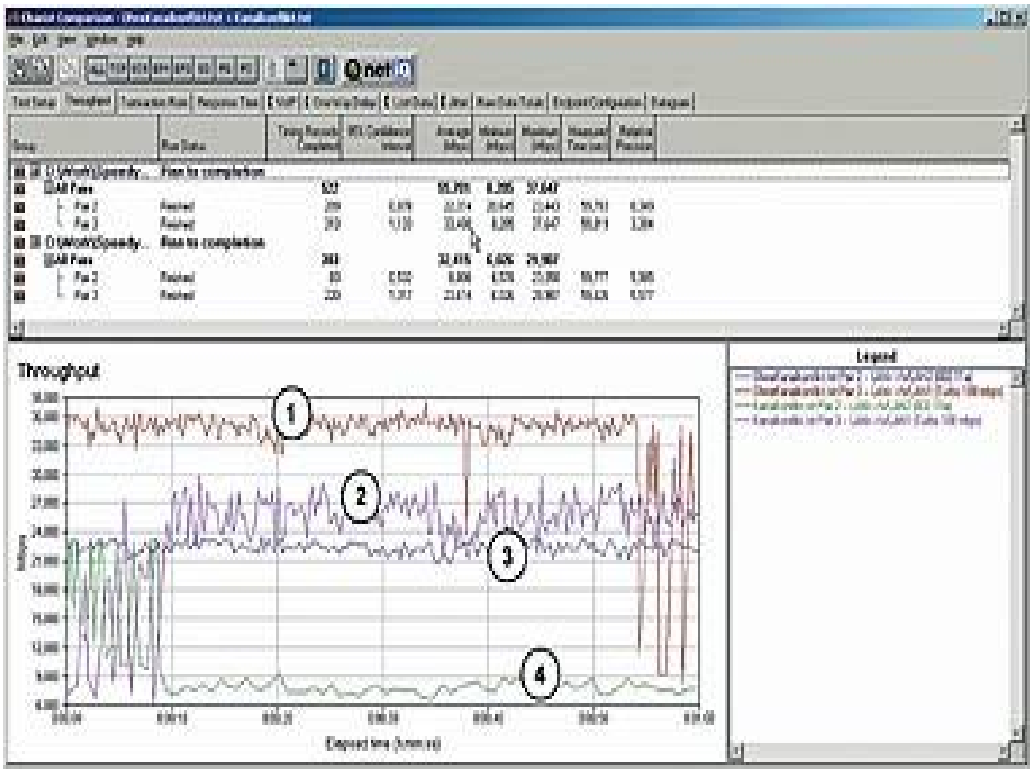

Рисунок 1.8 - Що протиставили один одному результати вимірювань в Chariot 4.3 від Netiq: при перекритті каналів двох радіоосередків продуктивність падає (турборежім 108 Мбіт/с, крива 1 - без конфлікту і крива 2 - з конфліктом; як і 54 Мбіт/с 802.11a, крива 3 - без конфлікту і крива 4 - з конфліктом).

Ефективним виявилося застосування ноутбука з двома адаптерами WLAN (оптимальними на даний момент є карти формату PC Card стандартів a/b/g з набором мікросхем від Atheros, наприклад Netgear WAG511 або Proxim Orinoko 11a/b/g ComboCard, а також другий багаторежимний адаптер у виконанні Mini PCI).

На першому адаптері аналізатор в “режимі прийому всіх пакетів″ прослуховує радіоефір, а через другу карту встановлюється активне бездротове з’єднання, для якого за допомогою консолі Chariot проводяться вимірювання пропускної спроможності і ініціюється мережевий трафік. Ноутбук не повинен бути складовою частиною вимірювань, тому його вплив на результат мінімально, і аналізатору надається вся обчислювальна потужність для обробки в оптимальній для вимірювань крапці.

І останнє зауваження: разом з Chariot компанія Netiq пропонує безкоштовну утиліту під назвою Qcheck (http://www.qcheck.net). Вона дозволяє проводити прості вимірювання пропускної спроможності і часу відгуку по вибору для TCP, UDP, SPX або IPX між двома “кінцевими точками продуктивності”.

Проте користь від застосування Qcheck в швидких бездротових мережах невелика, оскільки для отримання репрезентативних результатів вимірювань величина 1000 Кбайт - дуже невеликий об’єм. А повторні вимірювання дають сильні спотворення.

1.4 Висновок до першого розділу

В першому розділі проведено аналіз відомих програмно-технічних засобів для оцінки продуктивності локальних безпровідних мереж, встановлено їх основні переваги та недоліки. Проаналізовано аналітичні методи оцінки ефективності безпровідних локальних мереж.

2 ОСОБЛИВОСТІ ОЦІНОК ЕФЕКТИВНОСТІ ТА МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ ПРОДУКТИВНОСТІ БЕЗПРОВІДНИХ МЕРЕЖ ПРИ ДОВІЛЬНОМУ НАВАНТАЖЕННІ

2.1 Аналіз відомих аналітичних методів оцінки ефективності

Аналізуючи відомі публікації, що стосуються дослідження ефективності безпровідних локальних мереж встановлено, що пропускна здатність 802.11 WLAN під управлінням механізму DCF досліджувалася або експериментально, або шляхом спрощеного аналітичного або імітаційного моделювання, базованого на припущеннях, які суттєво спрощують реальний алгоритм затримки. Найбільш детальний аналіз схеми DCF наведений в роботах [12, 13], в яких розроблені аналітичні методи оцінки пропускної здатності безпровідної локальної мережі 802.11 WLAN при високому навантажені, коли до всіх станцій мережі завжди присутні непорожні черги (умова насичення мережі). Цей показник визначений в [13] як saturation throughput (пропускна здатність в умовах насичення), одержаний в допущені ідеального каналу передачі, тобто при відсутності шумів та скритих станцій.

Розглянемо 802.11 WLAN, яка складається з N станцій та працює у умовах насиченості та ідеальності каналу. При відсутності перешкод число повторних звернень передачі пакету обмежено $R = N_s$. Усі станції такої мережі вважаються статистично однорідними. Статистична однорідність станцій заключається в одинаковій ймовірності розподілу довжини пакетів, яка вибарається кожною станцією із черги.

Слідуючи підходу, запропонованому Бянкі в [14] застосуємо дискретну та цілочисельну часову шкалу роботи мережі: моменти t та $t+1$ відповідають початкам віртуальних слотів, які йдуть один за одним. Віртуальні слоти не одинакові, і кожний з них може бути представлений: 1) порожній слот відстрочки σ, в якому жодна із станцій не веде передачу; 2) «успішний» слот, в

якому тільки одна із станцій проводить передачу сигналів; 3) колізійний слот, в якому дві або більше станцій намагаються провести передачу пакетів.

Згідно моделі Бянкі в [14] припускається що на початку кожного слоту кожна із станцій намагається провести відправку пакетів з однаковою ймовірністю, яка рівна τ. В моделі Калі [14] припускається, що час відстрочки b не залежить від числа пере повторів n_r поточної передачі і вибирається із геометричного розподілу з параметром τ, тобто $b = 0,1,2...$ із ймовірностями τ, $(\tau - 1)$, $\tau(\tau - 1)^2$, … .

Очевидно, що дані припущення еквівалентні, якщо не враховувати ефект захвату канала. У обох розглянутих моделях припускається, що будь-яка станція може розпочати передачу на початку слота. Прийнявши будь-яке із введених припущень не складно отримати вираз для ймовірності порожнього слота (p_e), успішного слота (p_s), та колізійного слоту (p_c):

$$p_e = (1-\tau)^N,\ p_s = N_\tau(1-\tau)^{N-1},\ p_c = 1-(1-\tau)^N - N_\tau(1-\tau)^{N-1}. \quad (2.1)$$

У даному випадку ймовірність колізії не залежить від розміру пакету, який передається, тому припускаємо, що тривалість t_s та t_c «успішного» та «колізійного » слотів не залежать від числа спроб (або декількох значень числа спроб у випадку колізії) і визначається тільки функцією розподілу ймовірності $F(\bullet)$ для розміру пакету даних $P \in [0, P_{max}]$, що нормалізований швидкістю каналу V_c. Знаходимо середнє значення t_s та t_c:

$$T_s = [1 - F(P_l)](t_{RTS} + t_{CTS} + 2\delta + 2SIFS) + H + E(P) + t_{ACK} + 2\delta + SIFS + DIFS, \quad (2.2)$$

де P_l - поріг $RTS / CTS\ \overline{P}$, нормалізованим V_c; t_{RTS}, $t_{CTS} = t_{ACK}$ та H - це часи відповідно для передавання кадрів RTS, CTS та ACK, а також заголовку $DATA$; δ - це затримка передачі, прийнята однаковою для всіх пар станцій; $E[P]$ - середнє значення P; $E[P*]$ - середня тривалість колізії , тобто середній час, який необхідний для передавання самого тривалого кадру, який входить в колізію.

Остання величина визначається за формулою:

$$E[P^*] = p_c^{-1} \sum_{k=2}^{N} \binom{N}{k} \tau^k (1-\tau)^{N-k} E[P^* \mid k], \qquad (2.3)$$

де $E[P^* \mid k]$ - це середня тривалість колізії, в якій приймають участь k станцій. Для того щоб знайти $E[P^* \mid k]$, ми приймемо відношення Бянкі: а) функція розподілу $F(\bullet)$ однакова для всіх станцій; існує похідна $f(P) = dF / dP$ для всіх $P \in [0, P_{max}]$. Тоді

$$\begin{aligned} E[P^* \mid k] &= t_{RTS}[1 - F(P_l)]^k + k\int_0^{P_l} (x + H) f(x)[F(x) + 1 - F(P_l)]^{k-1} dx = \\ &= H + P_l - (H - t_{RTS})[1 - F(P_l)]^k - \int_0^{P_l} [F(x) + 1 - F(P_l)]^k dx \end{aligned} \qquad (2.4)$$

Підставивши (2.4) в (2.3) та провівши деякі перетворення отримаємо

$$E[P^*] = H + P_l - \frac{H - t_{RTS}}{p_c} Z_N(0) - p_c^{-1} \int_0^{P_l} Z_N(x) dx,, \qquad (2.5)$$

де

$$E[P^*] = H + P_l - \frac{H - t_{RTS}}{p_c} Z_N(0) - p_c^{-1} \int_0^{P_l} Z_N(x) dx,, \qquad (2.6)$$

$$Z_N(x) = \{1 - \tau[F(P_l) - F(x)]\}^N - (1-\tau)^N - N\tau[F(x) + 1 - F(P_l)](1-\tau)^{N-1} \qquad (2.7)$$

Таким чином ми визначили середню тривалість усіх типів віртуальних слотів.

Розглянемо часовий інтервал t_v між двома послідовними успішними передачами. Цей інтервал називається віртуальним часом передавання, являє собою час між двома послідовними закінченнями інтервалів *DIFS*. Тоді пропускна здатність в умовах насичення визначається наступним чином:

$$S = \frac{V_C E[P]}{E[T_V]}, \qquad (2.8)$$

де $E[T_V]$ - середній час t_v. У загальному випадку час передавання t_v може складатися із $l = 1,2...$ віртуальних слотів, де останній слот «успішний», $k = 0,...l-1$ - колізійні слоти та $l-1-k$ - порожні слоти, тобто $t_v = T_s + kT_C + (l-1-k)\sigma$. Тоді

$$E[T_V] = p_S \sum_{l=1}^{\infty} \sum_{k=0}^{l-1} [T_s + kT_C + (l-1-k)\sigma] \binom{l-1}{k} p_c^k p_e^{l-1-k} \quad (2.9)$$

Обчисливши цю суму отримаємо

$$E[T_V] = T_s + \frac{p_c}{p_S} T_C + \frac{p_e}{p_S} \sigma \quad (2.10)$$

Виходячи із формул (2.9) та (2.10) для знаходження пропускної здатності S в умовах насиченості залишається визначити ймовірність передавання τ. Щоб розв'язати поставлену задачу модифікуємо алгоритм з тим щоб узагальнити значення параметрів правила відстрочки та узагальнити порогове значення числа повторних запитів R. Прийнявши до уваги геометричний розподіл часу відстрочки b маємо $\tau = 1/(E[b]+1)$, де $E[b]$ - середнє значення часу відстрочки. Так як значення b вибирається із набору $\{0,...,w-1\}$, $E[b]$ визначається через середнє значення $E[w]$:

$$E[b] = (E[w]-1)/2. \quad (2.11)$$

Звідси

$$\tau = 2/(E[w]+1), \quad (2.12)$$

де необхідно знайти середнє значення конкурентного вікна $E[w]$. Станція може знаходитися в одному із R станів, де номер стану $i(i = 0,...,R-1)$ рівний поточному числу спроб передавання. Із стану i в якому значення конкурентного вікна визначається (2.2), станція переходить в стан 0, якщо передача пройшла успішно, а якщо пройшла колізія, то в стан $i+1 \, mod \, R$, так як ймовірність невдалої передачі рівна

$$p = 1-(1-\tau)^{n-1}, \quad (2.13)$$

то ймовірність відмови визначається за формулою

$$p_{rej} = p^R = \left[1-(1-\tau)^{N-1}\right]^R, \quad (2.14)$$

Проаналізовані аналітичні методи часто використовуються для оцінки основних показників функціональності безпровідних локальних мереж, проте необхідно відзначити що оцінка продуктивності безпровідних локальних мереж

при довільному навантажені є досліджена недостатньо, що вимагає поглиблення напрацьованих результатів у цій сфері.

2.2 Продуктивність безпровідних локальних мереж при довільному навантажені

Для вирішення проблеми забезпечення можливості доступу до світової мережі з будь-якого місця і у будь-який час бурхливо розвиваються різні бездротові мережеві технології, що стають одним з основних напрямів розвитку мережевої індустрії. Для забезпечення ефективного управління доступом до бездротового середовища розроблено низку міжнародних стандартів, протоколів і рекомендацій, які специфікують фізичний і Mac-рівні бездротових мереж. Серед розробників бездротових локальних мереж особливо популярний протокол IEEE 802.11, розроблений Institute of Electrical and Electronics Engineers (IEEE) і затверджений в якості міжнародного стандарту в 1997 р.

Схема розподіленого управління DCF (Distributed Coordination Function), яка реалізує метод множинного доступу CSMA/CA з уникненням колізій (Carrier Sense Multiple Access with Collision Avoidance), є основним режимом роботи протоколу IEEE 802.11. У цьому режимі інформаційні пакети передаються в загальному випадку двома способами. Короткі пакети, чия довжина не перевищує певної межі L, передаються за допомогою механізму Базового Доступу (Basic Access) (рисунок 3.1, верхня діаграма). Станція, успішно прийняла кадр DATA, що містить інформаційний пакет, через короткий міжкадровий інтервал SIFS (Short InterFrame Space) відповідає позитивним підтвердженням ACK. Для пакетів з більшою довжиною використовується механізм RTS/CTS (Request-To-Send/Clear-To-Send) (рисунок 3.1, нижня діаграма). У цьому випадку передача кадру DATA передує посилкою короткого службового кадру RTS, який станція задовольняє після SIFS кадром CTS. Якщо CTS-кадр отримано правильно, пізніше SIFS, передається кадр DATA, який у свою чергу підтверджується кадром ACK.

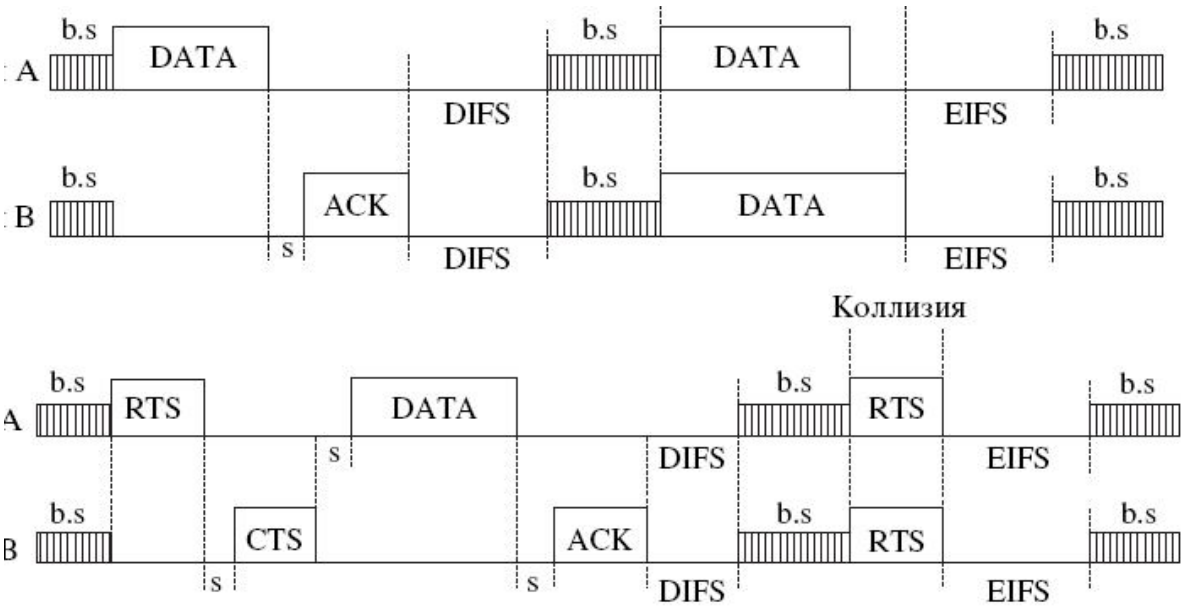

Рисунок 2.1 – Основні механізми DCF: механізм базового доступу – верхня діаграма та механізм RTS/CTS – нижня діаграма

Як видно з рисунка 2.1, тривалість колізії різниться в залежності від застосовуваного механізму. При Базовому доступі тривалість колізії визначається максимальною довжиною колізуючих кадрів DATA, а при механізмі RTS/CTS - тривалістю кадру RTS. Очевидно, що чим довші пакети, що передаються методом Базового Доступу, тим триваліша колізія. У той же час використання механізму RTS/CTS передбачає накладні витрати у вигляді передачі двох додаткових службових кадрів, причому ці витрати тим істотніші, чим менша довжина пакету. Таким чином, правильний вибір межі L названої RTS-межею, може значно поліпшити продуктивність мережі. Після завершення чергової спроби передачі пакету станція переходить у стан відстрочки через DIFS (Distributed Inter Frame Space), якщо спроба була успішною (тобто колізія була відсутня), або EIFS (Extended InterFrame Space, EIFS>DIFS) при невдалій спробі (EIFS використовується також в якості тайм-ауту очікування АСК). При цьому лічильник інтервалу відстрочки встановлюється в початкове значення b, що вимірюється в слотах тривалістю σ і з однаковою ймовірністю вибирається з багатьох $(0,...,W-1)$. Величина W називається вікном конкуренції CW (Contention Window), і залежить від стадії

відстрочки, яка визначається кількістю i невдалих спроб передачі пакету, тобто $W = W_i$. У першу спробу передачі W встановлюється рівним величині $W_0 = CW_{min}$, тобто мінімальним вікном конкуренції. Після кожної невдалої передачі W подвоюється, тобто $W_i = 2_i W_0$ і так до досягнення максимальної величини CW_{max}. На стадії відстрочки $i = m$ станція робить останню спробу передати пакет і, якщо вона невдала, то пакет видаляється з черги (ситуація відмови).

Станція, що знаходиться як в стані відстрочки, так і в стані простою (при порожній черзі), відстежує активність каналу. У міру того як канал відчувається вільним, лічильник інтервалу відстрочки зменшується і "заморожується", коли визначається передача в каналі, і знову починає зменшуватися, коли канал знову відчувається вільним на час, більше DIFS або EIFS (залежно від того, чи була остання передача по каналу успішною чи ні). Станція робить чергову спробу передачі, коли лічильник інтервалу відстрочки зменшується до 0. По закінченню процесу передачі чергового пакету (незалежно від його результату, тобто як після успішної передачі, так і при втраті пакету після $(m+1)$-ї невдалої спроби) станція повертається на стадію $i = 0$ і переходить в стан відстрочки. Якщо черга станції виявилася порожньою після закінчення часу відстрочки, станція переходить в стан простою.

Пакет, що надійшов в чергу станції, що знаходиться в стані простою, негайно передається, як і в момент надходження, так і протягом інтервалу DIFS або EIFS коли канал був вільний. В іншому випадку станція переходить у стан відстрочки на стадію $i = 0$.

В останні роки ведуться інтенсивні наукові дослідження, спрямовані на підвищення ефективності бездротових радіомереж і вибір оптимальних параметрів схеми DCF протоколу IEEE 802.11. У ранніх роботах оцінка продуктивності проводилася або шляхом імітаційного моделювання (наприклад, в [13]), або з допомогою наближених аналітичних моделей [13,14], заснованих на припущеннях, що істотно спрощують правило визначення

інтервалу відстрочки. Особливості схеми DCF найбільш повно враховані в роботах [15,16] в яких розроблені аналітичні методи оцінки пропускної здатності локальної бездротової мережі 802.11 при високому навантаженні (випадок насичення), коли в будь-який момент часу до всіх станцій завжди є непусті черги. На жаль, отримані результати виявляються непридатними в умовах нормального навантаження, коли черги станцій періодично виявляються порожніми, зважаючи на істотне завищення оцінок середнього часу обслуговування пакетів.

У даній роботі розробляється марківська модель поведінки станції безпровідної мережі з урахуванням цих факторів. Ця модель застосовна при довільному (як при нормальному, так і при високому) навантаженні і дозволяє оцінювати середній час, необхідний для обслуговування пакету, а також інші показники продуктивності.

2.3 Математичний опис моделі

Основний показник ефективності, оцінюваний в даному дослідженні - це середнє значення часу обслуговування пакету T, причому цей час відраховується від моменту або надходження пакету в порожню чергу цієї 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).

Дослідимо мережу, що складається з N статистично однакових станцій, в чергу кожного з яких надходить пуассонівський потік пакетів з інтенсивністю λ і розподілом $D(l_i)$ довжин пакетів l_i. Канал вважається ідеальним, а час поширення сигналу між станціями - дуже незначним. Крім того, передбачається, що черга пакетів кожної станції може містити не більше B пакетів, поріг RTS-межа L однаковий для всіх станцій, а час поширення сигналу дуже малий.

Будемо називати пакети, передача яких починається в момент надходження, переданими асинхронно, а всі інші - переданими синхронно. Асинхронна передача має місце, якщо в момент приходу пакету станція була в стані простою і канал був вільний протягом, як мінімум, DIFS або EIFS. Таким чином асинхронна передача відбувається тільки за відсутності синхронних передач інших станцій, а так як $N\lambda\sigma \le 1$, то можна вважати, що за час одного слота відстрочки в мережі може відбутися не більше однієї асинхронної передачі. Отже, асинхронна передача завжди успішна.
Для оцінки часу T побудуємо модель поведінки досліджуваної станції у вигляді ланцюга Маркова з дискретним цілочисловим часом, одиницею якого є віртуальний слот - проміжок часу між послідовною зміною лічильника відстрочки у кожній станції, що не знаходиться в стані простою. Нехай $b(t)$ - стохастичний процес зміни лічильника відстрочки для даної станції, моменти часу t та $t+1$ відповідають початку двох послідовних віртуальних слотів, причому станція передає, коли $b(t)=0$. У той же час, $s(t)$ - стохастичний процес зміни стадії відстрочки $0,...,m$, розширений (в порівнянні з моделлю Бьянкі) значенням -1 для ситуації, коли в черзі немає пакету.

Зауважимо, що, виходячи з прийнятої моделі, ця шкала віртуального часу не має прямої відповідності шкалі реального часу і віртуальні слоти неоднорідні. Як вже було сказано, лічильник відстрочки "заморожується", якщо станція зауважує передачу іншої станції. Тому реальний час, що минув між t та $t+1$, більше слота відстрочки σ при наявності передачі іншій станції. Таким чином, отримаємо три види віртуальних слотів: а) "порожній" слот, під час якого жодна станція не вела передачу, б) "успішний" слот, коли одна і тільки одна станція вела передачу, і в) "колізійний" слот, під час якого сталася колізія.

Двовимірний процес $\{s(t),b(t)\}$ опишемо ланцюгом Маркова, який зображено на рисунку 2.2, де станом простою станції відповідає стан (-1,0). Стани, коли станція не має пакета для передачі, але виконує процедуру відстрочки після вдалої передачі або відмови, - це $(-1,1...W_0-1)$. Нарешті, стан,

коли станція має пакет і виконує процедуру відстрочки, - це всі інші (i,k), де $k = 0,...,W_i - 1$ - значення лічильника відстрочки, а $i = 0,...,m$ - стадія відстрочки.

Нехай $\alpha(i,k)$- стаціонарна імовірність стану (i,k), а $P\{i_2,k_2 \mid i_1,k_1\}$ ймовірність однокрокового переходу з (i_1,k_1) в (i_2,k_2).Введемо наступні позначення:

P_0 - ймовірність спустошення черги після завершення синхронного обслуговування;

P_S - ймовірність приходу хоча б одного пакету за час віртуального слота за умови, що черга даної станції порожня. Очевидно, ця ймовірність включає в себе два компоненти: $P_S = P_S^F + P_S^E$, де P_S^F і P_S^E - ймовірності приходу хоча б одного пакету за час відповідно непорожнього і порожнього слота за умови, що черга даної станції порожня;

P_T - ймовірність приходу хоча б одного пакету за час успішної передачі іншого пакета;

p - ймовірність невдалої спроби передачі через колізії (ймовірність колізії). Вважаємо, що вона не залежить від стадії відстрочки i. Визначимо можливі однокрокові переходи між станами та відповідні їм ненульові ймовірності переходів:

$$P\{i,k \mid i,k+1\} = 1, i \in (0,m), k \in (0,W_i - 2) \tag{2.15}$$

- зменшення лічильника відстрочки;

$$P\{i,k \mid i-1,0\} = p / W_i, i \in (1,m), k \in (0,W_i - 1) \tag{2.16}$$

- невдала спроба передавання і перехід на наступну стадію;

$$P\{0,k \mid i,0\} = (1 - P_0 e^{-\lambda DIFS})(1-p)/W_0, i \in (0,m-1), k \in (0,W_0 - 1) \tag{2.17}$$

- вдала передача, в черзі є ще пакети;

$$P\{-1,k \mid i,0\} = P_0 e^{-\lambda DIFS}(1-p)/W_0, i \in (0,m-1), k \in (0,W_0 - 1) \tag{2.18}$$

- вдала передача, в черзі немає пакетів;

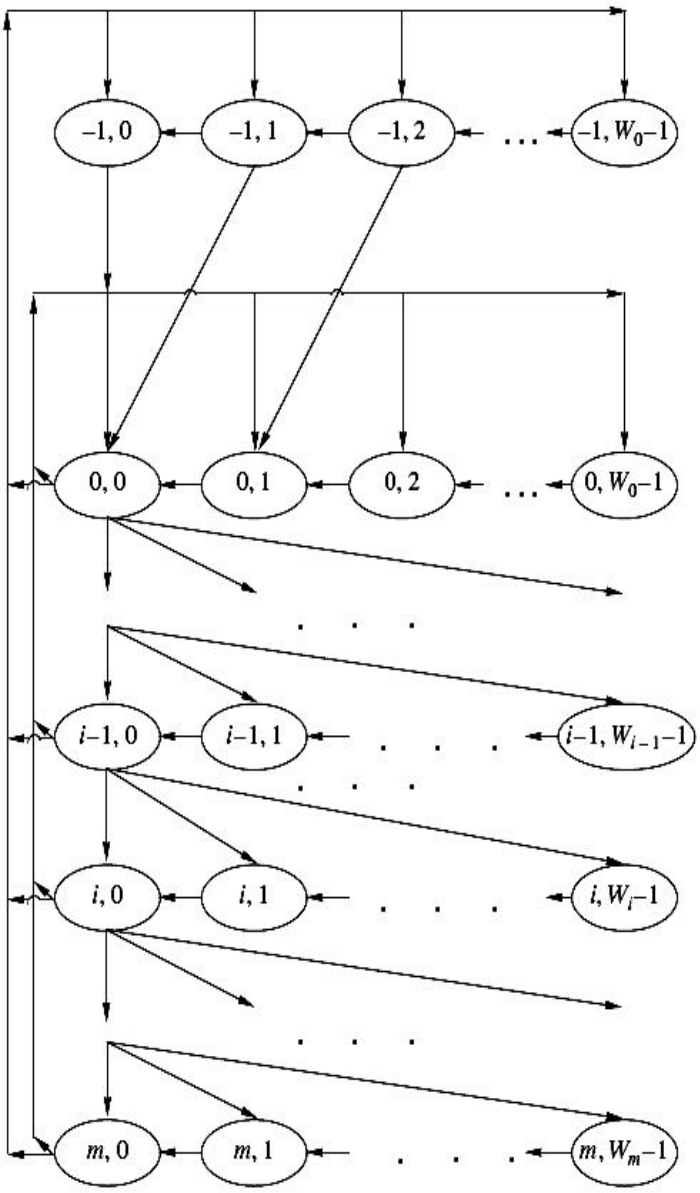

Рисунок 2.2 – Ланцюги Маркова

$$P\{0,k\,|\,m,0\} = \left[\left(1 - P_0 e^{-\lambda DIFS}\right)(1-p) + \left(1 - P_0 e^{-\lambda EIFS}\right)p\right] / W_0, k \in (0, W_0 - 1) \quad (2.19)$$

- остання спроба передачі, після якої пакет видаляється із черги; в черзі залишаються пакети;

$$P\{-1,k\,|\,m,0\} = P_0\left[e^{-\lambda DIFS}(1-p) + e^{-\lambda EIFS}p\right] / W_0, k \in (0, W_0 - 1) \quad (2.20)$$

- остання спроба передачі, після якої пакет видаляється із черги; в черзі немає пакетів;

$$P\{0,k\,|\,-1,k+1\} = P_S, k \in (0, W_0 - 2) \quad (2.21)$$

- зменшення лічильника відстрочки, і в порожню чергу надходить пакет;

$$P\{-1,k\,|-1,k+1\}=1-P_S, k\in(0,W_0-2) \tag{2.22}$$

- зменшення лічильника відстрочки, черга порожня;

$$P\{0,k\,|-1,0\}=\left(P_S^F+P_S^E P_T\right)/W_0, k\in(0,W_0-1) \tag{2.23}$$

- перехід від стану простою в стан відстрочки. Такий перехід має місце, якщо в момент приходу пакета канал був зайнятий або в момент асинхронної передачі приходить ще один пакет;

$$P\{-1,k\,|-1,0\}=P_S^E(1-P_T)/W_0, k\in(0,W_0-1) \tag{2.24}$$

- перехід відповідає асинхронній передачі. Після якої в черзі не залишається пакетів і початкове значення відстрочки $b=k>0$;

$$P\{-1,0\,|-1,0\}=1-P_S+P_S^E(1-P_T)/W_0 \tag{2.25}$$

- немає пакетів, або мала місце асинхронна передача, за час якої не надійшло більше пакетів і $b=0$.

$$\sum_{i=0}^{m}\sum_{k=0}^{W_{i-1}}\alpha(i,k)+\sum_{k=0}^{W_{0-1}}\alpha(-1,k)=1 \tag{2.26}$$

Для $i\in(1,m) i\, k\in(0;W_i-1)$, які відповідають процедурі відстрочки при вибраному пакеті для передавання і вже при першій спробі передати його, стаціонарні ймовірності визначаються за формулами:

$$\begin{aligned}&\alpha(i,k)=\frac{p}{W_i}\alpha(i-1,0)+\alpha(i,k+1),\\&\alpha(i,0)=\frac{p}{W_i}\alpha(i-1,0)+\alpha(i,1)=\ldots=p\alpha(i-1,0)\end{aligned} \tag{2.27}$$

тобто

$$\alpha(i,k)=\frac{W_i-k}{W_i}\alpha(i-1,0), \alpha(i,0)=p^i\alpha(0,0), \tag{2.28}$$

і відповідно їх сума обчислюється наступним чином:

$$\sum_{i=1}^{m}\sum_{k=0}^{W_{i-1}}\alpha(i,k)=\sum_{i=1}^{m}\frac{W_i+1}{2}p^i\alpha(0,0) \tag{2.29}$$

Для $i\in(1,m) i\, k\in(1;W_0-1)$ - тобто стан, який відповідає процедурі відстрочки після вдало переданого пакету або відмови, но при відсутності пакета для передавання, із рівнянь глобального балансу отримаємо:

$$\alpha(-1,k)=\alpha(0,0)P_S\hat{P}_0A(k)/C, \tag{2.30}$$

а для стану простою $(-1,0)$:

$$\alpha(-1,0)=\alpha(0,0)\hat{P}_0A(k)/C, \tag{2.31}$$

де

$$\hat{P}_0=P_0\left[e^{-\lambda DIFS}\left(1-p^{m+1}\right)+e^{-\lambda EIFS}p^{m+1}\right], \tag{2.32}$$

$$A(k)=\sum_{t=k}^{w_0-1}\left(1-P_S\right)^{W_0-1-t}, k=0,\ldots,W_0-1, A=A(0), \tag{2.33}$$

$$C=P_SW_0+P_S^E\left(1-P_T\right)A \tag{2.34}$$

Після спрощення отримаємо:

$$\sum_{k=0}^{w_0-1}\alpha(-1,k)=\alpha(0,0)\hat{P}_0W_0/C \tag{2.35}$$

Для $i=0$ та $k=1$, …, W_0-1 після перетворень отримаємо:

$$\alpha(0,k)=\left[\frac{W_0-k}{W_{0i}}\left(1-\hat{P}_0+\left(P_S^F+P_S^EP_T\right)\frac{\hat{P}_0A}{C}\right)+\frac{\hat{P}_S^2\hat{P}_0}{C}\sum_{t=k+1}^{W_0-1}A(t)\right]\alpha(0,0). \tag{2.36}$$

Далі із наведених вище формул отримаємо:

$$\begin{aligned}\alpha(0,0)^{-1}&=1+\sum_{i=1}^{m}\frac{W_i+1}{2}p\frac{W_0\hat{P}_0}{C}+\\&+\frac{W_0-1}{2}\left(1-\hat{P}_0+\left(P_S^F+P_S^EP_T\right)\frac{\hat{P}_0A}{C}\right)+\frac{\hat{P}_S^2\hat{P}_0}{C}\sum_{k+1}^{W_0-2}\sum_{t=k+1}^{W_0-1}A(t)\end{aligned}. \tag{2.37}$$

Нехай τ - ймовірність синхронної передачі даної станції під час віртуального слоту.

$$\tau=\sum_{i=0}^{m}\alpha(i,0)=\sum_{i=0}^{m}p_i\alpha(0,0)=\frac{1-p^{m+1}}{1-p}\alpha(0,0) \tag{2.38}$$

Приймаючи до уваги незалежність стохастичних процесів $\{s(t),b(t)\}$ всіх станцій, знайдемо ймовірність того, що синхронна передача буде невдалою із-за колізії:

$$p=1-(1-\tau)^{N-1} \tag{2.39}$$

Ймовірність асинхронної передачі за час віртуального слота рівна

$$\tau_a=\alpha(-1,0)P_S^E \tag{2.40}$$

Перейдемо до визначення ймовірностей P_S, P_S^F, P_S^E, P_T. Оскільки $N\lambda\sigma \le 1$, ймовірність потрапляння в чергу даної станції хоча б одного пакета за час порожнього слоту, при умові що ця черга порожня:

$$P_S^E = 1-(1-\tau)^{N-1}\left(1-e^{-\lambda\sigma}\right) \tag{2.41}$$

Для того щоб визначити ймовірності P_S^F, P_T знайдемо часи «непорожніх» слотів, за які пройшла або успішна передача або колізія. Час успішної передачі пакета довжиною l_i рівний:

$$t_i^S = l_i / V + t_{const}^S, при\ \ l_i \le L \tag{2.42}$$

$$t_i^S = t_{RTS} + t_{CTS} + l_i / V + 2\times SIFS + t_{const}^S, при\ \ l_i > L \tag{2.43}$$

$t_{RTS}, t_{CTS} = t_{ACK}, H$ - це час необхідний для передачі відповідно RTS, CTS, ACK, а також заголовку $DATA$. V - швидкість передавання MAC частини кадру. Таким чином ймовірність передачі хоча б одного пакета за час успішної передачі:

$$P_T = 1-\sum_i 1-e^{-\lambda t_i^S} D(l_i) \tag{2.44}$$

При визначені часу колізії знехтуємо ймовірністю настання колізії, в яку задіяно більше двох кадрів. Тоді час колізії складається із часу передавання фрейму максимальної довжини із числа фреймів, які задіяні в колізію, тобто довжина колізії рівна

$$t_{L+1}^C = t_{RTS} + EIFS, при\ \ l_j > L \tag{2.45}$$

з ймовірністю D_{L+1}^C, де

$$D_{L+1}^C = \left(\sum_{j:l_j>L} D(l_j)\right)^2, \tag{2.46}$$

або

$$t_j^C = \left(l_j / V\right) + t_H + EIFS, при\ \ l_j \le L \tag{2.47}$$

з ймовірністю

$$D_j^C = D^2(l_j) + 2D(l_j)\left[\sum_{h:l_h>l_j} D(l_h) + \sum_{h:l_h>L} D(l_h)\right] \tag{2.48}$$

Таким чином ймовірність приходу хоча б одного пакету за час колізії рівна

$$P_C = 1 - \sum_{h \le L+1} e^{-\lambda t_h^C} D_h^C . \qquad (2.49)$$

P_C^F - ймовірність потрапляння пакета за час не порожнього слоту, при умові, що черга даної станції не пуста. Розглянемо три ситуації, які можуть відбутися.

1. Синхронна успішна передача другої станції. Ймовірність надходження пакета в даному випадку буде рівна $Q_S^S P_T$, де $Q_S^S = (N-1)\tau(1-\tau)^{N-2}$ - умовна ймовірність для даної ситуації.

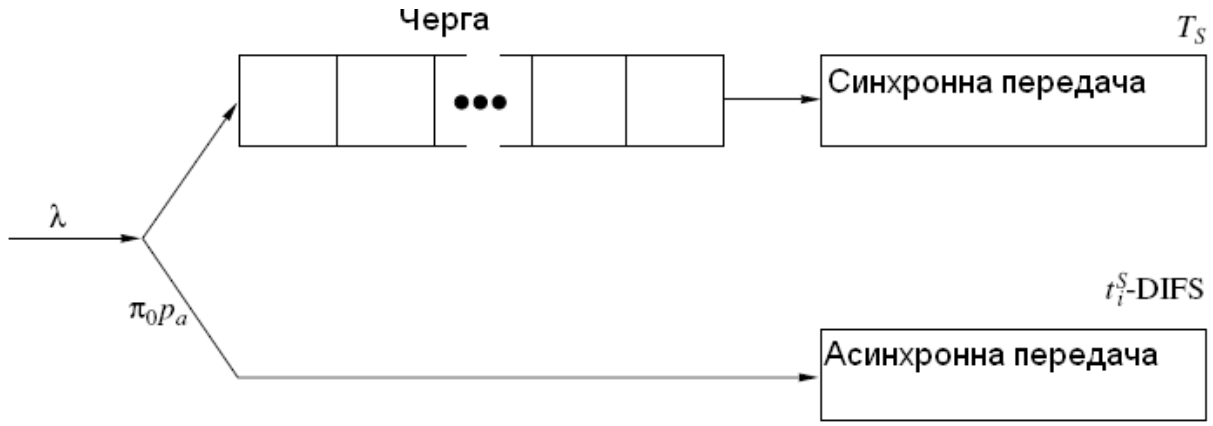

Рисунок 2.3 – Процес зміни черги

Асинхронна передача другої станції. При аналіза даного випадку використовуємо припущення про те, що за один віртуальний слот може пройти тільки одна псинхронна передача та одна успішна. Тоді умовна ймовірність для даного випадку рівна $Q_A = (N-1)\tau_A$, а ймовірність надходження $Q_A P_T$.

3. У випадку колізії ймовірність надходження рівна $Q_S^C P_C$, де $Q_S^C = 1 - Q_E - Q_S^S - Q_A$ - ймовірність колізії, в якій не задіяна дана станція, а $Q_E = (1-\tau-\tau_A)^{N-1}$ - ймовірність порожнього слота при умові відсутності передачі даної станції.

$$P_S^F = (Q_S^S + Q_A)P_T + Q_S^S P_C . \qquad (2.50)$$

Для завершення побудови моделі залишилося знайти P_0 - ймовірність спустошення черги після завершення обслуговування. Проце зміни черги показано на рисунку 2.3.

Пакети, які поступають на станцію, яка не зайнята обслуговуванням інших пакетів, з ймовірністю p_a обслуговуються асинхронно, а тому успішно протягом t_i^S-DIFS (при довжині пакета l_i). В інших випадах вони потрапляють буфер розміром B і обслуговуються синхронно протягом випадкового часу із середнім значенням T_S.

Припустимо, що час середнього обслуговування розподілено за експоненціальним законом. Тоді зміна черги синхронної передачі пакетів описуються процесом «появи-знищення», стаціонарна ймовірність настання i якого рівна

$$\pi_i = \pi_0 \lambda_0 \lambda^{i-1} T_S^i,\ i = 1,\ldots,B, \tag{2.51}$$

де $\lambda_0 = (1 - p_a)\lambda$. Ймовірність спустошення черги після завершення синхронної передачі рівна $P_0 = \pi_1 / (1 - \pi_0)$, а

$$\pi_0 = \frac{1}{1 + (1 - p_a)\sum_{i=1}^{B} (\lambda T_S)^i}, \tag{2.52}$$

то

$$P_0 = \frac{1}{\sum_{i=1}^{B} (\lambda T_S)^{i-1}} = \frac{1 - \lambda T_S}{(1 - \lambda T_S)^B}, \tag{2.53}$$

2.4 Висновок до другого розділу

Запропонована у даному розділі модель оцінки продуктивності безпровідної локальної мережі з довільним навантаженням дозволяє отримувати оцінку таких основних показників як середній час обслуговування пакета, середній час його затримки на MAC-рівні та ймовірність відмови, а

також оптимізувати механізм передавання пакетів в залежності від інтенсивності їх потрапляння та конфігурації мережі.

3. РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ ЕФЕКТИВНОСТІ БЕЗПРОВІДНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1. Оцінка показників ефективності безпровідних локальних мереж

Для знаходження ймовірності p_a та середнього часу синхронного обслуговування розібє'мо пакети, які обслуговуються синхронно, які поступають протягом всіх можливих віртуальних слотів (i,k) на чотири категорії:

1) надходження протягом слотів $(i \geq 0, k)$;

2) надходження протягом слотів $(-1, k > 0)$;

3) надходження протягом передавання іншій станції під час слотів $(-1, 0)$;

4) надходження протягом асинхронної передачі даної станції;

Для кожної із цих категорій підрахуємо середню кількість надійшовших протягом синхронного обслуговування пакетів n_i та n_i^0 $(i = 1,...,4)$, де n_i - їх загальна кількість, а n_i^0 - кількість таких пакетів, які поступають у порожню чергу.

Відомо, що

$$\begin{aligned} T_S &= \left[\left(T_S^* + \Delta * \right) \sum_{i=1}^{4} \left(n_i - n_i^0 \right) + \sum_{i=1}^{4} T_S^i n_i^0 \right] / \sum_{i=1}^{4} n_i, \\ p_a &= \tau_a / \left(\tau_a + \sum_{i=1}^{4} n_i^0 \right) \end{aligned} \tag{3.1}$$

де

$$T_S^* = \sum_{i=0}^{m} p_i \left(\frac{W_i - 1}{2} t_1 + t_2 - (1-p) DIFS \right), \tag{3.2}$$

а

$$t_1 = Q_E \delta + \left(Q_S^S + Q_A \right) \sum_i t_i^S D(l_i) + Q_S^C \sum_{i \leq L+1} t_i^C D_i^C \tag{3.3}$$

$$t_2 = (1-p)\sum_i t_i^S D(l_i) + p\sum_{i\le L+1} t_i^C D_i^C \qquad (3.4)$$

- середня тривалість віртуальних слотів, в які дана станція відповідно утримується від передачі та передає. T_S^i - середній час обслуговування пакетів різних категорій i, які поступають у порожню чергу, а $\Delta^* = (1-p^{m+1})$ DIFS відображає той факт, що передача пакету, який поступив в не порожню чергу, починаються з інтервалу DIFS, який наступає після підтвердження успішної передачі, крім випадку відмови, коли обслуговування відбувається після закінчення інтервалу EIFS. Знайдемо значення n_i, n_i^0 та T_S^i для кожної із введених категорій.

Категорія 1. Надходження протягом слотів $(i \ge 0, k)$. Пакети поступають в порожню чергу протягом інтервалів DIFS (або EIFS у випадку відмови), який наступає після успішної передачі (або відказом) даної станції його попереднього пакету. Тому $n_1^0 = n_{1S}^0 = n_{1C}^0$, де

$$n_{1S}^0 = (1-e^{-\lambda DIFS})(1-p)P_0\sum_{i=0}^{m}\alpha(i,0) \qquad (3.5)$$

і

$$n_{1C}^0 = (1-e^{-\lambda EIFS})(1-p)pP_0\alpha(m,0) \qquad (3.6)$$

а загальна кількість поступивших пакетів цієї категорії

$$n_1 = \lambda t_1 \sum_{i=0}^{m}\sum_{k=1}^{w_i-1}\alpha(i,k) + \lambda t_2 \sum_{i=0}^{m}\alpha(i,0) \qquad (3.7)$$

і

$$T_S^1 = T_S^* + \frac{n_{1S}^0}{n_1^0}\frac{DIFS}{2} + \frac{n_{1C}^0}{n_1^0}\frac{EIFS}{2} \qquad (3.8)$$

Категорія 2. Надходження протягом слотів $(-1, k>0)$. Як тільки перший пакет, що надійшов протягом кожного із даних слотів поступає в порожню чергу, то

$$n_2^0 = Q^*\sum_{k=1}^{w_0-1}\alpha(-1,k), n_2 = \lambda t_1 Q^*\sum_{k=1}^{w_0-1}\alpha(-1,k), \qquad (3.9)$$

де

$$Q^* = Q_E\left(1-e^{-\lambda\sigma}\right)+\left(Q_S^S+Q_A\right)\sum_i\left(1-e^{-\lambda t_i^S}\right)D(l_i)+Q_S^C\sum_{\lambda\le L+1}\left(1-e^{-\lambda t_i^C}\right)D_i^C \qquad (3.10)$$

У цьому випадку при надходженні пакета в порожню чергу середній час до першої спроби передавання скорочується до $\left(k-\frac{1}{2}\right)t_1$ і середній час обслуговування

$$T_S^2 = T_S^* - \frac{Q^* t_1}{n_2^0}\sum_{k=1}^{w_0-1}\left(\frac{W_0}{2}-k\right)\alpha(-1,k), \qquad (3.11)$$

Категорія 3. Надходження протягом слотів $(-1,0)$ і в цей час йде передавання другої станції. Для цього випадку

$$n_3^0 = \left[\left(Q_S^S+Q_A\right)\sum_i\left(1-e^{-\lambda t_i^S}\right)D(l_i)+Q_S^C\sum_{i\le L+1}\left(1-e^{-\lambda t_i^C}\right)D_i^C\right]\alpha(-1,0), \qquad (3.12)$$

а

$$n_3 = \left[\left(Q_S^S+Q_A\right)\lambda\sum_i t_i^S D(l_i)+Q_S^C\lambda\sum_{i\le L+1}t_i^C D_i^C\right]\alpha(-1,0), \qquad (3.13)$$

і середній час обслуговування $T_S^3 = \Delta_3 + T_S^*$, де

$$\Delta_3 = \frac{1}{2(Q_E)}\left[Q_S^S\lambda\sum_i t_i^S D(l_i)+Q_S^C\sum_{i\le L+1}t_i^C D_i^C\right] \qquad (3.14)$$

Категорія 4. Надходження протягом слотів $(-1,0)$ і протягом цього слоту проходить асинхронна передача цієї станції. Тоді середній час обслуговування для пакета, що потрапив у порожню чергу синхронно обслуговуючих пакетів протягом асинхронної передачі пакетів цієї ж станції обчислюється

$$T_S^4 = T_S^* + \frac{1}{2} - \sum_i t_i^S D(l_i), \qquad (3.15)$$

а кількість таких пакетів рівна $n_4^0 = \tau_A P_T$ у той час як загальна кількість пакетів цієї категорії

$$n_4 = \tau_A\lambda\sum_i t_i^S D(l_i) \qquad (3.16)$$

В загальному, враховуючи асинхронну передачу, отримаємо середній час, який затрачається на обслуговування одного пакету (відкидаючи «помилкові» пакети із-за переповнення буфера):

$$T = \frac{\pi_0 p_a}{1-\pi_b}\sum_i \left(t_i^S - DIFS\right)D(l_i) + \frac{1-\pi_0 p_a - \pi_b}{1-\pi_b}T_S \qquad (3.17)$$

Перший доданок відображає асинхронний механізм передачі, а другий додано синхронний.

Знайдемо інші показники ефективності. Очевидно, що ймовірність відмови в обслуговуванні пакету

$$p_r = 1-(1-\pi_b)\left[1-\pi^{m+1}(1-\pi_a)\right] \qquad (3.18)$$

Відмова відбувається при: а) повній черзі, коли кількість пакетів у ній рівна B з ймовірністю π_B; б) коли завершується кількість попиток на передавання пакетів з ймовірністю $p^{m+1}(1-p_a)$.

На основі формули Літла знаходимо середній час затримки пакета на MAC рівні (також відкидаючи «помилкові» пакети із-за переповнення буфера), тобто середній час його перебування на даній станції, включаючи можливу затримку в черзі та обслуговуванні:

$$T_{MAC} = \frac{\pi_0 p_a}{1-\pi_b}\sum_i t_i^S D(l_i) + \frac{1-\pi_0 p_a - \pi_b}{1-\pi_b}\frac{\sum_{i=1}^{B} i\pi_i}{\lambda_0\pi_0 + \lambda\sum_{i=1}^{B-1}\pi_i} = \qquad (3.19$$

$$\frac{\pi_0 p_a}{1-\pi_b}\sum_i t_i^S D(l_i) + \frac{1}{(1-\pi_b)\lambda}\sum_{i=1}^{B} i\pi_i$$

)

3.2. Проектування, практична реалізація та тестування веб-застосунку

Веб-додаток для моделювання ефективності роботи безпровідної локальної мережі реалізовано як Java аплет з можливістю прикріплення даного додатку до веб-сторінки з метою розширення її функціональних можливостей.

На рисунку 3.1 наведено архітектуру розробленого Java-аплету та показано процес взаємодії його основних модулів.

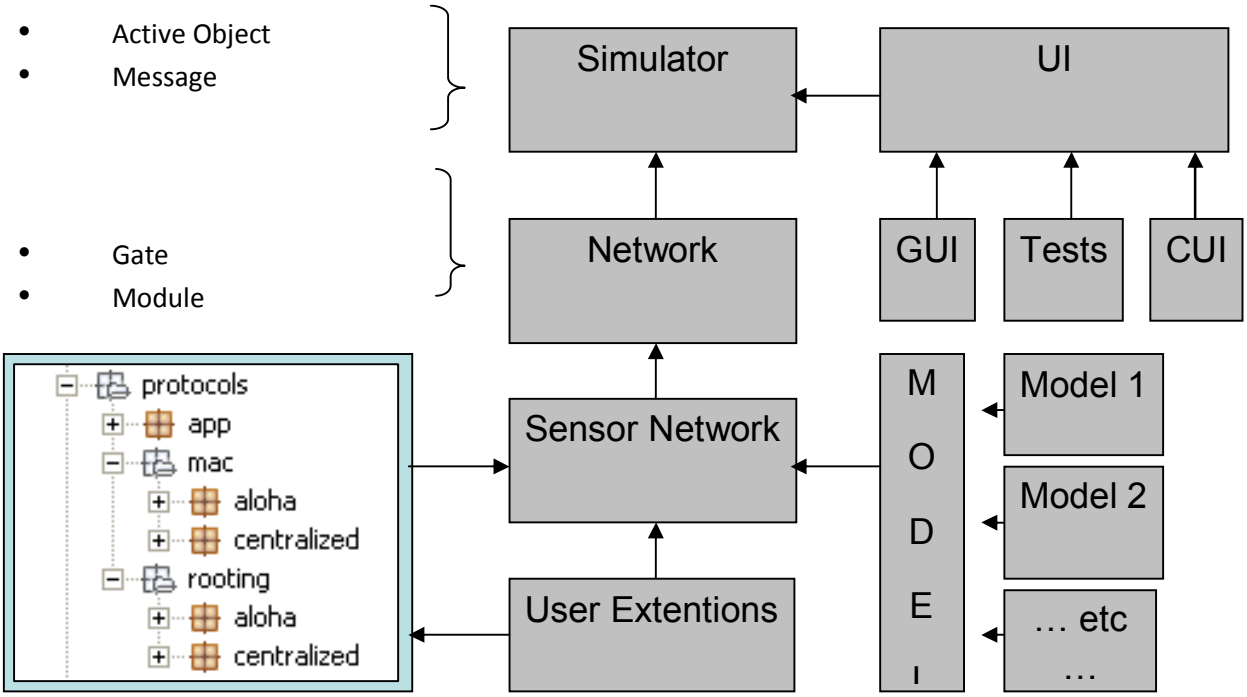

Рисунок 3.1 – Архітектура веб-застосунку для моделювання ефективності локальної безпровідної мережі

Ядром системи є Dispatcher, який проводить управління повідомленнями IMessage між об'єктами ActiveObject. Стандартна реалізація - NetObject, інтерфейс INetObject. Mot є розширенням цього класу, в який додані методи IMovingObject, потужність передавача, поріг прийому і стандартна лінійна топологія (топологія - те, як сполучені модулі всередині нього, дивіться Tutorial_Protocol). Основна функціональність NetObject - надає можливість керувати наповненням його модулями і Гейт (для прийому повідомлень). Гейт - якийсь «зв’язок», що з'єднує два модулі. Параметрами методів для роботи з гейтом є «Class <? extends IPacket> msgClass ». Це означає, що диспетчер диференціює повідомлення IMessage за належністю об'єкта його даних (IMessage містить метод Object getData ()) до того чи іншого класу msgClass. Видно, що цей клас повинен реалізовувати інтерфейс IPacket. Цей інтерфейс - те, що можна пропускати через гейти і, відповідно, передавати між модулями усередині одного NetObject. Докладніше - в Tutorial_Protocol.

Далі розглянемо життєвий цикл при передачі повідомлення IMessage в web-додатку.

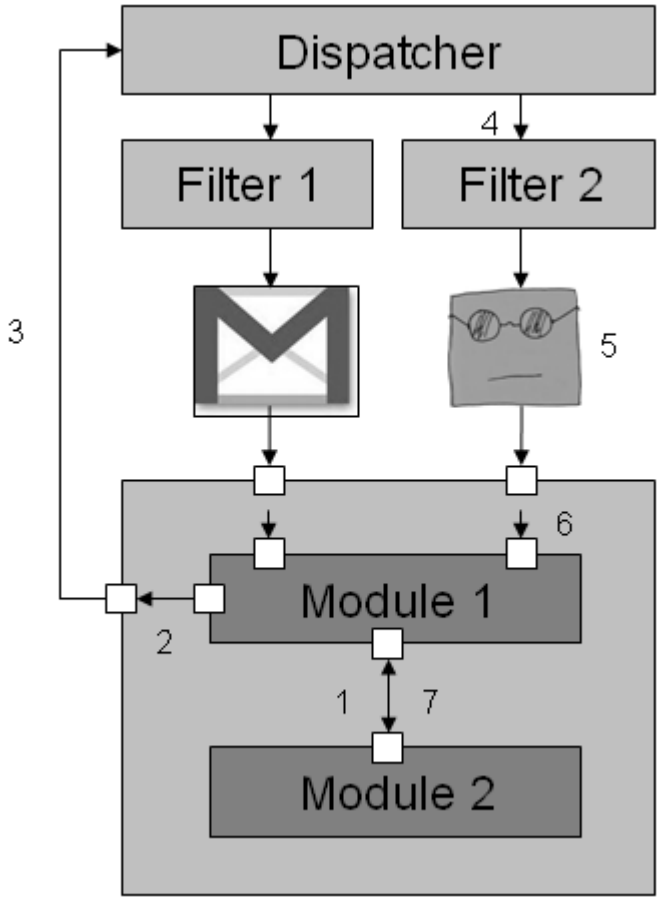

Рисунок 3.2 – Процес передачі повідомлень

На даній схемі зображено передача повідомлення по кроках (підписано цифрами):

1. Модуль2 мота1 відсилає повідомлення IPacket типу «квадрат в окулярах ».

2. Модуль1 мота1 формує IMessage з отриманими «квадратом » в якості даних.

3. Диспетчер отримує повідомлення і відсилає його моту2 через фільтр.

4. Фільтр визначає, що повідомлення є «квадратом» і виробляє відповідні дії, потім пересилає адресату.

5. Мот2 приймає повідомлення на відповідний класу «квадрат» гейт. Припустимо, що до нього приєднаний модуль1. Він обробляє повідомлення і передає модулю2.

На рисунку 3.3 Наведено головне вікно розробленого веб-додатку, яке включає відображення між станціями безпровідної локальної мережі, а також процес логування передачі пакетів, з метою отримання відповідних статистичних даних для подальшого аналізу.

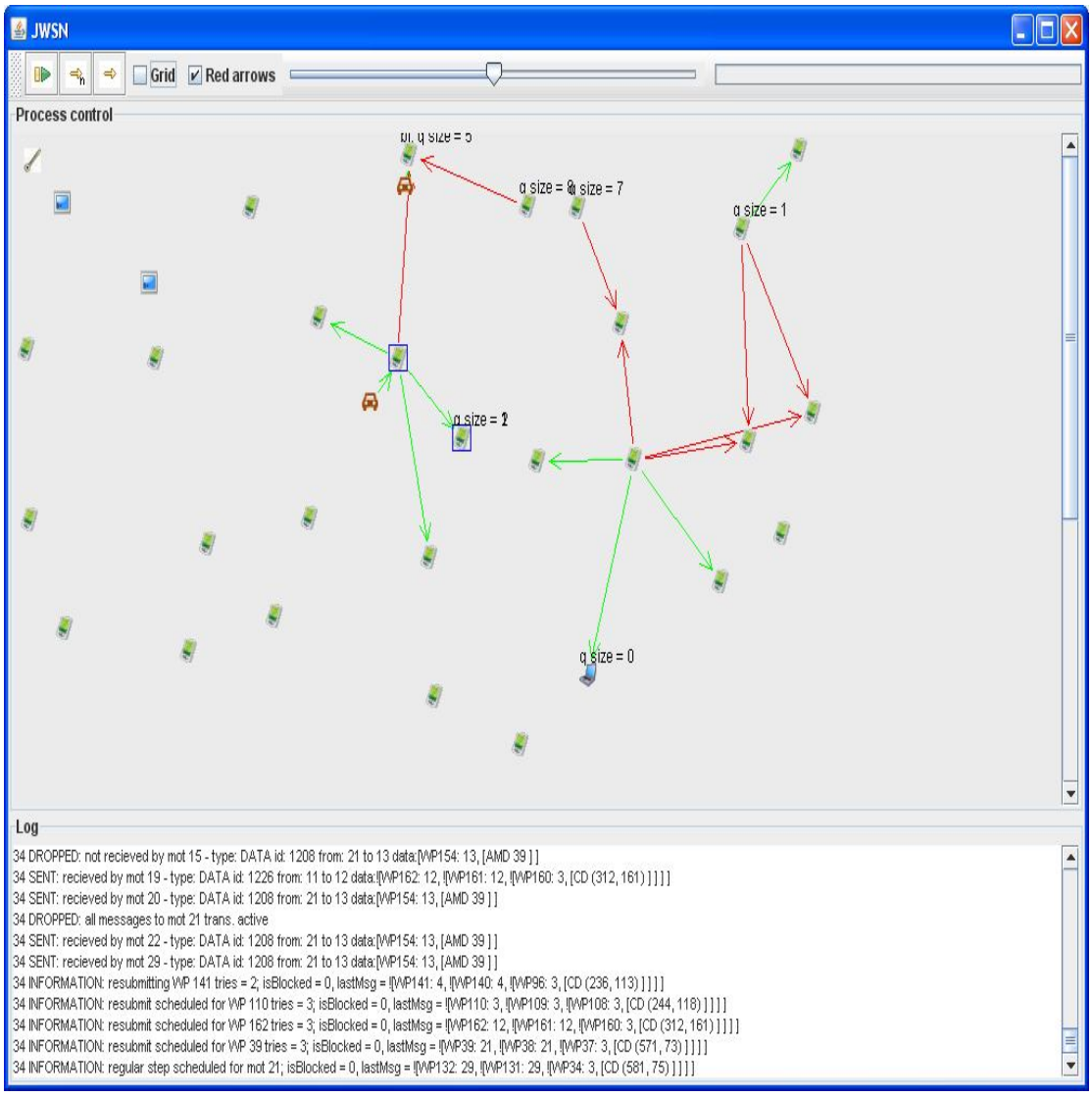

Рисунок 3.3 – Веб-додаток для моделювання безпровідної мережі

На рисунку 3.4 показано процес логування відправки пакетів

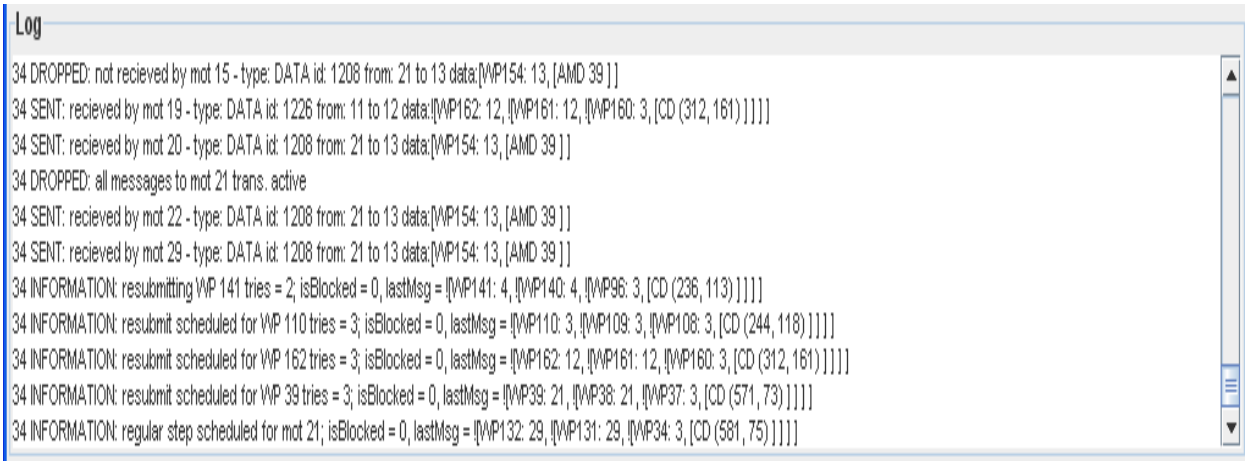

Рисунок 3.4 – Логування відправки пакетів

Розглянемо коротко процес функціонування розробленого додатку з метою моделювання роботи безпровідної локальної мережі.

1. Оголосити необхідну кількість пакетів передачі або будь-яких інших об'єктів з суперкласом NetObject.

Mot m1 = new Mot (100, 100, power, threshold);

Mot m2 = new Mot (300, 100, power, threshold);

Mot m3 = new Mot (200, 100, 100 * power, threshold);

m1.addModule ("mac", new CommonMac (m1));

m1.addModule ("net", new Net (m1));

m1.addModule ("app", new SenderApp (m1));

m2.addModule...

m3.addModule ...

2. При лінійній топології модулів всередині можна безпосередньо її задати, перші 3 рівня зарезервовані під mac, net і app. Інакше або з'єднувати вручну (як показано в Tutorial_Protocol), або перевантажувати createTopology.

m1.createTopology ();

m2.createTopology ();

m3.createTopology ();

3. Можливо зчитати параметри для моделювання з файлу.

List mots = new LinkedList ();

mots.add (m1); mots.add (m2); mots.add (m3);

```
try {
FieldParser.ReadStyles (new FileInputStream ("Descriptions.xml"), mots);
} Catch (FileNotFoundException nf) {... }
```

4. Поставити топологію мережі для hard-coded протоколів.

```
IDispatcher disp = Dispatcher.getInstance ();
IGraph g = new Graph ();
for (int i = 0; i <3; i + +) {
g.newVertex (new Integer (i));
}
 g.addNeighbour (0 +1);
 ...
g.solvePaths (2);
disp.setTopology (g);
```

5. Створити UI.

```
BasicUI.createUI ();
```

6. Додати станції, щоб їх відобразив візуалізатор.

```
disp.addActiveObjectListener (m1);
disp.addActiveObjectListener (m2);
disp.addActiveObjectListener (m3);
```

Щоб створити новий протокол, необхідно виконати наступну послідовність дій:

Кожен NetObject збирається з таких модулів, які пересилають один одному об'єкти класу IPacket. Для цього в кожного модуля є методи інтерфейсу IModule, такі, як:

```
IGate declareGate (String name)
 IGate getGate (String name)
```

Вони дозволяють задати "порти", через які пресилаются повідомлення. Параметр name - унікальний в рамках модуля ім'я порту. Щоб позначити зв'язок, пару таких портів потрібно з'єднати між собою або односторонньо, або дуплексно, наприклад, так:

/ / IGate gate <-> IGate dest

gate.setTo (dest);

dest.setFrom (gate);

gate.setFrom (dest);

dest.setTo (gate);

Очевидно, одностороннє підключення виглядає так:

//IGate gate -> IGate dest

gate.setTo (dest);

dest.setFrom (gate);

Щоб обробляти пакет, необхідно перевантажити метод recieveMessage модуля: - boolean recieveMessage (IPacket m); Усередині цього методу можна звертатися до поля модуля "String arrivedOn", щоб визначити, на який з портів прийшло повідомлення (IPacket), це поле містить ім'я відповідного порту . Тепер необхідно зайнятися створенням елемента мережі (EC - NetObject або Mot), який містить цей протокол. Для обміну повідомленнями з іншими елементами мережі служить метод sendMessage (IMessage m) диспетчера. Відповідно, отримують повідомлення від диспетчера у вигляді IMessage: recieveMessage (IMessage m). Вони містять IPacket в якості даних. Відповідно, щоб визначити, якому з модулів прийшло повідомлення, додаток містить по порту на кожен клас, методи:

- IGate declareInputGate (Class msgClass);

- IGate getInputGate (Class msgClass);

- Boolean hasInputGate (Class msgClass);

І саме з ними необхідно з'єднати модуль, який отримає вихідне повідомлення.

Розроблений Java аплет дозволяє ефективно моделювати роботу безпровідної локальної мережі (додавати, видаляти станції, управляти пакетами, часом та швидкістю передавання між станціями). Даний додаток дозволяє отримувати сатистичні дані для описаної в попередньому розділі

моделі, а також після її застосування проводити апробацію на основі змодельованих даних.

3.3. Експериментальні дослідження з моделлю

Для оцінки точності проведено порівняння результатів, отриманих за допомогою описаної вище моделі з даними із літературних джерелі. Дані для моделі одержано на основі імітації функціонування безпровідної локальної мережі у розробленому веб-додатку. Об'єктом чисельних досліджень була безпровідна локальна мережа ad hoc, яка працює під управлінням протоколу IEEE 802.11b із швидкістю $V = 11 мбіт/с$. Значення параметрів протоколу, які використовувалися при моделюванні, наведено у таблиці 4.1. Розмір пакету l (в байтах) вибирався рівномірно із множини $\{1,...,2000\}$, а розмір черги кожної станції обмежений значенням $B = 16$ (пакетів).

На рисунках 3.5 та 3.6 представлені деякі результати оцінки середнього часу обслуговування T і середнього часу затримки T_{MAC} при варіюванні інтенсивності надходження пакетів λ для випадків при $N = 10$ та $N = 40$ з використанням RTS-межі $L = 560$ байт. Ці результати, отримані як аналітично (суцільні лінії), так і імітаційно (пунктирні лінії), демонструють порогоподібний характер залежностей $T(\lambda)$ і $T_{MAC}(\lambda)$: із збільшенням A значення T і T_{MAC} спочатку повільно ростуть, що відповідає періоду нормального навантаження на мережу, а потім після короткого перехідного періоду, який тим коротший, чим більше число станцій N, стають рівними деяким граничним значенням, відповідно до випадку високого навантаження. Видно, що як при нормальній, так і при високому навантаженні аналітична модель досить точна: похибка не перевищує 8%. Великі розбіжності значень показників продуктивності, отриманих аналітично та імітаційно, спостерігаються тільки в короткий перехідний період: в аналітичних кривих поріг більш різкий (майже вертикальний).

Таблиця 3.1- Значення параметрів протоколу IEEE 802.11b

Час передавання заголовку H	227 мкс	Слот, σ	20 мкс
Час передавання кадру ACK, t_{ACK}	202 мкс	SIFC	10 мкс
Час передавання RTS, t_{RTS}	207 мкс	DIFC	50 мкс
Мінімальне конкурентне вікно, CW_{MIN}	32	EIFC	364 мкс
Максимальне конкурентне вікно, CW_{MAX}	1024	m	7

Застосуємо розроблений аналітичний метод для оптимізації RTS-межі L, мінімізуючи показник T. На рисунку 4.3 показані залежності оптимальної межі L_{opt} від інтенсивності λ при різних N. Ці залежності також порогоподібні: до деякого порогу (який, як можна помітити, - дивіться криві для $N = 40$ на рисунках 4.5, 4.6 і 4.7 - приблизно збігається з порогом для кривих $T(\lambda)$ і $T_{MAC}(\lambda)$ мережа працює в режимі нормального навантаження, ймовірність колізії мала і тому оптимальний механізм Базового Доступу, тобто $L_{opt} = 2000$, так як всі пакети не довше 2000 байт.

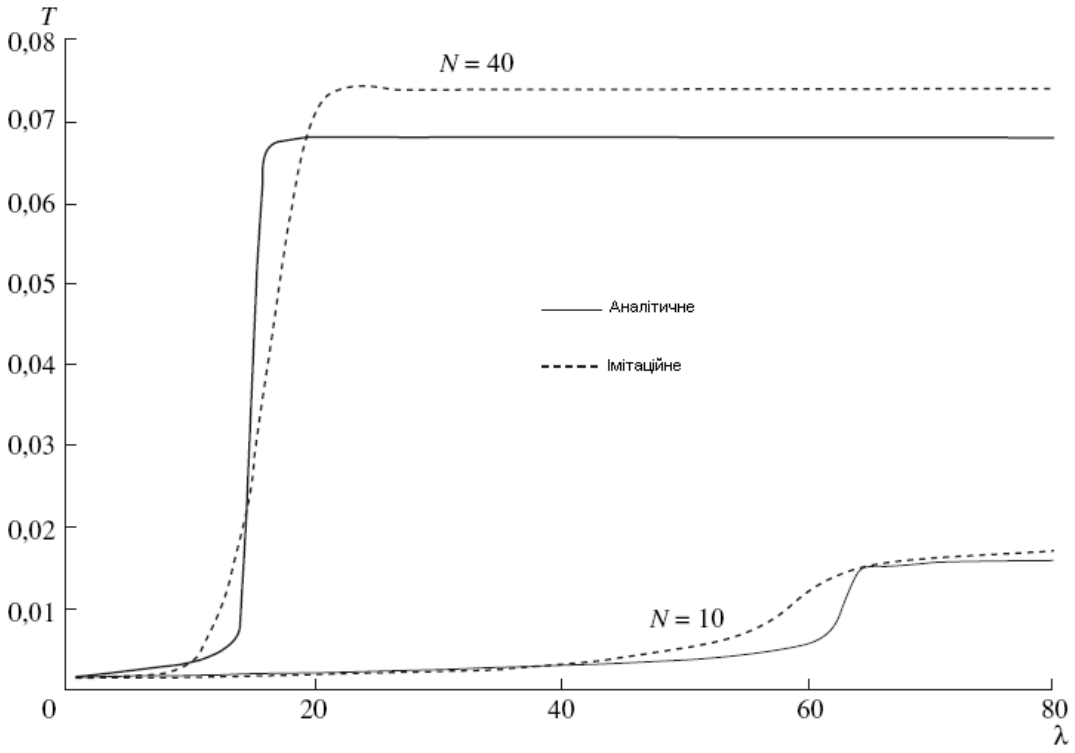

Рисунок 3.5 – Залежність середнього часу обслуговування $T(c)$ від інтенсивності надходження пакетів $\lambda(c^{-1})$

Після цього порогу, який тим різкіший, чим більше N, межа L_{opt} встановлюється рівною фіксованим значенням, залежним від N. Результати застосування цього оптимізованого гібридного методу доступу в порівнянні зі сценаріями, коли для всіх пакетів використовується або (а) тільки механізм Базового Доступу, або (б) тільки механізм RTS/CTS, показані на рисунку 3.8. Видно, що для будь-якої інтенсивності λ така детальна оптимізація дозволяє лише злегка поліпшити значення T в порівнянні з мінімумом із значень, що відповідають сценаріям а) та б).

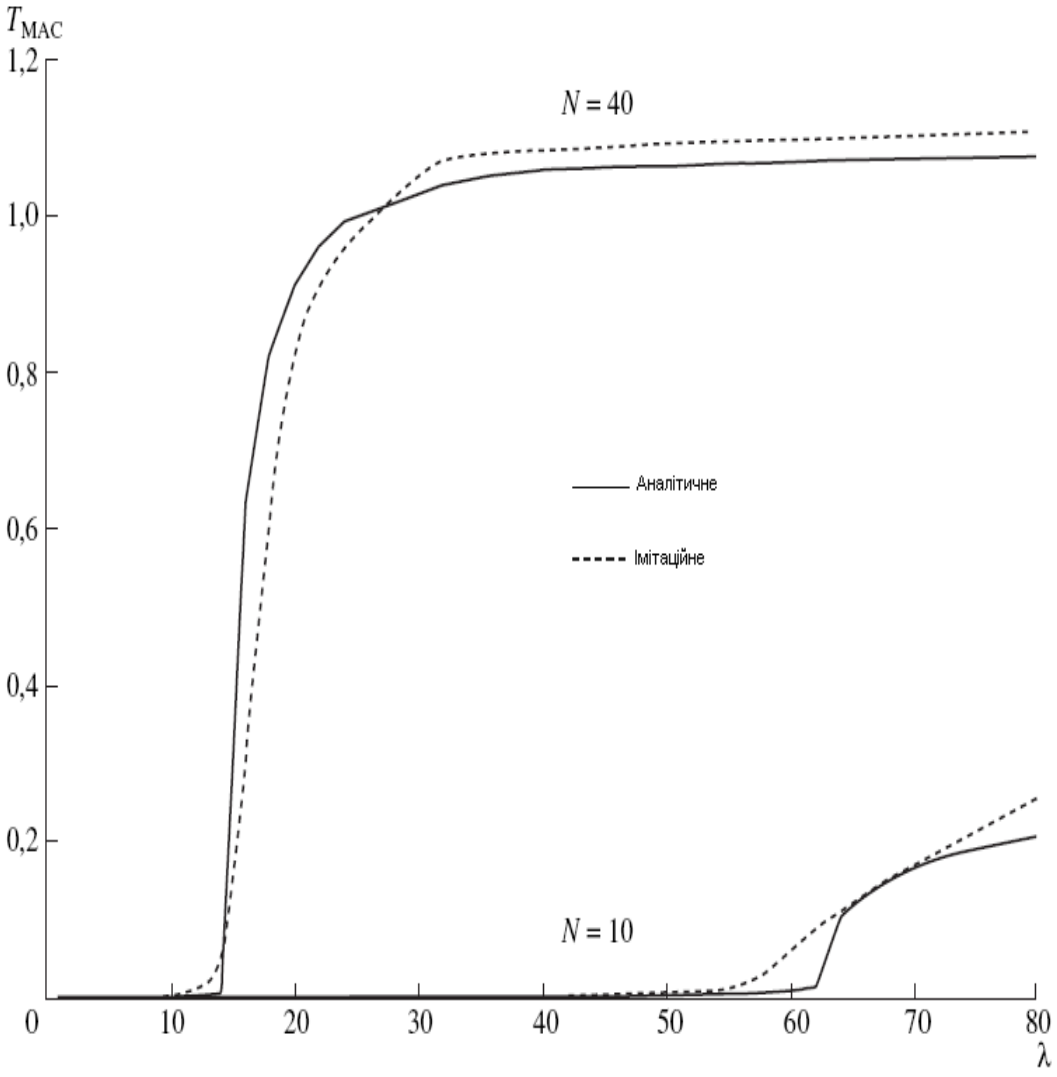

Рисунок 3.6–Залежність середнього часу затримки $T_{MAC}(c)$ від Інтенсивності λ

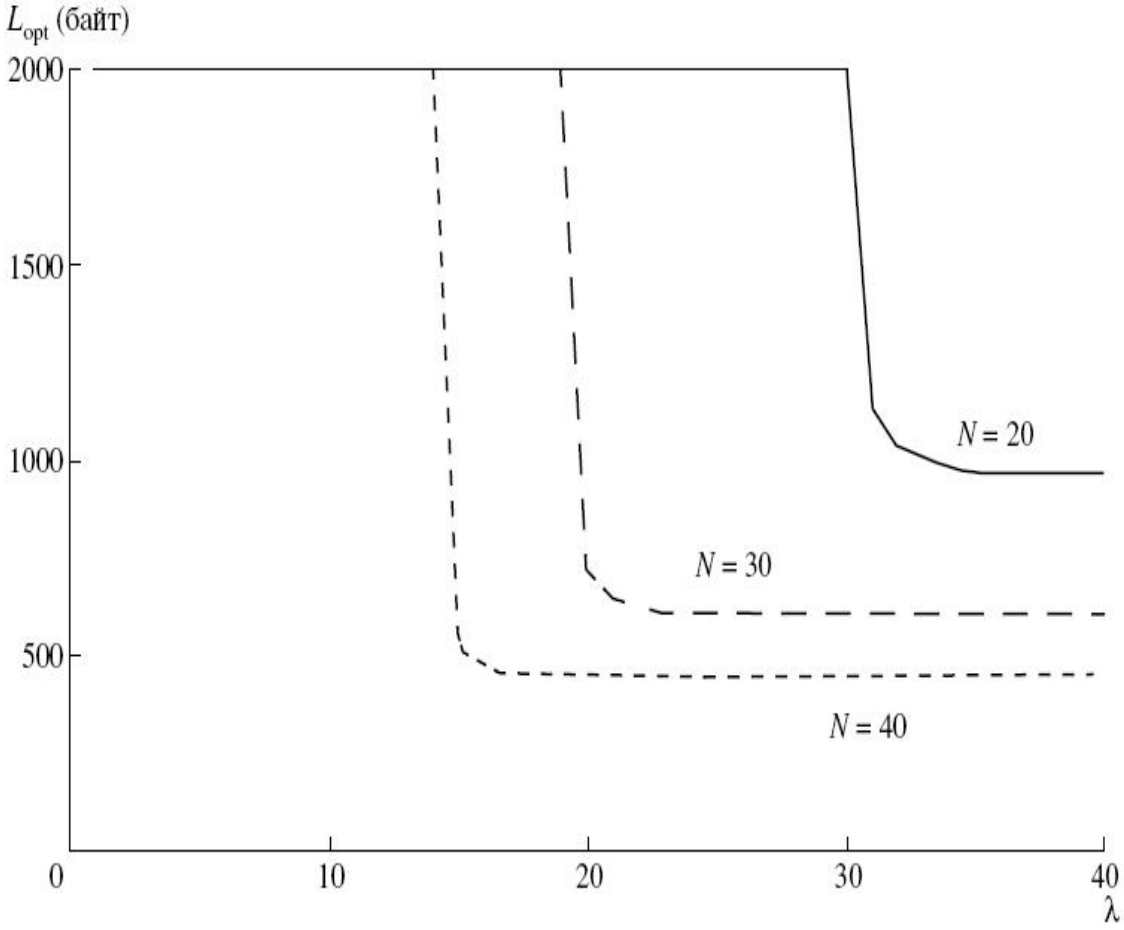

Рисунок 3.7 – Залежність оптимальної RTS межі L_{opt} - від інтенсивності λ при різних N

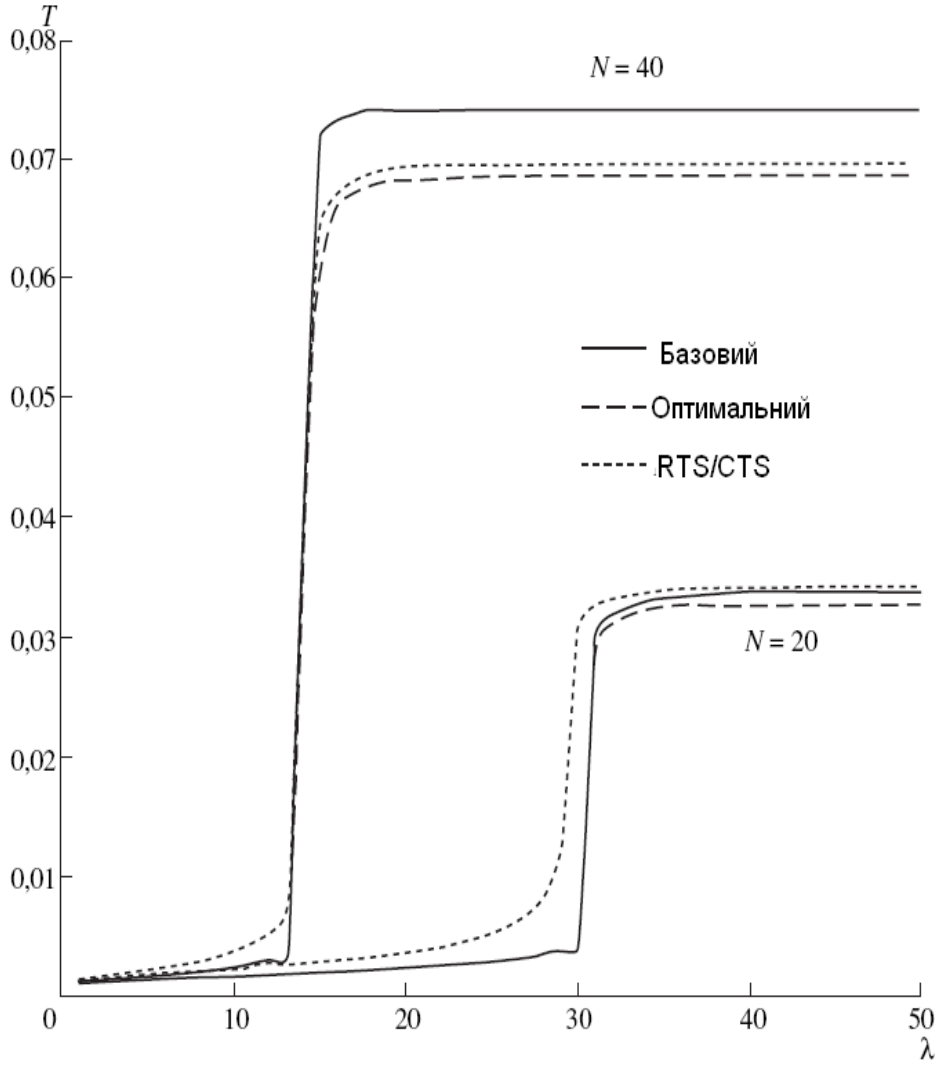

Рисунок 3.8 – Середній час обслуговування $T(c)$ при різних механізмах доступу

Це означає, що можна використовувати наступну стратегію, застосовуючи тільки розроблений аналітичний метод:

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

2) вибрати порогове значення $\lambda_t(N)$, якому відповідає значення T, менше T_{opt} на $d\%$;

3) застосовувати механізм базового доступу при $\lambda < \lambda_T(N)$ та гібридний механізм при порозі $L = L_{opt}(N)$ при $\lambda \geq \lambda_T(N)$. Наприклад вибираємо $d = 5\%$. Тоді при $N = 40$ отримаємо $L_{opt} = 453$, $T_{opt} = 68.2$ мс та $\lambda_t(N) \approx 16c^{-1}$. Порівнюючи значення T, отримані за допомогою імітаційної моделі при

$\lambda = \lambda_T(N)$: для механізму базового доступу $T = 63.9$ мс, а для гібридного механізму $T = 62$ мс, тобто значення T при інтенсивності $\lambda_t(N)$, які знайдені аналітично, практично співпадають, і звідси випливає, що інтенсивність дійсно є пороговою.

3.4. Висновок до третього розділу

В третьому розділі кваліфікаційної роботи розроблений Java аплет який дозволяє ефективно моделювати роботу безпровідної локальної мережі (додавати, видаляти станції, управляти пакетами, часом та швидкістю передавання між станціями). Даний додаток дозволяє отримувати статистичні дані для описаної в попередньому розділі моделі, а також після її застосування проводити апробацію на основі змодельованих даних.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Основні принципи конструювання робочого місця користувача ЕОМ.

Ергономіка (від грецьк. ἔργον наука про пристосування посадових– у традиційному розумінні –роботи») обов‘язків, робочих місць, обладнання та комп‘ютерних програм задля створення найбільш безпечних та ефективних умов праці для людини, виходячи з фізичних і психічних особливостей людського організму.

Більш широке визначення ергономіки, яке було прийняте в 2010 році Міжнародною асоціацією ергономіки (IEA) (Міжнародною ергономічною це наукова дисципліна, що вивчає–асоціацією), звучить так: «Ергономіка взаємодію людини та інших елементів системи, а також сфера діяльності щодо застосування теорії, принципів, даних і методів цієї науки для забезпечення благополуччя людини та оптимізації загальної продуктивності системи».

З цього визначення випливають такі головні завдання ергономіки:

1. Проведення досліджень, спрямованих на пристосування елементів системи "людина – трудовий процес" до природних фізичних і психічних можливостей працівника.

2. Прагнення до забезпечення таким шляхом умов для максимальної ефективності праці.

3. Прагнення запобігти всім можливим загрозам для здоров‘я працівника.

4. Прагнення до оптимальної витрати біологічних ресурсів у процесі праці.

Загальні ергономічні вимоги для організації робочого місця користувача ПЕОМ (ГОСТ 12.2.049-80, ГОСТ 122032-78, ГОСТ 22269-76). Ці вимоги встановлюють основні параметри робочого місця, оснащеного дисплеєм, і враховують особливість виконуваних робіт.

ПАРАМЕТРИ РОБОЧОГО МІСЦЯ ПОВИННІ БУТИ НАСТУПНИМИ.

Площа кабінету, в якому буде проходити робота повинна бути не менш 6 м², а об’єм не менш 24 м³. Для внутрішньої обробки приміщення повинні використовуватися дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі – 0,7-0,8; для стін – 0,5-0,6; для підлоги – 0,3-0,5.

Конструкція робочого столу повинна забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання. Конструкція крісла повинна забезпечувати підтримку раціональної робочої пози під час роботи з відео-дисплейним терміналом (Далі ВДТ) і ПЕОМ, дозволяти змінювати позу з метою зниження статичного напруження м'язів шийно-плечової області і спини для попередження розвитку втоми працюючого (згідно з ГОСТ 12.2.032-78). Поверхня сидіння, спинки та інших елементів стільця (крісла) повинна бути напівм'якою, з покриттям, що не електризується, неслизьке та повітронепроникне, що забезпечує легке очищення від забруднення.

Висота робочої поверхні столу, за відсутності можливості її регулювання повинна складати 725 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною – не менше 500 мм, не менше 450 мм в глибину на рівні колін і на рівні простягнутої ноги – не менше 650 мм. Робоче місце має бути обладнане підставкою для ніг, має ширину не менше 300 мм, глибину не менше 400 мм, регулювання по висоті в межах 150 мм за кутом нахилу опорної поверхні підставки до 20 градусів.

Відстань від очей користувача до екрану дисплея має становити 500-700 мм. Кут зору 10-20°, але не більше 40°; кут між верхнім краєм дисплея і рівнем очей користувача має становити не менше 10°. Кращим є розташування екрану перпендикулярно до лінії зору користувача.

Робочі місця по відношенню до світлових прорізів повинні розташовуватися не ближче 3 м так, щоб природне світло падало збоку, переважно зліва. Освітленість також впливає на стан здоров'я і працездатність

людини. У відповідності зі СНіП 11-4-79 ВСТАНОВЛЕНІ НАСТУПНІ ВИМОГИ ДО ОСВІТЛЕНОСТІ**:**

ДЛЯ ШТУЧНОГО ОСВІТЛЕННЯ**:**

- Комбіноване освітлення – освітленість 1500 лк;
- Загальне освітлення – освітленість 400 лк.

ДЛЯ ПРИРОДНОГО ОСВІТЛЕННЯ**:**

- Верхнє або комбіноване освітлення – коефіцієнт природної освітленості (далі КПО) 10%;
- Бічне освітлення – КПО 3.5%.

ДЛЯ СУМІЩЕНОГО ОСВІТЛЕННЯ**:**

- Верхнє або комбіноване освітлення – КПО 3-6%;
- Бічне освітлення – КПО 1.1-2%.

До основних показників, що визначають умови здорової роботи, належать: фон, контраст об'єкта з фоном, видимість, показник осліпленості, коефіцієнт пульсації освітленості.

Фон характеризується коефіцієнтом відбиття. Контраст об'єкта з фоном (К) характеризується співвідношенням яскравості розглянутого об'єкта (точки, лінії, знаки) і фону. Оскільки роботи користувача ПЕОМ відносяться до категорії 1а – легкі фізичні роботи (роботи проводяться сидячи і супроводжуються незначним фізичним напруженням, з енерговитратами до 120 ккал / годину), необхідно дотримуватися наступних норм: коефіцієнт відображення більше 0,4, тобто світлий фон; контраст об'єкта з фоном великий і середній при К більше 0,2 (згідно СНіП 11-4-79).

У полі зору користувача ПЕОМ має бути забезпечений відповідний розподіл яскравості. Відношення яскравості екрана до яскравості оточуючих його поверхонь не повинно перевищувати у робочій зоні 3:1 (СНіП 11-4-79). У зв'язку з цим дисплей ПЕОМ повинен відповідати наступним вимогам:

- Яскравість свічення екрану не менше 100 кд/м;
- Мінімальний розмір світної точки для кольорового дисплея не більше 0,6 мм ;

- Контрастність зображення знаку – не менше 0,8;
- Низькочастотне тремтіння зображення в діапазоні 0,05-1,0 Гц повинно знаходитися в межах 0,1 мм;
- Екран повинен мати покриття антивідблиску;
- Відеомонітор повинен бути обладнаний поворотним майданчиком, що дозволяє переміщати відеотермінал в горизонтальній і вертикальній площинах в межах 130-220 мм і змінювати кут нахилу на 10-15 мм.

Коефіцієнт відбиття світла матеріалами і обладнанням всередині приміщень має велике значення для освітлення: чим більше світла відбивається від поверхонь, тим вище освітленість. Коефіцієнт відображення відповідно повинен бути для: стелі 60-70%, стін 40-50%, підлоги 30%, для інших поверхонь 30-40%.

Результати досліджень показують, що найбільшою мірою негативний фізіологічний вплив на операторів ПК пов'язаний з дискомфортними зоровими умовами через неправильно спроектоване освітлення. Згідно СНіП II-4-79 освітленість на горизонтальній площині робочого місця оператора ЕОМ повинна складати 400 лк при висоті цій площині 0,8 м над підлогою.

4.2 Забезпечення захисту працівників суб’єкта господарювання від іонізуючих випромінювань

Іонізуюче випромінювання або радіоактивність є небезпечним явищем для людського організму. При взаємодії впливу іонізаційних випромінювань у навколишнє середовище можуть відбутись різні утворення зарядів . Існують два різновиди випромінювання – «альфа» та «бета».

В залежності від носія та енергії, вони мають різну проникаючу здатність. Альфа це випромінювання яке проявляється важкими частинами складеними з протонів і нейтронів.

В свою чергу бета випромінювання являє собою ланцюг електронів та позитронів які є більшу здатність проникати у середовище. Працюючи на таких територіях, де існує радіаційна атмосфера можуть виникнути різні випадки.

На підприємстві можуть виникнути інциденти при користуванні ядерними матеріалами , зберіганні радіоактивних відходів в наслідок чого працівники можуть отримати травму у вигляді дози опромінення, використання іонізуючих джерел випромінювання.

Також у випадку такої радіаційної аварії забруднюється навколишнє середовище, люди можуть отримати травму у вигляді потужної дози опромінення. Призвести аварію на підприємстві може також якщо активна реакційна речовина знаходиться у роботі та це відбувається незаконно.

Це може привезти до опромінення жителів та перевищити межу дози опромінення. Частинки з цього випромінювання можуть залишати сліди на дихальній системі на травній системі людського організму. Також ці елементи можуть бути у водних каналах, які постачають питну воду людям.

На підприємстві де проводяться роботи з радіаційними речовинами обов’язково мають вживатись заходи проти радіації. Протирадіаційні захисти це така система правових, організаційних норм та санітарної гігієни.

До переліку таких захистів можна включити медичні заходи для забезпечення радіаційної безпеки персоналу та проектно-конструкторські. Для організації заходів проти іонізації опромінювання підприємство має ввести обов’язкові методи щоб подбати про безпеку працюючого персоналу. До таких методів можуть належати заходи які обмежують допуск працівників до джерел які випромінюють радіацію.

До таких працівників можемо віднести таких, які не підходять за віком, за статтю та працівники які вже отримали дозу випромінення. Підприємство мусить створити сприятливі умови що дотримуються встановлених норм та вимог для працівників та застосовувати індивідуальні засоби для захисту працівника цього підприємства.

Організація повинна контролювати рівні опромінювання та вести інформаційну систему про стан радіації на підприємстві та призначених місць для праці.

На підприємстві повинні бути проведені заходи щодо організації безпеки для робіт які проводяться у радіаційних ділянках а саме: -організація роботи нарядів та розпоряджень; -організація та перевірка пропусків до робочих місць; -оформлення контролю за процесом виконання роботи; -введення примусового часу на перерву та вчасне закінчення робочого процесу.

Реалізувати заходи проти радіації за певний відрізок часу можливо, тим що працівники , які працюють з іонізованими випромінюваннями можуть виконувати вчасно свою роботу ,відповідно керівництво може за якісну роботу зменшити кількість робочих днів у тижні.

Цим самим вони застереженням вони зменшать знаходження працівників у зоні випромінювання та відповідно буде менше контактування з радіаційними приладами. Захистити працівників за допомогою відстані підприємство може шляхом доцільного розміщення приміщення, правильно розставити та розрахувати робочі місця для працівників а також забезпечити приладами, які зможуть контактувати, керувати робочим процесом з технікою яка має радіаційний вплив на відстані.

Слугувати захистом може покриття свинцем меблів які присутні у приміщенні (двері, вікна, робочі столи), створення перекриття між поверхами та перегородки. Працівникам обов’язково має бути виданий спеціальний одяг ,такі як фартухи, шапочки та рукавиці зшиті з просвинцевої тканини.

Розміщення робочих місць повинно мати правильний розрахунок на загальну кімнату, не робити перенабір та забезпечити відповідним та необхідним обладнанням робочі кабінети. При користуванні відкритими приладами іонізованого опромінення провести герметизації цих систем, при можливості використовувати роботу техніки. Підприємство повинне вжити усіх санітарно-гігієнічних заходів та соціальних, а також важливо необхідний є медичний захист робочих на об’єкті.

4.3 Висновок до четвертого розділу

В даному розділі описано основні принципи конструювання робочого місця користувача ЕОМ, зазначено діючі вимоги щодо ергономіки робочого місця. А також визначені заходи та методи із забезпечення радіаційних впливів та іонізації опромінювання на підприємствах. Описані вимоги для керівництва та підлеглих працюючих на об’єктах щодо їхніх дій в разі виникнення радіації .

ВИСНОВКИ

Безпровідна локальна мережа (англ. WLAN) - це мережа в якій передача даних здійснюється через радіоефір; об'єднання пристроїв у мережу відбувається без використання кабельних з'єднань. Найбільш поширеними на сьогоднішній день способами побудови є Wi-Fi мережі.

Wi-Fi являє собою еквівалент звичайній, з’єднаний витими парами, локальній мережі, але вже в безпровідному варіанті, за допомогою передачі інформації високочастотними радіохвилями.

Основними перевагами використання безпровідних мереж є:

- Дозволяє розвернути мережу без прокладки кабеля, що може зменшити вартість розгортання і/або розширення мережі. Місця, де не можна прокласти кабель, наприклад, поза приміщеннями і в будівлях, що мають історичну цінність, можуть обслуговуватися безпровідними мережами.
- Дозволяє мати доступ до мережі мобільним пристроям.
- Випромінювання від безпровідникових пристроїв у момент передачі даних на два порядки (у 100 разів) менше, ніж біля стільникового телефону.

Основними недоліками безпровідних мереж є:

- Частотний діапазон і експлуатаційні обмеження в різних країнах неоднакові. У багатьох європейських країнах дозволено два додаткові канали які заборонені в США; У Японії є ще один канал у верхній частці діапазону, а інші країни, наприклад Іспанія, забороняють використання низькочастотних каналів. Більш того, деякі країни, наприклад в Італії, вимагають реєстрації всіх мереж Wi-fi приміщень, що працюють зовні, або вимагають реєстрації Wi-fi-оператора.
- Найпопулярніший стандарт шифрування WEP може бути відносно легко взломаний навіть при правильній конфігурації (із-за слабкої стійкості алгоритму). Не дивлячись на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і Wpa2, багато старих точок доступу не

підтримують його і вимагають заміни. Ухвалення стандарту IEEE 802.11i (Wpa2) зробило доступною безпечнішу схему, яка доступна в новому устаткуванні. Обидві схеми вимагають стійкіший пароль, ніж ті, які зазвичай призначаються користувачами. Багато організацій використовують додаткове шифрування (наприклад VPN) для захисту від вторгнення.

У роботі проведено аналіз відомих програмно-технічних засобів для оцінки продуктивності локальних безпровідних мереж, встановлено і основні переваги та недоліки. Проаналізовано аналітичні методи оцінки ефективності безпровідних локальних мереж.

У даному кваліфікаційному дослідженні проведена оцінка продуктивності безпровідникової локальної мережі з протоколом IEEE 802.11 при довільному навантаженні. Для цього розроблена і застосована модель маркова з дискретним часом, що описує поведінку станції мережі. На відміну від відомих рішень, модель враховує такі особливості протоколу, які у режимі нормального навантаження, як 1) перехід в стан відстрочки після будь-якої передачі пакета і 2) можливість негайної, асинхронної передачі пакету, який прийшов в порожню чергу. Показано, що модель застосовна для оцінки різних показників продуктивності (середній час обслуговування пакету, середній час його затримки на MAC-рівні і ймовірність відмови), а також для порівняльного аналізу ефективності і оптимізації механізмів передачі пакетів.

Розроболено Java аплет, який дозволяє моделювати роботу безпровідної локальної мережі з метою оцінки її ефективності. Даний додаток забезпечує можливість отримання даних для їх подальшої модельної обробки, а також дозволяє застосовувати перевірку адекватності

ПЕРЕЛІК ДЖЕРЕЛ

1. Буров Є.В. Комп’ютерні мережі: Підручник. – Львів: Магнолія, 2007. – 261 с.

2. Вишняков В.М. Принципи побудови комп’ютерних мереж. Навчальний посібник. – К.: КНУБА, 2022. – 128 с

3. Жураковський Б.Ю., Зенів І.О. Комп'ютерні мережі Частина 1: Навчальний посібник [Електронний ресурс] – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

4. Комп'ютерні мережі. Підручник у двох томах / Касаткін Д.Ю., Блозва А.І., Матус Ю.В. // НУБіП України, - Київ, Видавничий центр Компрінт. –2019., том 1 - 452 с., том 2 - 387 с.

5. Комп’ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] — Вінниця : ВНТУ, 2013. — 371 с. ISBN 978-966-641-543- 4.

6. Комп’ютерні мережі. Загальні принципи функціонування комп’ютерних мереж. Навчальний посібник. С. В. Мінухін, С. В. Кавун, С. В. Знахур. – Харків: Вид. ХНЕУ, 2008.

7. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.

8. Комп’ютерна схемотехніка та логіка. [навчальний посібник] / Гусєв Б.С., Касаткін Д.Ю., Матус Ю.В, Смолій В.В // НУБіП України, - Київ, Видавничий центр Компрінт. 2017, - 348 с.

9. Комп’ютерна схемотехніка та логіка. навчальний посібник (частина 2) / Лапко В.В., Лахно В.А., Гусєв Б.С., Касаткін Д.Ю., Сагун А.В., Іваник Ю.Ю. // - Київ, НУБіП України, Видавничий центр Компрінт. 2020, - 291 с.

10. Жабін В.І., Жуков І.А., Клименко І.А., Ткаченко В.В. Прикладна теорія цифрових автоматів. Навчальний посібник. Київ, Національний авіаційний університет, 2007р., 363с.

11. Комп’ютерна схемотехніка. Частина 1 [навчальний посібник] / Б.С. Гусєв, Д.Ю. Касаткін, Т.Ю.Осипова // - К.: НУБіП України, 2022.- 265с.

12. Комп’ютерна схемотехніка та логіка. Частина 2 [навчальний посібник] / Лапко В.В., Лахно В.А., Гусєв Б.С., Касаткін Д.Ю., Сагун А.В., Іваник Ю.Ю. // - Київ, НУБіП України, Видавничий центр Компрінт. 2020, - 291 с.

13. Комп’ютерна схемотехніка та логіка. [навчальний посібник] / Гусєв Б.С., Касаткін Д.Ю., Матус Ю.В, Смолій В.В // НУБіП України, - Київ, Видавничий центр Компрінт. 2017, - 348 с

14. Бабич М. П., Жуков І.А. Комп’ютерна схемотехніка: Навчальний посібник. – К.: МК – Прес, 2004. - 576с.

15. Робототехнічні комп'ютерні системи. навчальний посібник / В.А.Лахно, А.І.Блозва, Д.Ю.Касаткін // НУБіП України, - Київ, Видавничий центр Компринт 2021, 24 уда.

16. Спеціалізовані комп'ютери. навчальний посібник / А.В.Сагун, В.А.Лахно, В.Б.Бобков, Д.Ю.Касаткін, В.В.Хайдуров // НУБіП України, - Київ, Видавничий центр Компринт 2021, 24 уда.Computer architecture. A Quantitative approache. 5-th edn. http://elearn.nubip.edu.ua/mod/resource/view.php?id=134671 Principels of computer architecture http://elearn.nubip.edu.ua/mod/resource/view.php?id=134672

17. Організаційне забезпечення захисту інформації: Навчальний посібник Лахно В.А., Мамченко С.М.., Касаткін Д.Ю., Шкарупило В.В. // - К.: НУБіП України, 2022. – 432 с.

18. Technical means of information protection [навчальний посібник англ.мовою “Технічні засоби захисту інформації”] / В.А. Лахно, Мамченко С.В., Д.Ю. Касаткін, О.М. Дубовик // - Київ:ВЦ «Компрінт», 2022. – 388 с.

19. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно – телекомунікаційних системах: Навчальний посібник Харків ХНУРЕ, 2014 р. – 368 с.

20. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. (https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf)

21. Основи інформаційної безпеки. Підручник / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. –255 с.

22. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.) (http://kist.ntu.edu.ua/textPhD/tzi.pdf)

23. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Вид. група BUV, 2009. – 608 с.

24. . Конспект лекцій з дисципліни «Програмування для мобільних пристроїв» для студентів денної форми навчання спеціальності 126 «Інформаційні системи та технології» / Укладачі: Готович В.А., Михайлович Т.В. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2020. – 216 с.

25. Коноваленко І. В. Платформа .NET та мова програмування C# 8.0 : навчальний посібник / І. В. Коноваленко, П. О. Марущак. – Тернопіль : ФОП Паляниця В. А., 2020. – 320 с.

26. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.

27. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж. Навчальний посібник. Київ. ун-т ім. Б. Грінченка, 2011. 291 с.

28. Болілий В.О., Котяк В.В. Комп'ютерні мережі : навчальний посібник Кіровоград : ПП «Центр оперативної поліграфії «Авангард», 2008. 144 с.

29. Комп’ютерні мережі: навчальний посібник / Азаров О.Д., Захарченко С.М., Кадук О. В. та ін. Вінниця : ВНТУ, 2013. 371 с.

30. Кулаков Ю.О., Луцький Г.М. Комп’ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. Київ : Видавництво „Юніор”, 2005. 400 с.

31. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі [навчальний посібник]. Львів, «Магнолія 2006», 2013. 256с.

32. Олещенко Л.М. Організація комп’ютерних мереж: конспект лекцій: КПІ ім. І. Сікорського. Київ : КПІ ім. І. Сікорського, 2018. 225 с.

33. Коноваленко І.В., Федорів П.С. Системне програмування у Windows з прикладами на Delphi. Навч. посіб. Для тех. спец. Вищих навчальних закладів. Тернопіль: ТНТУ ім. І. Пулюя, 2012. 320 с.

34. Операційні системи : навчальний посібник. [за ред. В. М. Рудницького] / І.М.Федотова-Півень, І.В.Миронець, О.Б.Півень, С.В. Сисоєнко, Т. В. Миронюк; Черкаський державний технологічний університет. Харків : ТОВ «ДІСА ПЛЮС», 2019. 216 с.

35. Погребняк Б.І., Булаєнко М.В. Операційні системи : навч. посібник; Харків. нац. ун-т міськ. госп-ва ім. О.М.Бекетова. Харків: ХНУМГ ім. О.М.Бекетова, 2018. 104с

36. Рисований О.М. Системне програмування : підручник для студентів напрямку “Компютерна інженерія” вищих навчальних закладів в 2-х томах. Том 1. Видання четверте: виправлено та доповнено. Харків : “Слово”, 2015. 576 с.

37. Системне програмування. Системні сервісні компоненти. Навч. посібник / Дерев’янко О.С., Межерицький С.Г., Гавриленко С.Ю., Клименко А. М. Харків: НТУ «ХПІ», 2009. 160 с.

38. Харченко В.П., Знаковська Є.А., Бородін В.А. Операційні системи та системи програмування: навч. посіб. Киіів: Вид-во Нац. авіац. ун-ту «НАУдрук», 2012. 360с. 41. Шеховцов В.А. Операційні системи: Підручник. Київ: Вид. група BNV, 2005. 576 с.

39. Nixon R. Learning PHP, MySQL & JavaScript. With jQuery, CSS & HTML5. O'Reilly, 2014. 1032 c.

40. Purewal S. Learning Web App Development. O'Reilly, 2014. 401 c.

41. Welling L., Thomson L. PHP and MySQL Web Development. AddisonWesley, 2017. 768c.

42. Осадчий В.В. Основи розробки веб-додатків. Навчальний посібник / В.В. Осадчий, В.С. Круглик – Мелітополь: ТОВ «Видавничий будинок ММД», 2012. – 540 с.

43. Пасічник О.Г., Пасічник О.В., Стеценко І.В. Основи веб-дизайну. [Навч. посіб.]. К.: Вид. група BHV. 2009. 336 с.

44. Peltier, T. R. Information security risk analysis, Third Edition. / T. R. Peltier. – CRC Press, 2020. 456 p.

45. Olsson, T. Assessing security risk to a network using a statistical model ofattacker community competence / T. Olsson // Proceedings of the 11th internationalconference on Information and Communications Security. – 2019. – P. 308–324.

46. Peltier, T. R. Information security risk analysis, Third Edition. / T. R. Peltier. –CRC Press, 2020. 456 p.

47. Poolsappasit, N. Dynamic security risk management using Bayesian attackgraphs / N. Poolsappasit, R. Dewri, I. Ray // IEEE Transactions on Dependable andSecurity Computing. – 2012. – Vol.9, No.1 – P. 61–74.

48. Toth, T. Evaluating the impact of automated intrusion response mechanisms / T. Toth, C. Kruegel // Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC). – 2020.– P. 301–310.

49. Gibellini, E.; Righetti, C. Unsupervised Learning for Detection of Leakage from the HFC Network. In Proceedings of the ITUKaleidoscope: Machine Learning for a 5G Future (ITU K), Santa Fe, Argentina, 26–28 November 2018; pp. 1–8. [CrossRef]

50. Baek, M.; Song, J.; Jung, J. Design and Performance Verification of Time-Domain Self-Interference Estimation Technique forDOCSIS 3.1 System with

Full Duplex. In Proceedings of the IEEE International Symposium on Broadband Multimedia Systemsand Broadcasting, Valencia, Spain, 6–8 June 2018; pp. 1–4. [CrossRef]

51. Петрик М.Р. Моделювання програмного забезпечення : науково методичний посібник / М.Р. Петрик, О.Ю. Петрик– Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2015. – 200 с.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професор.

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.
Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.
Науковий секретар: Семенишин Галина – старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.
Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; асистент Н. Шаблій; ст. викладач Л. Джиджора.

Матеріали XI науково-технічної конфції «Інформаційні моделі, системи та
М34 технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 13-14 грудня 2023 р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2023. – 257 с.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 254983.
E-mail: **conffis2023@gmail.com**

Редагування, оформлення, верстка: Семенишин Г.М.

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання;
- Інформаційні системи та технології;
- Комп'ютерні системи та мережі;
- Програмна інженерія та моделювання складних розподілених систем;
- Новітні фізико-технічні та освітні технології.

В збірнику надруковано тези доповідей XI науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 13-14 грудня 2023 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.031.6
Микола Лялик
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ АРХІТЕКТУРИ БЕЗПРОВІДНИХ ЛОКАЛЬНИХ МЕРЕЖ

Mykola Lyalik

ANALYSIS OF THE ARCHITECTURE OF WIRELESS LOCAL NETWORKS

Під час дослідження ефективності функціонування безпровідних локальних мереж необхідно детальніше зупинитися на компонентах їх архітектури.

Архітектура IEEE 802.11 містить окремі компоненти, які взаємодіють між собою, утворюючи безпровідну LAN, яка підтримує мобільність станцій (station – STA) прозоро щодо вищих рівнів. Основна архітектура, властивості та послуги 802.11b визначені оригінальним стандартом 802.11. Специфікації 802.11b впливають тільки на Фізичний рівень, додаючи вищі швидкості пересилання даних і більш стійке сполучення.

Базова система послуг (Basic Service Set - BSS) є основним блоком, з яких будується WLAN IEEE 802.11. На рисунку 1.1 показано дві BSS, кожна з яких містить по дві станції, які є членами BSS.

Доцільно вважати, що внутрішні еліпси на рисунку 1 окреслюють області охоплення, всередині яких станції, які входять до даної BSS, можуть здійснювати комунікацію між собою. Якщо ж ці станції перемістяться поза свою BSS, то вони не зможуть безпосередньо комунікуватися з іншими членами BSS.

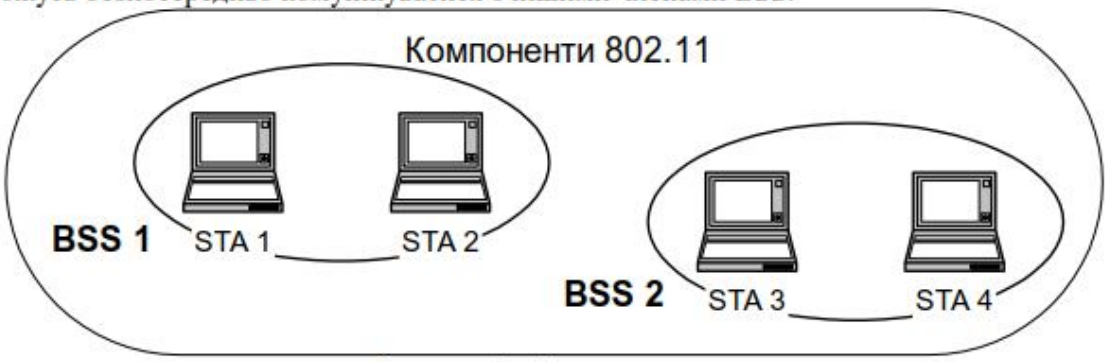

Рисунок 1 - Базова система послуг

Незалежна базова система послуг (Independent BSS – IBBS) є найбільш основним типом LAN стандарту IEEE 802.11. Найменша така LAN може складатися з тільки двох станцій. На рис. кожна з BSS 1 та BSS 2 – це IBSS. Цей режим можливий, коли станції здатні комунікуватися між собою безпосередньо. Оскільки такий тип мережі часто формується без попереднього планування, його називають одноразовою (ad hoc) мережею.

Пов'язання між станцією та BSS динамічне – станція може вмикатися, вимикатися, залишати межі області охоплення і повертатися в неї. Щоб стати членом інфраструктури BSS, станція мусить стати "асоційованою". Ця асоціація динамічна і включає використання послуг розподільчої системи (Distribution System Service – DSS), описаної нижче.

Концепція розподільчої системи полягає в наступному. Обмеження Фізичного рівня (PHY) визначають максимальну відстань між станціями, яка ще може обслуговуватися. Для певних мереж ця відстань достатня, для інших вона повинна бути збільшена. Тоді, замість незалежного існування, BSS може виступати як компонента розширеної форми мережі, побудованої з багатьох BSS. Архітектурна компонента, яка

вживається для взаємосполучення багатьох BSS, називається розподільчою системою (Distribution System - DS).

Стандарт IEEE 802.11 логічно відділяє безпровідне середовище (Wireless Medium - WM) від середовища розподільчої системи (Distribution SystemMedium - DSM). Кожне логічне середовище вживається для різних завдань, з різними компонентами архітектури мережі. Логічні середовища можуть бути фізично однаковими або різними. Розуміння того, що різні середовища логічно відмінні є ключовим лоя розуміння гнучкості архітектури. Архітектура LAN IEEE 802.11 визначена незалежно від фізичних характеристик будь-якого конкретного впровадження. Розподільча система уможливлює підтримку мобільних пристроїв, забезпечуючи логічні послуги, необхідні для обслуговування відображення адрес на призначення і, тим самим, об'єднання багатьох BSS.

Крім станції, IEEE 802.11 визначає пункт доступу (Access Point – AP), який діє як міст між безпровідною мережею та розподільчою системою. Пункт доступу – це станція, яка забезпечує доступ до DS, надаючи послуги розподільчої системи додатково до своїх дій як станції. Пункт доступу звичайно складається із радіо, кабельного мережевого інтерфейсу (наприклад, для 802.3) і програмного забезпечення для бріджінгу (операцій мостів), сумісного із стандартом 802.1 для бріджінгу. Пункт доступу діє як базова станція для безпровідної мережі, агрегуючи доступ до кабельної мережі для багатьох безпровідних станцій. Кінцевими станціями 802.11, наприклад, можуть бути карти мережевого інтерфейсу IEEE 802.11, або телефонні апарати, базовані на 802.11. На рисунку 1.2 показані компоненти архітектури IEEE 802.11, які включають пункти доступу (AP) та розподільчу систему (DS).

Дані переміщаються між BSS і DS через пункти доступу. Пункти доступу мають власні адреси (як станції); адреси, які використовуються AP для комунікації через безпровідне середовище (WM) і через середовище розподільчої системи (DSM), не обов'язково ті самі.

Розподільчі системи і базові системи послуг дозволяють створювати безпровідні мережі довільного розміру і складності. Стандарт IEEE 802.11 називає такий тип мережі розширеною системою послуг (Extended Service Set – ESS). Ключова концепція полягає у тому, що мережа ESS виглядає на підрівні LLC так само, як IBSS.