Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УУРЕ ФРЕТ
(повне найменування інституту, назва факультету)
Радіотехніки та телекомунікацій
(повна назва кафедри)

Пояснювальна записка

до магістерської роботи
магістр
(рівень вищої освіти (освітньо-кваліфікаційний рівень))

на тему Моделювання протоколів множинного доступу в безпроводових мережах

Виконав: студент VI курсу, групи РТ-912м
спеціальності (напряму підготовки)
172 Телекомунікації та радіотехніка
(код і назва напряму підготовки, спеціальності)
Спец. Інформаційні мережі зв'язку
Ковальчук М.К.
(прізвище та ініціали)
Керівник Кабак В.С.
(прізвище та ініціали)
Рецензент Тюхфєв О.С.
(прізвище та ініціали)

м. Запоріжжя
2017 рік

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Запорізький національний технічний університет

(повне найменування вищого навчального закладу)

Інститут, факультет ІУРЕ ФРЕТ

Кафедра Радіотехніки та телекомунікацій

Рівень вищої освіти (освітньо-кваліфікаційний рівень) магістр

Спеціальність 172 „Телекомунікації та радіотехніка"

(код і назва)

Напрям підготовки Спец. Інформаційні мережі зв'язку

(код і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри К.Т.Н. доц.

Мірошавка С.В.

"__" _____ 20__ року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Ковальчук Марії Костянтинівні

(прізвище, ім'я, по батькові)

1. Тема роботи Моделювання протоколів множинного доступу в бездротових мережах

керівник роботи К.Т.Н. доц. Кабак Владислав Семенович,

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

затверджені наказом вищого навчального закладу від "27" жовтня 2017 року № 426

2. Строк подання студентом роботи 15.12.2017р.

3. Вихідні дані до роботи $M_{терм}$ - кількість терміналів = 100; S_{rate} = 256 символ/секунду символьна швидкість; R = 100 м - радіус зони обслуговування; $B_{ТД}$ = 5 м - висота розташування точки доступу; $P_{сп}$ = 128 символів - довжина пакету; $A_{ФД}$ = 3 - коефіцієнт затухання; $Sigma_{ФД}$ = 6 дБ - стандартна девіація для логарифмічно нормального закону; $T_{сп}$ = 10 дБ - коефіцієнт захоплення.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз методів доступу, принципи роботи конкурентних методів доступу, створення моделі роботи з пакетною передачею даних, моделювання алгоритмів роботи ALOHA, S-ALOHA, NP-CSMA, I-CSMA.

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

Презентація Power Point, 32 слайди

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	Прийняв виконане завдання
1, 2	к.т.н., доц. Кабак В.С.		
Економ. ОПУВ	асист. Крупікова В.В		
Охорона праці	ст. викл. Коробко О.В.		
Нормоконтроль	ст. викл. Лоханова Л.М.		

7. Дата видачі завдання 1 вересня 2017 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури	1 тиждень	
2	Аналіз методів доступу	1 тиждень	
3	Аналіз принципів роботи конкурентного методу доступу	1 тиждень	
4	Створення моделі роботи з пакетного передачею даних	3 тижні	
5	Моделювання алгоритмів роботи ALOHA, S-ALOHA, NP-CSMA і ISMA	2 тижні	
6	Економічні розрахунки	1 тиждень	
7	Охорона праці та безпека у надзвичайних ситуаціях	1 тиждень	
8	Оформлення ПЗ	1 тиждень	
9	Підготовка презентації	1 тиждень	

Студент _____ (підпис) Ковальчук М.К. (прізвище та ініціали)

Керівник роботи _____ (підпис) Кабак В.С. (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 162 сторінки, 59 рисунки, 15 таблиць, 9 джерел

Об’єкт дослідження – безпровідна мережа.

Мета роботи – дослідження алгоритмів роботи протоколів множинного доступу.

Метод дослідження – математичний та експериментальний.

Задачею роботи було визначення показників ефективності протоколів конкурентного доступу для моделі системи передачі інформації з пакетною передачею даних.

В першому розділі наведена загальна інформація про протоколи множинного доступу, їх класифікація та характеристика. В другому розділі показані принципи роботи протоколів та описується експериментальна частина з моделюванням протоколів множинного доступу, визначення їх пропускної здатності і затримки передачі з метою порівняння різних протоколів доступу до каналу. Третій розділ дає економічну оцінку виконаної роботи. Четверта частина магістерської роботи присвячена охороні праці та безпеці життєдіяльності.

БЕЗПРОВІДНА МЕРЕЖА, МНОЖИННИЙ ДОСТУП, ПРОТОКОЛ, КОЛІЗІЯ, КОНКУРЕНТНІСТЬ, ТРАФІК, ПРОПУСКНА ЗДАТНІСТЬ, ЕФЕКТ ЗАХОПЛЕННЯ, СЛОТ, ТЕРМІНАЛ, КОРИСТУВАЧ

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ……8
ВСТУП……9
1 ПРОТОКОЛИ МНОЖИННОГО ДОСТУПУ……..12
1.1 Класифікація протоколів множинного доступу……12
1.2 Безконкурентні протоколи множинного доступу…….14
1.3 Протоколи з конкурентним доступом……16
1.3.1 Протоколи випадкового доступу з повторенням……..17
1.3.1.1 Протокол випадкового доступу ALOHA……17
1.3.1.2 Статистика отриманих повідомлень……18
1.3.2 ALOHA з виділенням часових інтервалів (S–ALOHA)……..22
1.3.3 Протокол множинного доступу з детектуванням несучої CSMA……...25
1.3.3.1 Протокол множинного доступу CSMA/CD……26
1.3.3.2 Протокол множинного доступу CSMA/CA……31
1.3.3.3 Централізований режим доступу PCF……41
1.4 Протокол доступу з цифровим детектуванням DSMA…….43
1.5 Методи випадкового доступу з резервуванням……43
1.5.1 Алгоритм ALOHA з використанням резервування……43
1.5.2 Порівняння продуктивності протоколів S-ALOHA і R-ALOHA……..46
1.5.3 Схема з резервуванням пакетів PRMA……49
2 МОДЕЛЮВАННЯ ПРОТОКОЛІВ МНОЖИННОГО ДОСТУПУ……51
2.1 Обґрунтування базового алгоритму програмного комплексу……..51
2.1.1 Канал зв’язку……...…52
2.1.2 Генерація пакетів…….54
2.1.3 Колізія……...54
2.1.4 Трафік……....55
2.1.5 Пропускна здатність……...56
2.1.6 Середній час затримки передачі……...56

2.1.7 Оцінка якості протоколів доступу……57
2.2 Базовий алгоритм програмного комплексу……...58
2.3 Опис головної програми……...60
2.4 Опис підпрограм, які необхідні для функціонування головної програми……73
2.4.1. Підпрограма розташування терміналів користувачів……..73
2.4.2 Підпрограма розрахунку відстані між точкою доступу і терміналом користувача……..74
2.4.3 Підпрограма виводу результатів теоретичного аналізу……..74
2.4.4 Підпрограма виводу результатів моделювання…….75
2.5 Моделювання чистої схеми ALOHA……75
2.5.1 Підпрограма моделювання протоколу ALOHA…..……77
2.5.2 Результати моделювання……..81
2.6 Моделювання протоколу ALOHA з виділенням часових інтервалів……..85
2.6.1 Підпрограма моделювання протоколу S–ALOHA……87
2.7 Протокол множинного доступу з детектуванням несучої CSMA……91
2.7.1 Підпрограма моделювання методу CSMA……..94
2.7.2 Результати моделювання для схеми CSMA……95
2.8 Протокол методу множинного доступу ISMA……102
2.8.1 Підпрограма моделювання протоколу ISMA……106
2.8.2 Результати моделювання……....106
3 ЕКОНОМІЧНІ РОЗРАХУНКИ……...112
3.1 Тенденції розвитку ринку бездротового зв’язку……..…..112
3.2 Визначення трудомісткості та тривалості роботи……115
3.3 Розрахунок кошторису витрат на практичну реалізацію магістерської роботи……118

3.3.1 Розрахунок вартості матеріалів…….119

3.3.2 Спеціальне устаткування…….120

3.3.3 Розрахунок заробітної плати……..120

3.3.4 Відрахування на соціальне страхування……121

3.3.5 Накладні витрати…….122

3.3.6 Бальна оцінка економічної ефективності проекту……...122

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ…125

4.1 Аналіз потенційних небезпек……125

4.2 Заходи по забезпеченню техніки безпеки……127

4.3 Заходи по забезпеченню виробничої санітарії та гігієни праці…129

4.4 Заходи з пожежної безпеки…….139

4.5 Заходи безпеки у надзвичайних ситуаціях……..140

ПЕРЕЛІК ПОСИЛАНЬ……...145

Додаток А……146

Додаток Б……...154

Додаток В…….156

Додаток Г…….158

Додаток Д…….160

ПЕРЕЛІК СКОРОЧЕНЬ

АС – Абонентська станція

БС – Базова станція

BSS – Basic Service Set

CA – Collision Avoidance

CD – Collision Detection

CSMA – Carrier Sense Multiple Access

DAMA – Demand Assigned Multiple Access

DSMA – Digital Sense Multiple Access

FDMA – Frequency Division Multiple Access

FIFO – First in – first out

ISMA – Inhibit Sense Multiple Access

TDMA – Time Division Multiple Access

RTS – Request to Send

ВСТУП

Однією з основних проблем побудови безпровідних мереж є вирішення задачі доступу багатьох користувачів до обмеженого ресурсу середовища передачі.

У телекомунікаційних системах для забезпечення паралельної передачі інформації багатьох користувачів в обох напрямках, необхідно встановити правила багатостанційного або множинного доступу до каналів зв'язку. Поняття множинного доступу (англійською multiple access) пов'язано саме з організацією сумісного використання обмеженого частотно-часового ресурсу багатьма користувачами. Це означає, що виділений радіочастотний спектр необхідно перерозподілити між рядом конкретних абонентів, але з накладанням певних обмежень на використання виділеного каналу за такими параметрами як простір, частота, час або код. Інколи, для такої визначеної процедури упорядкування частотно-часового ресурсу різних користувачів застосовують ще терміни ущільнення або мультиплексування.

У теперішній час загалі виділяють п'ять можливих варіантів множинного доступу [1, 2, 3]:

а) множинний доступ із частотним розділенням;

б) множинний доступ із часовим розділенням;

в) множинний доступ із кодовим розділенням;

г) множинний доступ із просторовим розділенням;

д) множинний доступ із поляризаційним розділенням.

Тобто, задача такого ущільнення або мультиплексування – це виділення кожному каналу простору, часу, частоти і/або коду з мінімумом взаємних завад і максимальним використанням характеристик середовища передачі. Наведені методи ущільнення практично представляють способи розділення єдиного ресурсу на канали передачі, але ці канали ще необхідно призначити конкретним пристроям.

Ця задача стає ще більш актуальною у безпровідних мережах, оскільки серед користувачів телекомунікаційної системи необхідно

досягнути певне погодження на використання каналу зв’язку, яке зазвичай трактують як протокол множинного доступу. Тобто, протокол множинного доступу визначається як погодження між користувачами з відповідним набором правил для успішної передачі інформації з використанням спільного виділеного ресурсу. За відсутністю такого протоколу виникає можливість конфлікту – коли декілька користувачів намагатимуться одночасно реалізувати доступ до виділеного ресурсу. Відповідно протокол множинного доступу повинен запобігти або розрішити такі конфлікти (колізії).

Проектування будь-якого конкретного протоколу, як правило, дуже пов’язано з кінцевою метою, що в свою чергу визначається середовищем передачі. Відповідно параметри і характеристики протоколу залежатимуть від кінцевої мети і призначення. Але, якщо визначити специфічні особливості середовища передачі, то можна визначити ряд характеристик, які повинен забезпечувати протокол множинного доступу [4]:

– перша і основна задача протоколів множинного доступу перерозподілити спільний канал передачі серед багатьох користувачів. Для вирішення цієї задачі протокол повинен керувати способом доступу конкретного користувача до каналу з дотриманням певних правил усіма користувачами мережі;

– протокол повинен реалізувати управління ємністю каналу із забезпеченням максимальної ефективності, зазвичай ознакою ефективності виступають пропускна здатність каналу і час затримки передачі;

– протокол повинен забезпечувати рівні права індивідуальним користувачам у наданні ємністю системи;

– протокол повинен бути достатньо гнучким з можливістю реалізації різних видів трафіку (мова, дані і т. ін.);

– протокол доступу повинен забезпечувати стійкий режим роботи системи зв’язку. Це означає, що якщо система знаходиться у стані рівноваги, то збільшення навантаження на систему переводить її у новий стан рівноваги без погіршення основних характеристик. Для нестійкого протоколу

збільшення навантаження призводить до перевантаження каналу з відповідним погіршенням пропускної здатності;

– протокол повинен бути достатньо робастним до похибок обладнання і зміни зовнішніх умов. Робастність також повинна проявлятися у нівелюванні некоректної роботи одного з користувачів на властивості системи.

В магістерській роботі основну увагу буде приділено безпровідним мережам, в яких принципово передбачається мобільність станцій. Для такого середовища протоколи повинні враховувати специфічні умови розповсюдження сигналу, зокрема, забезпечувати робастність щодо зміни характеристик каналу.

Можна виділити такі проблеми, які повинні вирішувати протоколи для безпровідних мобільних систем [2, 4, 5]:

– проблема схованих терміналів (два термінали не “бачать” одне одного через якісь перешкоди (пагорби, будівлі, або інші чинники), які перешкоджають розповсюдженню сигналу в діапазоні НВЧ, але обидва знаходяться у межах дії центральної або базової станції);

– ефект близько–далеко розташованих абонентів (затухання сигналу для далеко розташованих абонентів може мати суттєво більше значення);

– наслідки ефекту багатопроменевого розповсюдження радіохвиль і затінення;

– вплив внутрішньоканальних завад у стільникових мережах через роботу станції на одній і тій же частоті у сусідніх стільниках.

1 ПРОТОКОЛИ МНОЖИННОГО ДОСТУПУ

1.1 Класифікація протоколів множинного доступу

Починаючи з 1970 р., коли з’явився перший протокол множинного доступу ALOHA, була розроблена достатньо велика кількість протоколів. Відповідно було запропоновано декілька шляхів для класифікацій цих протоколів. Однією з найпоширеніших класифікацій є розбиття усіх протоколів на три класи:

– протоколи безконкурентного доступу;

– протоколи з конкурентним доступом;

– підклас протоколів CDMA.

Узагальнена класифікація протоколів множинного доступу наведена на рис.1.1 [4].

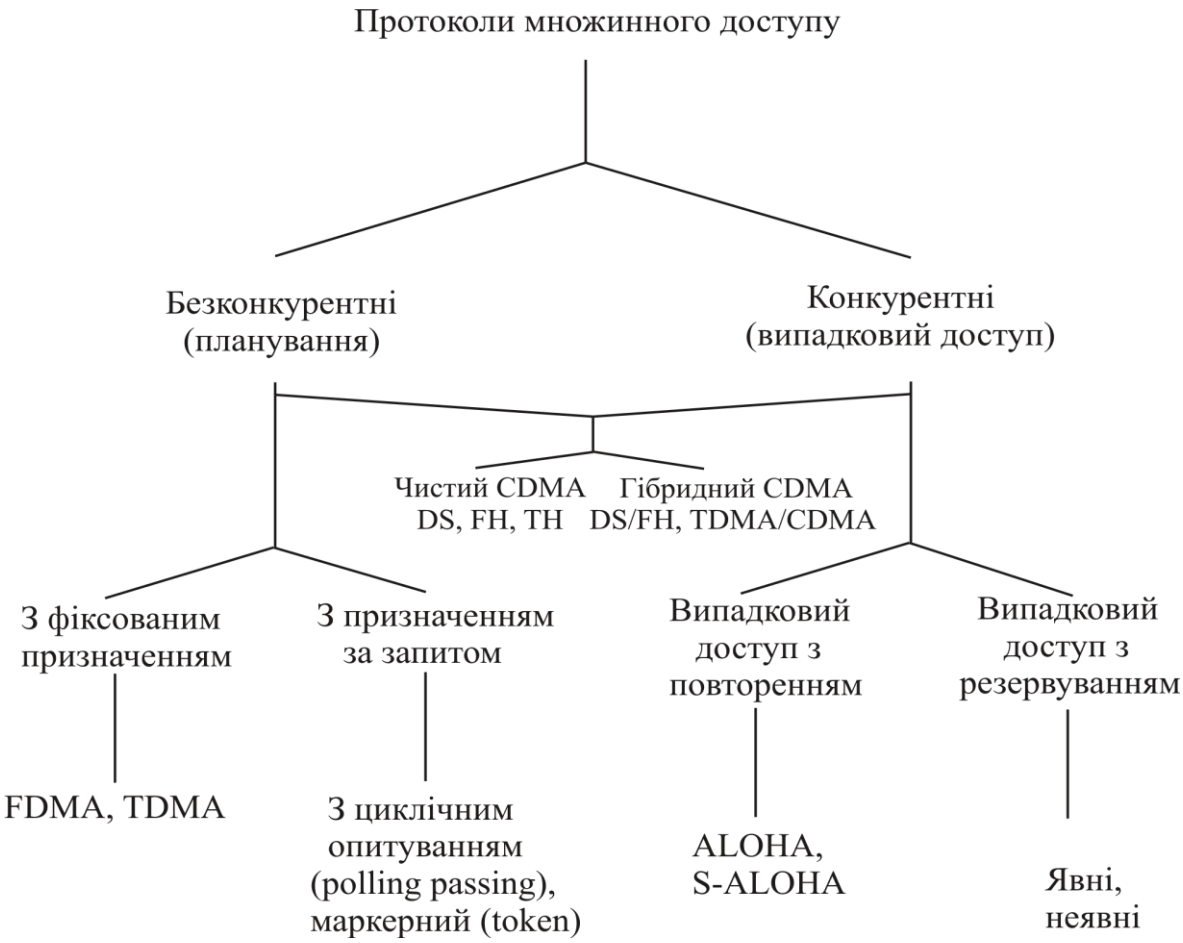

Рисунок 1.1 – Класифікація протоколів множинного доступу

Протоколи безконкурентного доступу уникають ситуацій, коли два або більше користувачів можуть отримати одночасний доступ до каналу зв’язку шляхом резервування інтервалів передачі для користувачів (протоколи без колізій). Це може бути реалізовано або фіксованим виділенням ємності каналу зв’язку, або наданням доступу до каналу за запитом, коли резервування здійснюється тільки між користувачами у яких з’явилася інформація для передачі.

Навпаки, протоколи конкурентного доступу не можуть гарантувати відсутність конфліктів, оскільки для цих протоколів можливий одночасний доступ до каналу і, відповідно, одночасна передача інформації декількома користувачами. Тому такі протоколи повинні мати властивості вирішувати такі конфлікти.

Підклас CDMA протоколів не можна віднести як ні до протоколів безконкурентного доступу, так і до протоколів конкурентного доступу. Цей підклас займає проміжне місце між цими протоколами. В принципі, застосування CDMA можна розглядати як протокол безконкурентного доступу, коли усі користувачі здійснюють передачу інформації без конфліктів. Але, коли кількість одночасно працюючих станції перевищить деякий поріг, то виникає певна конкурентність між користувачами.

Протоколи конкурентного доступу у свою чергу розділяються на два підкласи: повністю випадкові протоколи з повторним застосуванням і випадкові протоколи з резервуванням. Для другого підкласу початковий доступ до каналу здійснюється на підставі повністю випадкового протоколу, але у подальшому передача планується тільки для моментів, коли з’явиться наступна інформація для передачі. Виділяють два основних види таких протоколів – з явним резервуванням і з неявним резервуванням.

Явне резервування передбачає використання коротких пакетів резервування для запиту передачі у час, що планується. Протоколи з неявним резервування реалізуються без використання будь-яких пакетів резервування.

Підклас протоколів CDMA розділяють на протоколи чистого CDMA і гібридного CDMA.

1.2 Безконкурентні протоколи множинного доступу

Безконкурентні протоколи множинного доступу уникають ситуації для якої декілька користувачів можуть отримати одночасний доступ до виділеного каналу зв’язку шляхом планування (резервування) передачі для усіх користувачів. Таке планування передачі передбачає повну успішність передачі інформації.

Реалізація планування можлива у двох варіантах.

Найпростішим варіантом є планування з фіксованим призначенням ємності ресурсу. Для цього типу протоколів повний виділений ресурс системи зв’язку перерозподіляється між усіма користувачами з наданням кожному фіксованої частини ресурсу незалежно від активності користувача. Таке перерозподілення може проводитися або в часовій, або в частотній області.

Так, наприклад, для протоколу TDMA відбувається фіксований розподіл часових інтервалів між користувачами у межах кадру TDMA без перекриття їх у часі. Для протоколів FDMA відбувається перерозподіл усього виділеного частотного діапазону між користувачами без взаємного перекриття виділених частотних каналів і кожен з користувачів працює тільки у виділеному частотному підканалі [2, 6]. Графічна інтерпретація протоколів TDMA і FDMA представлена на рис.1.2.

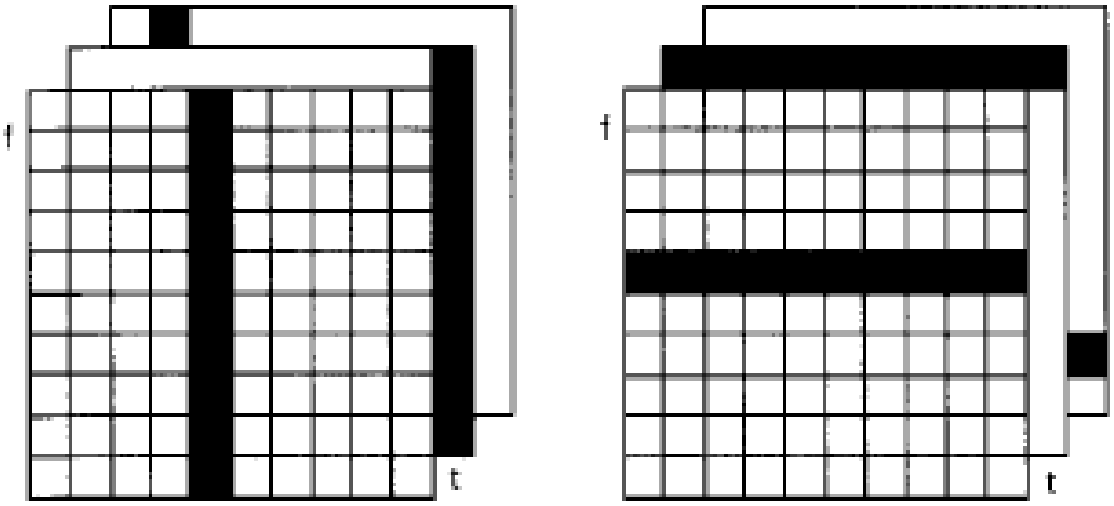

Рисунок 1.2 –Графічна інтерпретація протоколів TDMA і FDMA

Розподілом займається базова станція (центральний пристрій), яка повідомляє кожному абоненту про надання ємності каналу зв’язку (зокрема, час початку для протоколу TDMA або номер підканалу для протоколу FDMA). Подібна схема ідеально підходить для безпровідних мереж, які мають фіксовану пропускну здатність. Але у випадку нерегулярної передачі вона не може вважатися оптимальною, оскільки канал розглядається як зайнятий незалежно від того передається інформація конкретним користувачем чи він знаходиться у режимі мовчання. Відповідно або пустий часовий інтервал, або частотний підканал не можуть використовуватися іншими користувачами. Це означає, що для таких протоколів множинного доступу кількість абонентських станцій (або допустима пропускна здатність) принципово і суттєво обмежені.

Іншим варіантом безконкурентного доступу є протоколи з плануванням за запитом. На відміну від фіксованого планування ємність системи зв’язку надається конкретному користувачу, тільки коли у нього з’являється інформація для передачі. При цьому виділяють протоколи з централізованим управлінням і з розподіленим управлінням. При централізованому управлінні єдиний пристрій реалізує планування передачі. Прикладом такого протоколу є так званий протокол з циклічним

опитуванням (roll-call polling). При розподіленому управлінні усі користувачі залучені до процесу управління. Прикладом протоколу з розподіленим управлінням є протокол використанням маркера (token passing) [4].

1.3 Протоколи з конкурентним доступом

Для протоколів множинного доступу з конкурентним доступом ніякого планування передачі не планується. Це означає, що користувач готовий для передачі інформації не має ніякого уявлення в який момент часу він може здійснити передачу без завад від інших користувачів. Конкретний користувач в залежності від типу протоколу може як знати, так і не знати про зайнятість каналу на поточний момент часу (наприклад, прослуховуванням каналу). Але він принципово не має ніякого уявлення про готовність інших користувачів до передачі. Відповідно, якщо декілька користувачів почнуть передачу приблизно в один і той же момент часу, то усі передачі не дійдуть до адресатів через взаємні завади. В результаті процес успішної передачі за таких умов може вважатися наближенням до випадкового процесу, а задачею протоколу з випадковим доступом є вирішення цієї конкурентності серед багатьох користувачів.

Протоколи множинного доступу з конкурентним доступом розділяють на дві групи. По-перше, це протоколи випадкового доступу з повторенням. До цієї групи відносять класичний (чистий) протокол ALOHA, модифікація цього протоколу S-ALOHA (слотована ALOHA) протокол множинного доступу з детектуванням несучої CSMA (Carrier Sense Multiple Access) і протокол ISMA (DSMA).

До другої групи відносять протоколи випадкового доступу з резервуванням, найбільш відомі з яких це протокол R-ALOHA (ALOHA з резервуванням) і протокол множинного доступу з резервуванням пакетів PRMA (Packet Reservation Multiple Access) [2,3,4].

Для першої групи протоколів під час кожної передачі виникає ймовірність конкурентності. Для другої групи тільки під час першої передачі існує ймовірність конфліктів з іншими користувачами. Якщо ж перша передача закінчилася успішно, то усі наступні передачі для цього користувача відбуваються з плануванням, яке дозволяє для нього уникнути конфліктів (усувається конкурентність). Тобто, після успішної передачі частина ємності каналу надається даному користувачу і усі інші користувачі не можуть її використовувати. Доступ до каналу для цього користувача припиняється тільки після моменту часу, коли у нього стає відсутня інформація для передачі.

1.3.1 Протоколи випадкового доступу з повторенням

1.3.1.1 Протокол випадкового доступу ALOHA

Прикладом найпростішого протоколу з повністю випадковим доступом є класична схема ALOHA – один з перших протоколів доступу для систем безпровідного зв’язку, який розробив і почав використовувати у 1971 р. Гавайський університет. Під час передачі даних мобільним пристроєм за протоколом ALOHA не використовується будь-який механізм, який запобіг би виникненню колізій (одночасної роботи двох і більше передавачів одночасно на одній і тій же частоті). Це означає, що будь-який пристрій може передавати дані у будь-який час і не має ніякої гарантії, що дані будуть успішно доставлені одержувачу.

Для забезпечення зв’язку між декількома університетськими комп’ютерами застосовувався супутник з використанням такого протоколу довільного доступу. Принцип роботи системи надзвичайно простий і містить в собі такі режими [3].

1. Режим передачі. Користувачі передають дані у будь-який момент часу з використанням кодування з визначенням помилок.

2. Режим очікування. Після передачі повідомлення користувач очікує від адресату (приймача) підтвердження (acknolidgment - ACK) прийому даних. Очевидно, що цілком можлива ситуація, коли повідомлення різних користувачів передаються одночасно, що призводить до появи помилок у кожній передачі. У такому разі повідомлення різних користувачів називають конфліктуючими. Після визначення такої помилки користувач, що передавав повідомлення отримує негативне підтвердження прийому (negative acknowledgment - NAK).

3. Після отримання негативного повідомлення NAK інформація передається повторно. Очевидно, що якщо користувачі намагатимуться здійснити повторну передачу безпосередньо після виникнення помилки, то конфліктна ситуація має повторитися. Тому повторна передача відбувається після випадкової затримки.

4. Режим вичерпання часу очікування. Якщо після передачі повідомлення користувач впродовж визначеного інтервалу часу не отримав повідомлення ACK або NAK, то реалізується повторна передача повідомлення.

1.3.1.2 Статистика отриманих повідомлень

Припустимо, що для роботи деякої системи необхідна визначена середня частота успішного надходження повідомлень або пакетів λ. Через можливі конфліктні ситуації деякі з повідомлень не будуть отримані або будуть відхилені. Тоді загальну частоту надходження повідомлень λ_{tot} можна визначити як суму частоти успішного надходження λ і частоти відхилення даних λ_r:

$$\lambda_{tot} = \lambda + \lambda_r.$$

Позначимо розмір повідомлення або пакету через b біт. Тоді середній обсяг успішно переданих даних, або іншими словами, пропускну здатність каналу можна визначити як:

$$\rho' = b\lambda \text{ біт/с},$$

а повний інформаційний обмін каналу з урахування конфліктних ситуацій складе

$$G' = b\lambda_{tot} \text{ біт/с}.$$

Якщо позначити максимальну швидкість передачі бітів (ємність каналу) через R, то нормовану пропускну здатність каналу можна визначити як:

$$\rho = \frac{b\lambda}{R}, \tag{1.1}$$

і, відповідно, нормований інформаційний обсяг

$$G = \frac{b\lambda_{tot}}{R}, \tag{1.2}$$

Нормована пропускна здатність характеризує пропускну здатність як частину ($0 \le \rho \le 1$) ємності каналу. Нормований повний інформаційний обмін G також характеризує частину ємності каналу, але G може приймати значення, що перебільшують 1 ($0 \le G \le \infty$) [3].

Визначимо час передачі пакету

$$\tau = \frac{b}{R} \text{ секунд/пакет}, \tag{1.3}$$

З урахуванням (1.3) визначимо нормовану пропускну здатність (1.1) і нормований повний інформаційний обсяг (1.2) через час передачі пакету [3]

$$\rho = \lambda\tau, \tag{1.4}$$

$$G = \lambda_{tot}\tau, \tag{1.5}$$

Користувач може успішно передавати дані, якщо ні один з користувачів не почав передачу на інтервалі попередніх τ секунд або не почне її впродовж наступних τ секунд, оскільки за такої ситуації виникне конфлікт. Відповідно для успішної передачі кожного повідомлення необхідний часовий інтервал тривалістю 2τ секунд.

Статистика отримання повідомлень незалежними користувачами системи досить часто моделюється пуассонівським процесом. Ймовірність надходження нових K повідомлень впродовж τ секунд описується законом Пуассона [3,4]:

$$P(K) = \frac{(\lambda\tau)^K e^{-\lambda\tau}}{K!},\ K \geq 0, \tag{1.6}$$

де λ- середня частота надходження повідомлень.

Оскільки в протоколі ALOHA передають дані незалежно одне від одного, вираз (1.6) може бути застосованим для обчислення ймовірності випадку, коли впродовж інтервалу 2τ секунд буде отримано точно K інших повідомлень.

Позначимо через Ps – ймовірність успішної, тобто без конфліктів, передачі повідомлення користувача. Тоді з (1.6), підставляючи значення $\lambda_т$ і 2τ, можна обчислити

$$P_s = P(K=0) = \frac{(2\tau\lambda_{tot})^0 e^{-2\tau\lambda_{tot}}}{0!} = e^{-2\tau\lambda_{tot}}, \tag{1.7}$$

В останньому виразі загальна частота надходження повідомлень визначалася як сума частоти успішного надходження повідомлень λ і частоти відхилення даних $\lambda_т$. Тоді за визначення ймовірність успішного отримання пакету може бути визначена у вигляді:

$$P_s = \frac{\lambda}{\lambda_{tot}}, \tag{1.8}$$

Прирівнюючи (1.7) і (1.8) можна отримати

$$\lambda = \lambda_{tot} e^{-2\tau\lambda_{tot}}, \tag{1.9}$$

З урахуванням (1.4), (1.5) для нормованої пропускної здатності можна отримати [3,4]:

$$\rho = Ge^{-2G}, \tag{1.10}$$

Рівняння (1.10) пов’язує нормовану пропускну здатність і нормований повний інформаційний обсяг G при використанні протоколу ALOHA. Графік цієї залежності зображено на рис.1.3.

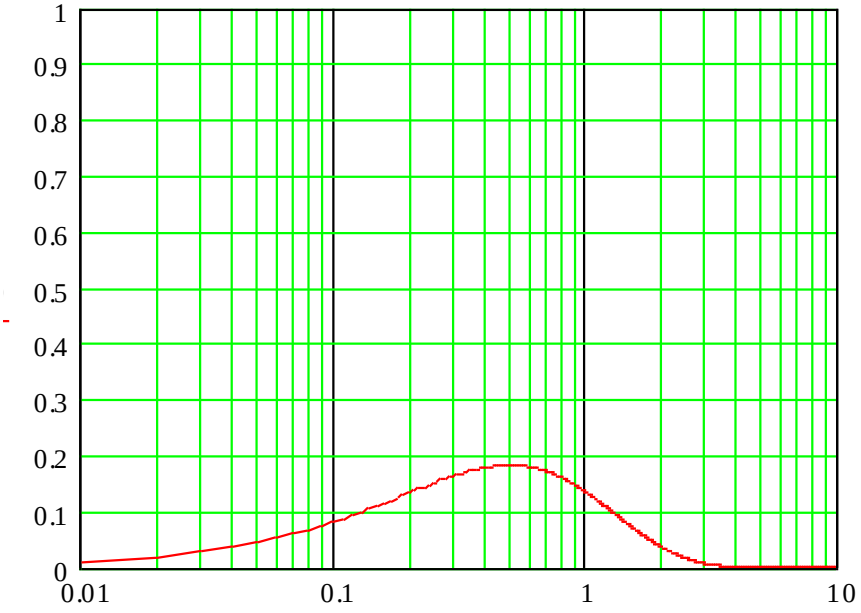

Рисунок 1.3 – Залежність пропускної здатності від нормованого інформаційного обсягу для класичного протоколу ALOHA

Аналіз графіка свідчить, що під час збільшення G зростає і пропускна здатність каналу, але до тих пір, поки суттєво не збільшиться кількість конфліктних ситуацій, що призводить до зменшення пропускної здатності.

Максимум нормованої пропускної здатності, рівний 1/2e=0,18, досягається при G=0,5. Тобто в каналі з чистим протоколом ALOHA може бути використано тільки 18 % ресурсу каналу зв’язку.

1.3.2 ALOHA з виділенням часових інтервалів (S-ALOHA)

Чистий протокол ALOHA можна покращити, якщо ввести певну координацію між станціями. Прикладом такого алгоритму є протокол ALOHA з виділенням часових інтервалів (slotted ALOHA – S–ALOHA). При цьому усім станціям передається послідовність синхронізуючих імпульсів. Як і для чистого протоколу ALOHA розмір пакетів, що передаються залишається незмінним. Повідомлення можуть передаватися тільки впродовж часового інтервалу між синхронізуючими імпульсами, а початок передачі пакета обов’язково повинен збігатися з початком інтервалу. Введення таких доповнень до чистого протоколу ALOHA дозволяє удвічі знизити кількість конфліктуючих ситуацій, оскільки конфліктувати тепер можуть тільки повідомлення, які передаються впродовж одного часового інтервалу. Доведено, що скорочення конфліктного часового інтервалу з 2τ до τ для S–ALOHA призводить до наступного співвідношення між нормованою пропускною здатністю ρ і нормованим повним інформаційним обсягом [2, 3, 4]:

$$\rho = Ge^{-G}, \tag{1.11}$$

Графік залежності (1.11) зображено на рис.1.4.

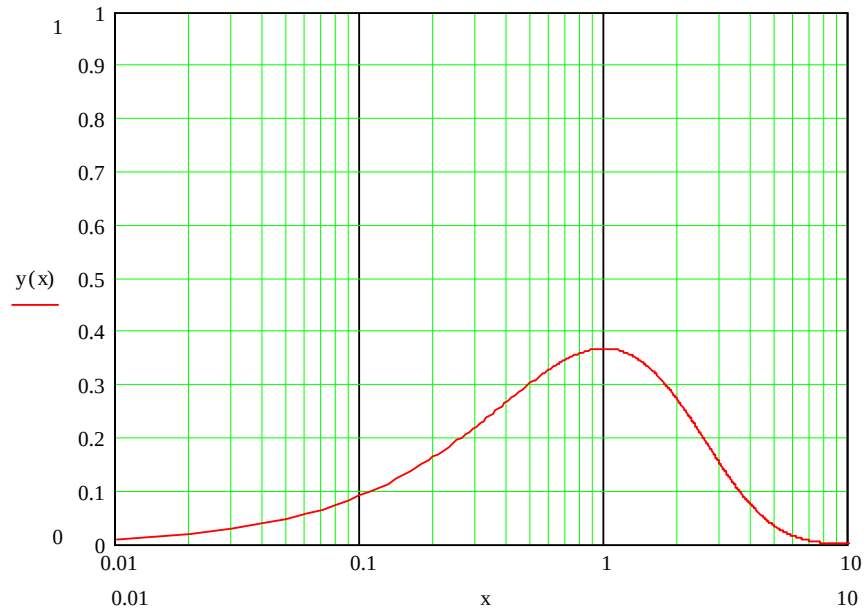

Рисунок 1.4– Залежність пропускної здатності від нормованого інформаційного обсягу для протоколу S–ALOHA

Порівнюючи з аналогічним графіком для чистої схеми ALOHA можна відзначити, що максимальне значення нормованої пропускної здатності для S–ALOHA рівняється 1/e=0,37, що практично удвічі перевищує можливості чистої ALOHA.

Режим повторної передачі системи S–ALOHA відрізняється від чистої схеми тим, що у разі отримання користувачем негативного підтвердження (NAK) наступна спроба передачі здійснюється через випадкову паузу, тривалість якої кратна тривалості часового інтервалу. Робота алгоритму продемонстрована на рис.1.5 [3].

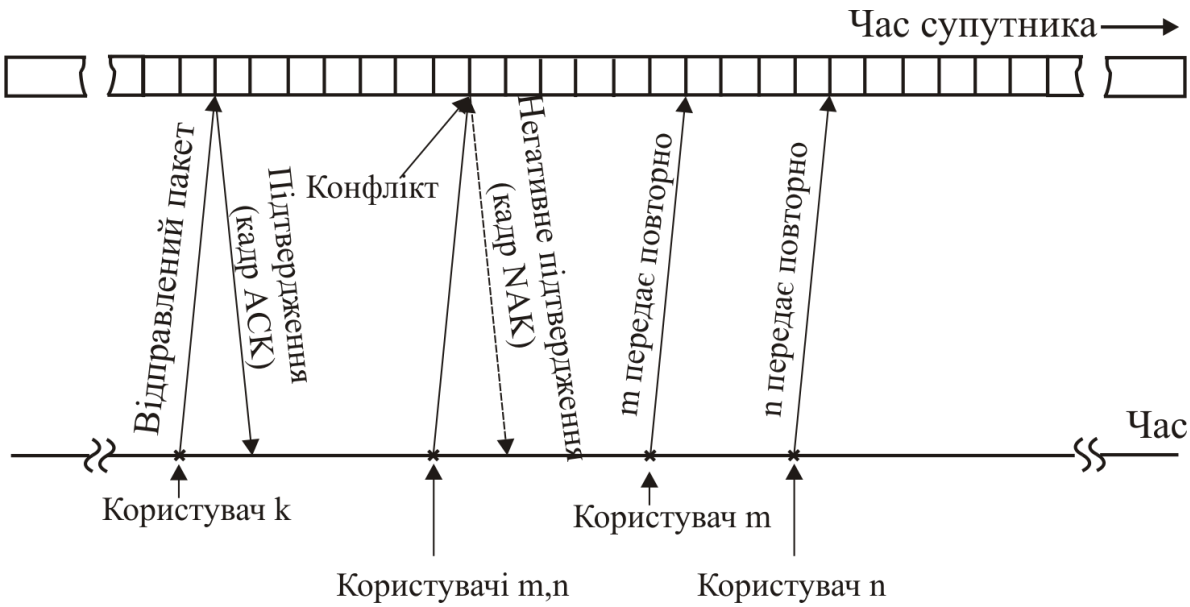

Рисунок 1.5 – Система довільного доступу: робота алгоритму ALOHA з виділенням часових інтервалів

Після успішної передачі пакету даних користувач k отримує (наприклад з супутника) підтвердження про отримання пакету. У той же час користувачі m, n у подальшому часовому фрагментові починають передачу одночасно, що призводить до виникнення колізії. В результаті до обох користувачів надходить негативне повідомлення. Для визначення часу повторної передачі обидві станції використовують генератор випадкових чисел. Далі показана ситуація безконфліктної передачі користувачами m, n після випадково обраної паузи. Хоча очевидно, що такий алгоритм запобігає конфлікту і під час повторної передачі відразу після першого конфлікту. У такому разі знову після випадкової паузи буде зроблена спроба повторної передачі.

1.3.3 Протокол множинного доступу з детектуванням несучої CSMA

Протокол множинного доступу з детектуванням несучої (Carrier Sense Multiple Access, CSMA) розглядається як вдосконалення основної схеми ALOHA. Термін детектування несучої означає лише той факт, що канал прослуховується відповідним пристроєм. Якщо він зайнятий, тобто інший пристрій передає дані, то передавач переходить до режиму очікування до того моменту, доки канал не звільниться. Цей метод дозволяє суттєво покращити пропускну здатність системи.

Як і в методі випадкового доступу, у такому середовищі не вимагається наявність центрального пристрою, тобто кожен пристрій приймає рішення про передачу самостійно. Оскільки фактично доступ до середовища отримує та станція, яка першою почала передачу, такий алгоритм називають методом конкурентного доступу.

Існує декілька версій схеми CSMA. При використанні, так званої, нестійкої схеми CSMA станції прослуховують канал і якщо канал вільний, то негайно починають передачу. Якщо канал зайнятий, станція перед повторним визначенням стану каналу вичікує випадковий проміжок часу, після чого знову прослуховує канал. Якщо на цей раз канал вільний, то термінал передає дані. Також можливі варіанти p-настійливих систем і l-настійливих систем. Для p-настійливих систем користувач також визначає стан каналу, але дані можуть передаватися з ймовірністю p. Пристрій також може відкласти передачу з ймовірністю 1- p, тобто здійснюється додатковий розподіл доступу до середовища передачі. Для p-настійливих систем CSMA усі користувачі, яким необхідно передати дані одночасно отримують доступ до каналу. як тільки він звільняється [2, 5].

1.3.3.1 Протокол множинного доступу CSMA/CD

На рис. 1.6 зображено формат бітового поля даних для специфікації Ethernet [3]. Наведемо пояснення до рис.1.6.

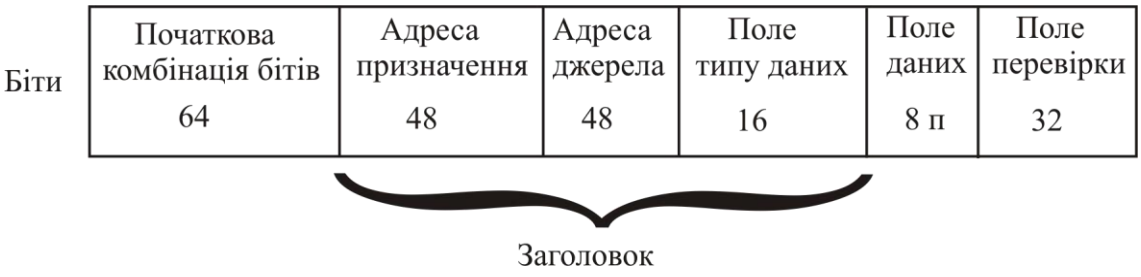

Рисунок 1.6 – Формат бітового поля для специфікації Ethernet

1. Максимальний розмір пакету рівняється 1526 байт. Структура пакету наступна: початкова комбінація бітів (8 байт) + заголовок (14 байт) + дані (1500 байт) + біти парності (4 байти).

2. Мінімальний розмір пакету рівняється 72 байти. Пакет містить початкову комбінацію бітів (8 байт) + заголовок (14 байт) + дані (46 байт) + біти парності (4 байти).

3. Мінімальна пауза між пакетами складає 9,6 мкс.

4. Початкова комбінація бітів містить 64-бітовий шаблон синхронізації, який складається з одиниць і нулів, що передуються, причому два останніх символи одиниці (101010…101011).

5. Станція – приймач вивчає поле адреси у заголовці пакету, після чого вирішує приймати їй цей пакет або ні. Перший біт указує тип адреси (0- індивідуальна адреса, 1 - групова). Поле , що складається тільки з одиниць, означає широкомовлення на усі станції.

6. Адреса джерела – унікальна адреса станції, що передає.

7. Тип поля визначає, як необхідно інтерпретувати поле даних. Наприклад, біти поля можуть використовуватися для опису кодування даних, шифрування, пріоритету повідомлень і т. ін.

8. Поле даних складається з цілого числа байт.

9. Поле перевірки парності містить біти парності, що генеруються за допомогою наступного полінома:

$$X32 + X26 + X23 + X22 + X16 + X11 + X10 + X8 + X7 + X5 + X4 + X2 + X + 1$$

В алгоритмі множинного доступу ETHERNET визначені наступні дії або відклики користувача.

1. Відкласти. Користувач не повинен передавати дані при виявлені несучої або впродовж мінімального інтервалу часу, що розділяє пакети.

2. Передавати. Якщо не використовується попередня дія, то користувач може передавати дані до закінчення часу передачі пакету або до виникнення конфлікту.

3. Перервати. Під час виникнення конфлікту користувач повинен зупинити передачу даних і сповістити про це інших користувачів задіяних у конфлікті.

4. Передати повторно. Користувач повинен реалізувати спробу повторної передачі після паузи випадкової тривалості (подібно до схеми ALOHA).

5. Відкат. Пауза перед n-ою спробою повторної передачі – це рівномірно розподілено випадкове число від 0 до 2^n-1, де ($0<n\leq10$). При $n>10$ інтервал залишається у межах від 0 до 1023. Одиницею виміру часу для інтервалу затримки перед повторною передачею є 512 біт (51,2 мкс).

На рис.1.7 зображено потік даних зі швидкістю 10 Мбіт/с при використанні манчестерської схеми з специфікації ETHERNET.

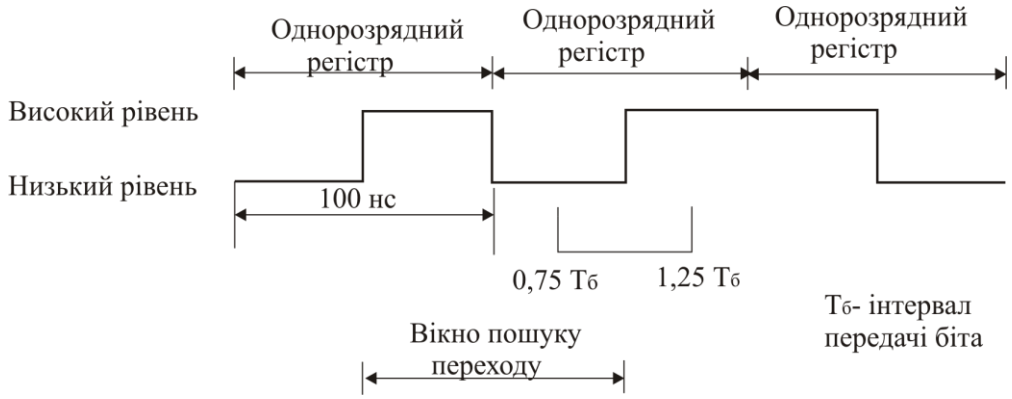

Рисунок 1.7 – Манчестерське кодування для схеми Ethernet

При такому форматуванні кожен одно бітовий елемент або позиція двійкового розряду містить перехід. Двійкова одиниця описується переходом з низького рівня на високий, а двійковий нуль – переходом з високого рівня на низький. Відповідно наявність переходів виступає показником наявності несучої у каналі. Якщо впродовж визначеного інтервалу часу (від 0,75 до 1,25 періода передачі біта) перехід не спостерігається – несуча втрачена, що свідчить про закінчення пакету.

Для отримання можливості передавати кадр, інтерфейс – відправник повинен переконатися що спільне середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, яку називають несучою частотою (Carrier Sense, CS).

Ознакою незайнятості каналу є відсутність несучої частоти, яка при манчестерському способі кодування рівняється 5…10 МГц (Ethernet 10 Мбіт/с) в залежності від послідовності одиниць і нулів, що передаються на поточний момент часу.

Якщо середовище вільне, то вузол-інтерфейс має право почати передачу. Приклад роботи мережі зображено на рис.1.8.

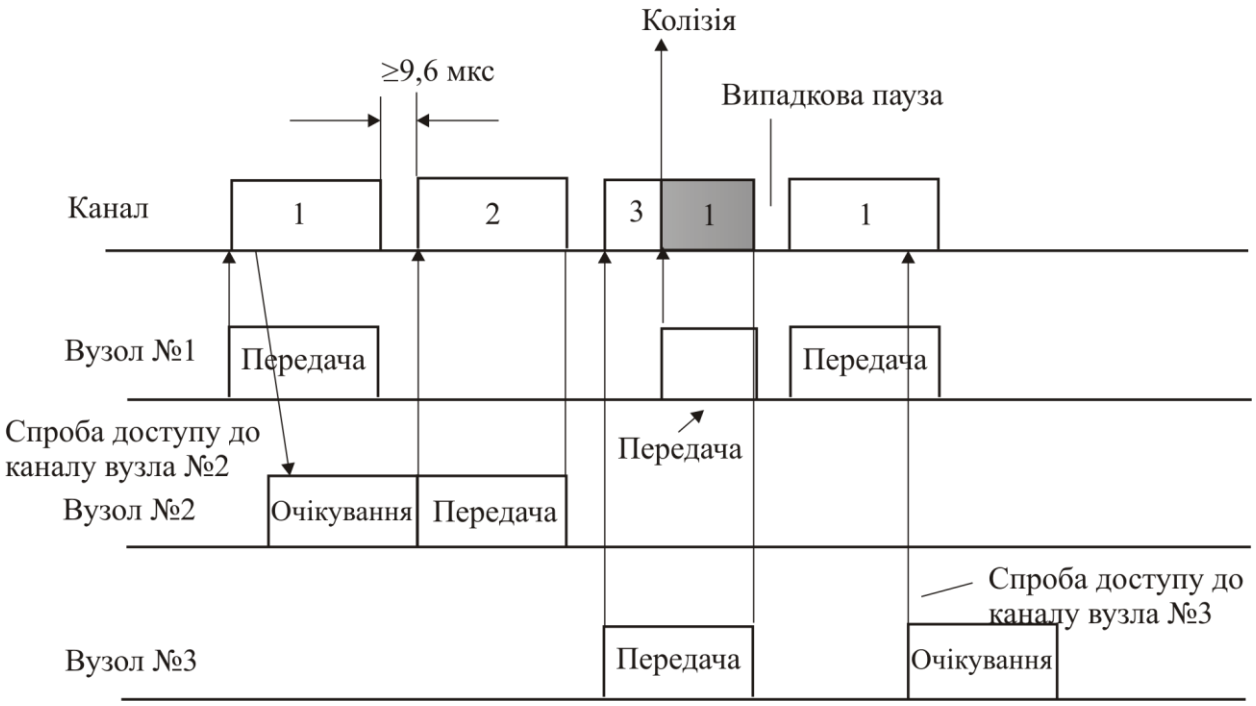

Рисунок 1.8 – Демонстрація виникнення колізії

Для ситуації, що зображена на рис. 1.8 вузол-інтерфейс 1 визначив, що канал вільний і почав передачу. У класичній мережі Ethernet на коаксіальному кабелі сигнали передавача 1 розповсюджуються на обидва боки, тому їх отримують усі вузли мережі. Як випливає з бітового формату (рис.1.6) кадр даних завжди супроводжується преамбулою і останній байт преамбули виступає обмежувачем початку кадру. Преамбула необхідна для входження приймача у побітову та побайтову синхронізацію з передавачем. Наявність двох підряд одиниць говорить приймачу, що преамбула закінчилася і наступний біт є початком кадру.

Усі користувачі мережі починають записувати байти кадру, що передається у свої внутрішні буфери. Перші 6 байт містять адресу призначення. Та станція, що впізнає свій власний адрес у заголовці кадру, продовжує записувати його вміст у внутрішній буфер, а інші прийом кадру припиняють. Станція призначення обробляє отримані дані і передає їх догори по своєму стеку. Кадр Ethernet містить не тільки адресу призначення, а і адресу джерела даних, тому станція-приймач знає кому необхідно надіслати відповідь.

Вузол-інтерфейс 2 під час передачі кадру вузлом також намагався почати передачу свого кадру, але визначає, що канал зайнятий (присутня несуча), тому вузол 2 примушений чекати, поки вузол 1 не припинить передачу кадру.

Після закінчення передачі кадру усі вузли мережі повинні дотримуватися технологічної паузи, яка рівняється міжпакетному інтервалу у 9,6 мкс. Ця пауза необхідна для приведення мережевих адаптерів у початковий стан, а також для запобігання монопольного захоплення каналу однією станцією.

Після закінчення технологічної паузи вузли мають право почати передачу свого кадру, оскільки середовище вільне.

У наведеному прикладі вузол 2 дочекався закінчення передачі кадру вузлом 1, зробив паузу у 9,6 мкс і почав передачу свого кадру.

Але, механізм прослуховування несучої і пауза між кадрами не гарантує ситуації, коли дві або більше станції одночасно вирішують що канал вільний і почнуть передавати свої кадри. При цьому виникає колізія, оскільки вміст обох кадрів стикається на одному кабелі і виникає спотворення інформації.

Колізія – це нормальна ситуація в роботі мережі Ethernet [3]. В наведеному прикладі колізію викликала одночасна передача кадрів вузлами 3 і 1. Для виникнення колізії не обов’язкова ситуація, коли декілька станцій почали передачу абсолютно одночасно, оскільки така ситуація малоймовірна. Більш ймовірна ситуація, коли один вузол почав передачу, а через деякий час інший вузол перевірив спільне середовище і не визначивши несучу(сигнали першого вузла ще не встигли до нього дійти), починає передачу свого кадру. Щоб коректно обробити колізію усі станції одночасно спостерігають за сигналами, що виникають на кабелі. Якщо сигнали, які передавалися і спостерігалися відрізняються, то фіксується факт визначення колізії (Collision Detection). Для збільшення ймовірності найшвидшого визначення колізії усіма станціями мережі, станція яка визначила колізію перериває

передачу свого кадру (у довільному місці) і підсилює ситуацію колізії передачею до мережі спеціальної послідовності, яку називають jam-послідовністю. Після цього, станція-передавач, що визначила колізію зобов'язана припинити передачу і зробити паузу впродовж короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення каналу і передачу кадру.

Випадкова пауза обирається за таким алгоритмом:

$$\text{Пауза} = L \cdot (\text{інтервал відтермінування}).$$

В технології Ethernet інтервал відтермінування обрано рівним 512 бітових інтервалів і для швидкості 10 Мбіт/с рівняється 100 нс. L – це ціле число, що обирається з рівною ймовірністю діапазону $[0, 2^N]$, де N – номер повторної спроби передачі даного кадру: 1, 2, …, 10.

Після 10-ї спроби, інтервал, з якого обирається пауза не збільшується. Тобто, випадкова пауза в технології Ethernet може приймати значення від 0 до 52,4 мкс.

Якщо 16 послідовних спроб передачі викликають колізію, то передавач повинен припинити спроби і відкинути цей кадр. Цей алгоритм має назву урізаного експоненціального двійкового алгоритму відтермінування.

Необхідно відзначити, що усі протоколи Ethernet підібрані таким чином, щоб при нормальній роботі мережі колізії чітко розпізнавалися.

1.3.3.2 Протокол множинного доступу CSMA/CA

Іншою варіацією методу CSMA є протокол CSMA/CA (CA - Collision Avoidance, із запобіганням конфліктів), який використовується у безпроводових локальних мережах IEEE 802.11.

Подібна ж схема – безпріоритетний множинний доступ з виключенням (Elimination Yield – Non Preemptive Multiple Access, EY-NPMA) використовується У специфікації HIPERLAN 1.

У мережах IEEE 802.11 рівень MAC забезпечує два режими доступу до спільного середовища: розподілений режим DCF і централізований режим PCF. Для розподіленого режиму реалізується саме метод CSMA/CA.

Метод CSMA/CA подібний до методу CSMA/CD, що використовується у специфікації Ethernet. Як і в методі CSMA/CD протокол CSMA/CA застосовує алгоритм виявлення несучої у спільному каналі з метою виявлення інших користувачів, що використовують спільний канал. Якщо канал виявляється вільним, то відразу починається передача пакетів. Але, якщо канал зайнятий, то методи CSMA/CD і CSMA/CA вирішують проблему конкурентності за різними алгоритмами.

У варіанті застосування CSMA/CD конкретний користувач у випадку зайнятості каналу (виявлення несучої) вичікує моменту звільнення каналу і як тільки виявляє незайнятість каналу відразу з ймовірністю 1 починає передачу пакетів. Якщо ж на цей момент два або більше користувачів готові для передачі, то обов’язково виникає колізія, оскільки усі ці користувачі починають передачу відразу після виявлення незайнятості каналу. Навпаки, для методу CSMA/CA користувачі також вичікують моменту звільнення каналу, але після його звільнення передача пакетів не починається, оскільки для цього протоколу після визначення незайнятості каналу додатково встановлюється затримка передачі, яка обирається випадково у деякому часовому інтервалі. Цю затримку називають затримкою відтермінування.

В результаті для протоколу CSMA/CA ймовірність виникнення колізій між декількома користувачами суттєво зменшується через випадковий вибір значення затримки відтермінування, що у значній мірі дозволяє усунути конкурентність у спільному каналі. До того ж, необхідно відзначити, що функція визначення колізій у протоколі CSMA/CD стає неефективною у безпровідних мережах, оскільки динамічний діапазон прийнятого сигналу, як

правило, досягає великого значення. Відповідно ймовірність помилок під час пакетної передачі у безпровідних мережах суттєво зростає [2…6].

Алгоритм випадкової затримки відтермінування подібний до схеми, що використовується в мережі Ethernet. Тривалість часових слотів, які формують затримку відтермінування визначається як сума часу на включення передавача, середнього часу затримки розповсюдження і середнього часу визначення зайнятості каналу.

Як відомо, у безпроводових мережах досить важливим питанням стає вирішення проблеми “схованих станцій”. Тому принципово протоколом MAC рівня стандарту IEEE 802.11 передбачені три альтернативних шляхи управління потоками пакетної передачі [7]. По-перше, найпростішим є варіант, коли тільки пакети даних використовуються для передачі. Така схема отримала назву базового методу CSMA/CA. Відповідно структура пакетів, що передаються може бути відображена так:

Базовий CSMA/CA: пакет даних – пакет даних – пакет даних-…

Відомо, що в радіоканалах через дію великої кількості факторів, таких як завади, шум, спотворення, затухання, перевідбиття і т. ін. можливі втрати даних. Для виключення втрат даних у стандарті IEEE 802.11 передбачається використання завадостійкого кодування і повторна передача за запитом на MAC рівні. Замість неефективного у безпровідних мережах прямого розпізнавання колізій за методом CSMA/CD, у цьому методі використовується їх неявне виявлення.

Відповідно другий альтернативний шлях пакетної передачі містить дві дії: передачу кадру від джерела повідомлення і передачу підтвердження від отримувача інформації. Для цього кожен кадр, що передається, повинен підтверджуватися кадром позитивної “квитанції”, що відсилається станцією призначення (одержувачем). Якщо впродовж визначеного інтервалу часу квитанція не надходить, то станція-передавач вважає, що виникла колізія.

Звичайно таку схему називають SW CSMA/CA, де абревіатура SW означає Stop- and-Wait (“Зупинись і Зачекай”)

Відповідно структура пакетів, що передаються для SW CSMA/CA може бути відображена так:

SW CSMA/CA: пакет даних – пакет підтвердження (ACK) – пакет даних – пакет підтвердження (ACK) - …

Тобто, для управління доступом до фізичного середовища стандарту 802.11 застосовується протокол DFW MAC, який ґрунтується на контролі несучої і усунені конфліктів шляхом підтвердження прийому даних при багатостанційному доступі.(CSMA-CA) Для визначення зайнятості каналу використовується алгоритм оцінки рівня сигналу у каналі, що передбачає вимірювання сигналів на вході приймача (RSSI) та якості сигналу (SQ).

Якщо потужність сигналу на вході приймача нижче наперед заданого значення, то канал вважається вільним, і на рівні доступу до каналу (MAC) стан каналу встановлюється “вільний (CTS)”. Якщо потужність прийнятих сигналів вище порогового значення, то передача даних не відбувається у відповідності до протоколу.

Протокол DFW MAC через процедури підтвердження прийому і повторної передачі на рівні MAC дозволяє поновлювати дані при низькому рівні сигналу, що забезпечує надійність зв’язку в умовах конфліктів при доступі до спільного середовища і наявності зовнішніх завад.

Конфлікти між пакетами, що передаються можливі, оскільки розпізнавання приймачем несучої сигналу, що передавався іншими станціями ускладнено через суттєвий розкид амплітуд сигналів через наявність затухання сигналу, а також через те, що станції працюють у напівдуплексному режимі і, відповідно, в процесі передачі не приймають сигнали, а значить, не визначають конфлікти. Як результат можливі помилки у визначення зайнятості каналу, і, як наслідок, одночасна передача пакетів

двома або більше користувачами. Усунення цього недоліку досягається зменшенням зони обслуговування або розширенням динамічного діапазону приймача абонентської станцій, що визначають наявність чужої несучої у каналі.

Для підвищення надійності передачі даних за таких умов, а також для усунення ефекту схованих станцій у режимі доступу DCF можливий також третій алгоритм передачі з чотирма кадрами (рис.1.9):

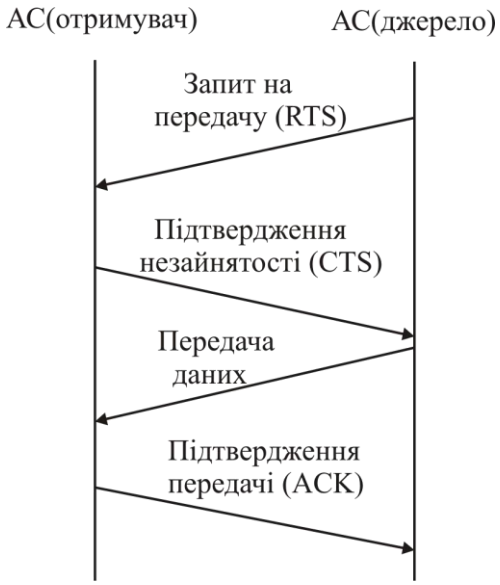

Рисунок 1.9 – Метод CSMA/CA з чотирма кадрами (4-WH CSMA/CA)

Абонентська станція, яка бажає захопити канал, у відповідності з описаним алгоритмом, починає передачу у визначеному слоті, замість кадрів даних надсилає станції призначення короткий службовий кадр RTS (Request To Send – запит на передачу). Тим самими вона сповіщає усі АС в зоні радіовидимості про, те що відбувається обмін інформацією. Усі станції, що прийняли кадр RTS, утримуються від передачі для виключення конфліктів. На цей запит станція призначення повинна відповісти службовим кадром CTS (Clear To Send – вільна для передачі), після чого станція-передавач надсилає кадр даних. Кадр CTS повинний сповістити про захоплення каналу ті станції, які знаходяться поза зоною сигналу станції-передавача, але в зоні досяжності станції призначення, тобто є схованими для станції передавача.

Після прийому кадру CTS АС-джерело передає кадр даних, а АС–одержувач після прийому кадру даних передає кадр підтвердження.

Максимальна довжина кадру даних для 802.11 складає 2346 байт, довжина кадру RTS кадру – 20 байт, CCTS – кадру – 14 байт. Оскільки RTS і CTS кадри набагато коротші порівняно з кадрами даних, то втрати даних в результаті колізій RTS або CTS–кадрів суттєво менші порівняно з колізіями даних. Цей третій режим робот відомий за абревіатурою 4–WH CSMA/CA (4–Way Handshaking – “ Чотирьохразове рукостискання ”)

Відповідно структура пакетів, що передаються для 4–WH CSMA/CA може бути відображена так [7]:

4-WH CSMA/CA: запит на передачу (пакет RTS) – підтвердження незайнятості (пакет CTS) – пакет даних – підтвердження передачі (пакет ACK) – …

Процедура обміну RTS і CTS – кадрами не є обов’язковою. При невеликому навантаженні у мережі від неї можна відмовитись, оскільки для такої ситуації колізії трапляються досить рідко,це означає, що не доцільно витрачати додатковий час на виконання процедури обміну RTS і CTS – кадрами.

Протокол DFWMAC дозволяє вводити пріоритети для передачі сигналів з різною категорією важливості або з підвищеними вимогами до затримки передачі. Пріоритети реалізуються через введення затримки дозволу на захоплення каналу.

Це можливо саме завдяки конкурентному способу захоплення каналу абонентською станцією – перший користувач, що почав передачу після вивільнення каналу і займає канал (рис.1.10).

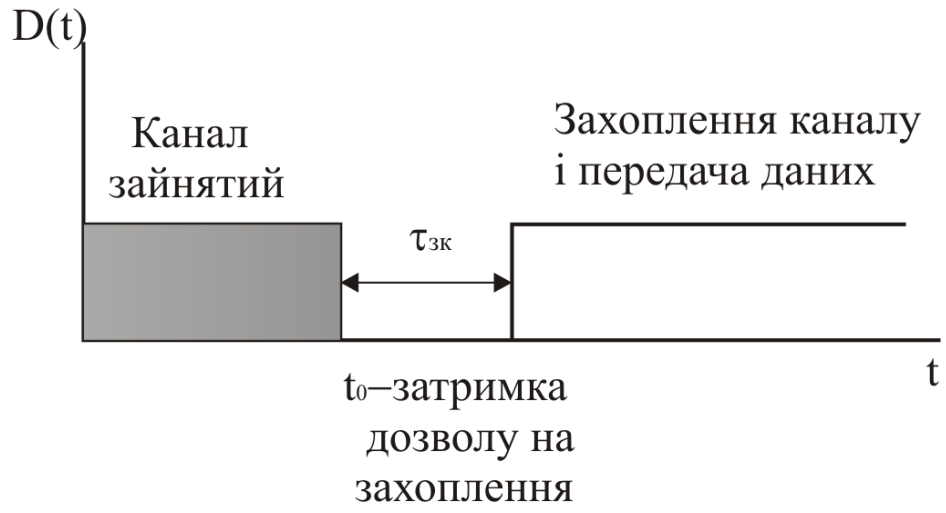

Рисунок 1.10 – Робота в режимі DCF

Протокол CSMA/CA із затримкою дозволу на захоплення каналу працює за таким алгоритмом: абонентська станція, яка готова до передачі, прослуховує канал і якщо канал вільний, то АС затримує передачу на час затримки дозволу на захоплення. Передача даних починається, якщо у момент часу $t_0+\tau_{зк}$ канал виявляється вільним.

Таким чином, якщо канал зайнятий або займається іншою АС впродовж часу затримки дозволу на захоплення каналу, то канал не може бути зайнятим АС у якої встановлено дане значення $\tau_{зк}$.

Тому, якщо вивільнення каналу для передачі даних очікують одночасно дві абонентських станції з різними значеннями $\tau_{зк}$, то канал після вивільнення буде зайнятим тією АС, для якої $\tau_{зк}$ буде меншим.(рис.1.11).

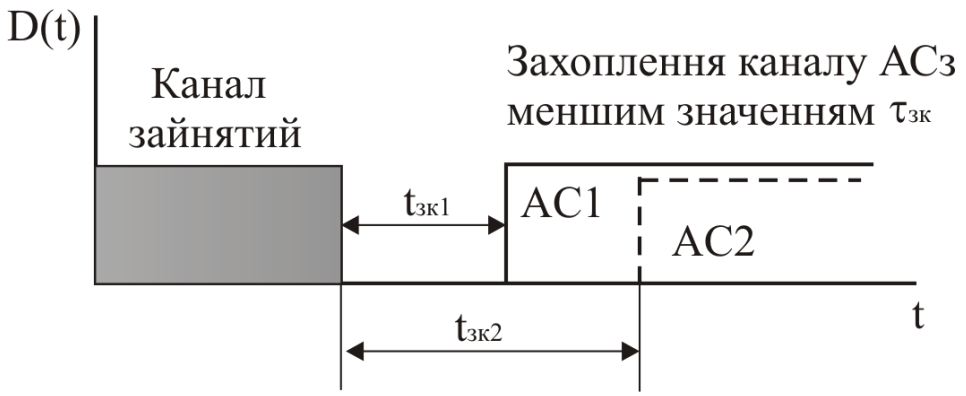

Рисунок 1.11 – Робота в режимі CSMA/CA із затримкою захоплення

Якщо АС з меншим значенням τз не потребується передача пакетів даних, то канал може зайняти абонентська станція АС2. Але, у будь-якому разі, абонентські станції з меншим значенням $\tau_{зк1}$ мають перевагу щодо захоплення каналу, оскільки менший час затримки надає їм можливість першочергового захоплення. Саме цим і реалізується пріоритетна передача інформації.

У протоколі DFW MAC використовуються три значення затримки захоплення каналів [7]. Найменша затримка захоплення використовується для повідомлень, що вимагають найменшої затримки передачі, наприклад, мови.

Для інформації про управління використовується середнє значення затримки захоплення і найбільше значення затримки захоплення використовується для асинхронної передачі даних. Мінімальна затримка захоплення використовується для передачі пакета підтвердження прийому даних, передачі блока даних рівня LLC, який розбивається на декілька пакетів MAC рівня. При передачі багато пакетного повідомлення LLC – рівня кожен пакет рівня MAC передається АС окремо. Після отримання пакета АС-одержувач через мінімальну затримку відправляє кадр підтвердження прийому, після отримання якого з мінімальною затримкою починається передача наступного пакета багатопакетного повідомлення. В результаті якщо АС захопила канал, то він буде утримуватися впродовж всього часу передачі пакетів завдяки мінімальній затримці захоплення каналу.

Розглянемо більш детально алгоритм формування затримки захоплення або затримки відтермінування (backoff algorithm).

По-перше, відзначимо, що режим доступу DCF вимагає синхронізації станцій. В специфікації 802.11 ця проблема вирішується так – часові інтервали починають свій відлік від моменту закінчення чергового кадру (рис.1.12).

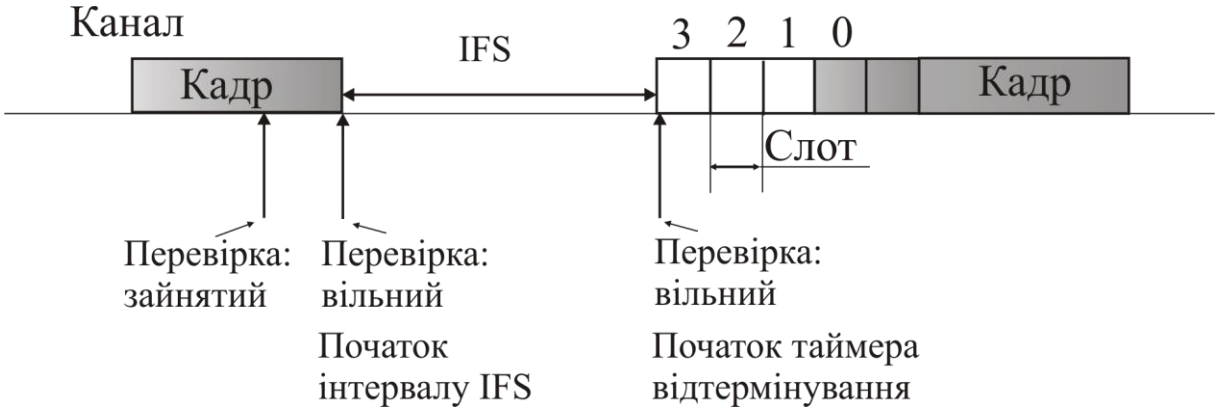

Рисунок 1.12 – Демонстрація роботи алгоритму CSMA/CA

Це не вимагає передачі будь-яких синхронізуючих сигналів і не обмежує розмір пакету розміром слота, оскільки слоти приймаються до уваги тільки при прийнятті рішення про початок передачі кадру.

Станція, яка бажає передати кадр, зобов’язана попередньо прослухати канал. Як тільки вона зафіксує закінчення передачі кадру, вона обов’язково відраховує так званий міжкадровий інтервал часу (IFS). Якщо після закінчення інтервалу IFS канал залишається вільним, то починається відлік часових слотів фіксованої тривалості. Кадр можна починати передавати тільки на початку якогось з слотів, якщо канал вільний. Станція обирає слот для початку передачі на підставі урізаного експоненціального алгоритму відтермінування, подібного до методу CSMA/CD. Номер слота обирається як випадкове число, яке рівномірно розподілене в інтервалі [0, CW], де CW означає так зване конкурентне вікно CW (Contention Window). Роботу методу доступу продемонструємо на підставі рис.1.12.

Нехай станція А обрала для передачі на підставі урізаного експоненціального двійкового алгоритму відтермінування слот №3. При цьому вона надає таймеру відтермінування значення 3 і починає перевіряти стан каналу на початку кожного слота. Якщо канал вільний, то від значення таймера віднімається одиниця, а якщо результат лічильника рівняється 0, то починається передача кадру. Таким чином, забезпечується умова

незайнятості усіх слотів, включаючи обраний. Ця умова є необхідною умовою початку передачі.

Якщо ж на початку якогось слота канал виявляється зайнятим, то віднімання одиниці не відбувається і таймер зупиняється (“заморожується”). У такому випадку станція починає новий цикл доступу до каналу, змінюючи алгоритм вибору слота для передачі. Як і в попередньому циклі, станція прослуховує канал і при його звільненні робить паузу на період міжкадрового інтервалу. Якщо середа залишилася вільною то станція використовує значення “замороженого таймера” в якості номера слота і повторює описану вище процедуру перевірки вільних слотів з відніманням одиниць, починаючи із “замороженого” значення таймера відтермінування.

Розмір слота залежить від способу кодування сигналу – так, для методу FHSS тривалість слота складає 28 мкс, а для методу DSSS – 1 мкс. Тривалість слота обирається таким чином, щоб вона перебільшувала час розповсюдження сигналу між будь-якими станціями мережі плюс час, що визначається станцією на визначення зайнятості каналу. Якщо така вимога виконується, то кожна станція може вірно розпізнати початок передачі кадру при прослуховуванні слотів, що передують обраному слоту для передачі. Це, у свою чергу, означає наступне – колізія може виникнути тільки у тому випадку, коли декілька станцій обирають один і той же слот для передачі. У такому випадку кадри спотворюються і квитанції від станції отримувача не приходять. Не отримавши квитанції впродовж визначеного інтервалу часу станція передавач фіксує факт колізії і намагається знову передати свої кадри.

При кожній невдалій спробі передачі кадру інтервал [0 CW] з якого обирається номер слота , подвоюється. Якщо, наприклад, початковий розмір вікна обрано рівним 8 (тобто CW=7), то після першої колізії розмір вікна повинен рівнятися 16 (CW=15), після другої послідовної колізії – 32 (CW=31). Початкове значення CW у відповідності до стандарту 802.11

залежить від типу фізичного рівня, що використовується у безпровідній локальній мережі.

Як і в методі CSMA/CD, для методу CSMA/CA кількість невдалих спроб передачі одного кадру обмежено, але стандарт не дає точного значення цієї верхньої межі. Коли верхня межа у N спроб досягнута, то кадр відкидується, а лічильник послідовних колізій встановлюється рівним 0. Цей лічильник також встановлюється у нуль, якщо кадр після деякої кількості невдалих спроб все ж таки передається успішно.

1.3.3.3 Централізований режим доступу PCF

Якщо в мережі з базовим набором послуг (Basic Service Set – BSS) присутня станція, що виконує функції точки доступу, то може використовуватися централізований метод доступу PCF, що забезпечує пріоритетне обслуговування трафіку. При цьому кажуть, що точка доступу відіграє роль арбітра каналу.

Режим доступу PCF у мережах 802.11 існує сумісно з режимом DCF. Обидва режими координуються за допомогою трьох типів міжкадрових інтервалів (рис.1.13) [7].

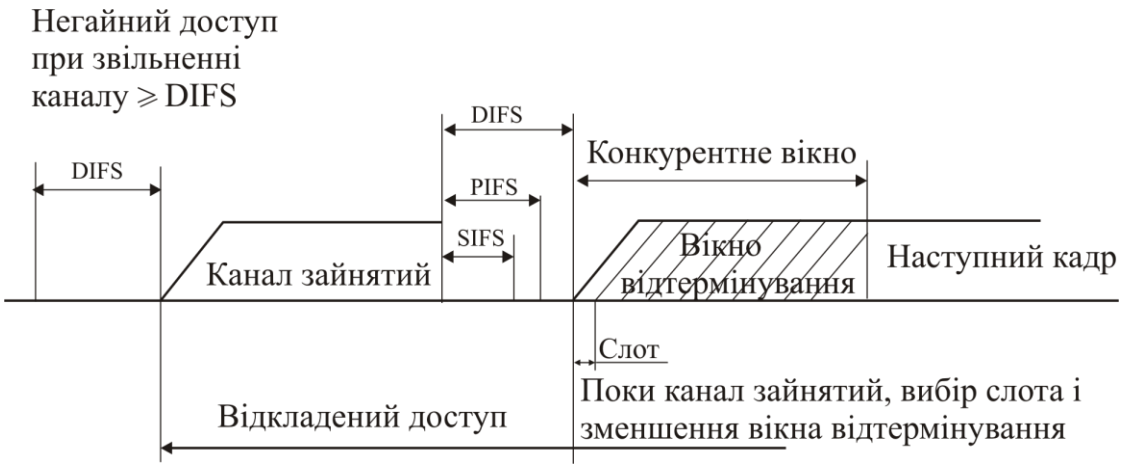

Рисунок 1.13 – Алгоритм централізованого доступу PCF

Після вивільнення каналу кожна станція оцінює час вільного стану каналу порівнюючи його з трьома значеннями:

– короткий міжкадровий інтервал (Short IFS);
– короткий міжкадровий інтервал режиму PCF(PIFS);
– короткий міжкадровий інтервал режиму DCF(DIFS).

Захоплення каналу за допомогою розподіленої процедури DCF можливий тільки у тому випадку, коли канал вільний впродовж часу рівного або більшого за DIFS. Тобто, як IFC у режимі DCF необхідно використовувати інтервал DIFS – найдовший інтервал з трьох можливих, що надає цьому режиму найнижчий пріоритет.

Міжкадровий інтервал SIFS має найменше значення, він використовується для першочергового захоплення каналу відповідними CTS– кадрами або квитанціями, які продовжують або завершують вже почату передачу кадру.

Значення міжкадрового інтервалу PIFS більше порівняно з SIFS, але менше порівняно з DIFS. Проміжком часу між PIFS і DIFS користується арбітр каналу, впродовж цього інтервалу він може передати спеціальний кадр, який сповіщає усі станції, про початок періоду, що контролюється. Отримавши цей кадр, станції які бажали скористатися алгоритмом DCF для захоплення каналу, вже не можуть цього зробити, оскільки вони повинні дочекатися закінчення інтервалу, що контролюється. Тривалість цього періоду визначається у спеціальному кадрі, але цей період може закінчитися і раніше, якщо у станцій немає чутливого до затримок трафіка. У цьому випадку арбітр передає службовий кадр, після якого по закінченню інтервалу DIFS починає роботу режим DCF.

На інтервалі, що управляється, реалізується централізований метод доступу PCF. Арбітр використовує процедуру опитування з метою по черзі надати кожній такій станції право на використання каналу, направляючи їй спеціальний кадр. Станція, отримавши такий кадр, може відповісти іншим

кадром, який підтверджує прийом спеціального кадру і одночасно передає дані (або за адресою арбітра, або безпосередньо від станції).

Для того, щоб якась частина каналу завжди надавалася асинхронному трафіку, тривалість періоду, що контролюється, є обмеженою. Після його закінчення арбітр передає відповідний кадр і починається неконтрольований період. Кожна станція може працювати в режимі PCF, для цього вона повинна підписатися на цю послугу в процесі підключення до мережі.

1.4 Протокол доступу з цифровим детектуванням DSMA

Протокол DSMA (Digital Sense Multiple Access) використовує схожий до CSMA/CA принцип роботи. Цей метод також називають множинним доступом з детектуванням придушення (Inhibit Sense Multiple Access, ISMA) []2,3,4]. Різниця полягає у тому, що зайнятість каналу визначається не шляхом прослуховування, а через надсилання базовою станцією пакета, в якому визначається статус каналу. Для нормальної роботи цього протоколу базова станція повинна бути синхронізована з передавачами таким чином, щоб передавачі не передавали дані під час передачі статусу каналу. Якщо канал зайнятий, то станції очікують випадкового часового інтервалу для наступної передачі. Оскільки декілька станцій можуть передавати дані, центральна станція надсилає пакет про підтвердження отримання пакету даних.

1.5 Методи випадкового доступу з резервуванням

1.5.1 Алгоритм ALOHA з використанням резервування

У сучасних безпровідних системах передачі інформації, як правило, застосовують сполучення механізмів централізованого призначення часових інтервалів і методів конкурентного доступу [3]. Тобто, практично робота

таких систем відбувається у два етапи. Перший етап – резервування ресурсів (часових інтервалів) для майбутньої передачі. На цьому етапі усі станції заявляють (або намагаються заявити) про свої потреби щодо канальних ресурсів. На другому етапі відбувається безпосередня передача даних у відведеному часовому інтервалі. В таких схемах використовується центральний термінал за допомогою якого реалізується синхронізація передачі і здійснюється резервування. Як правило, механізми резервування призводять до зростання часу затримки отримання пакетів при невеликому завантаженню системи, але забезпечують для неї більш високу пропускну здатність.

Прикладом такого механізму є схема множинного доступу з розподіленням за запитом – DAMA (Demand Assigned Multiple Access), яку також інколи називають схемою ALOHA з резервуванням. Суттєве покращення роботи протоколу ALOHA було досягнуто в результаті введення резервування (reservation ALOHA – R–ALOHA).

Такий протокол, зокрема, використовується в системах супутникового зв’язку. Впродовж визначеного часового інтервалу, який розбивається на міні-інтервали, усі станції намагаються зарезервувати для себе майбутні часові інтервали для передачі даних. Оскільки на стадії резервування виникають конфлікти, деякі станції не резервують для себе часові інтервали. Якщо станція спромоглася зарезервувати часовий інтервал, то ніяка інша станція не може у цей час здійснювати передачу. Таким чином, базова станція збирає усі успішні запити (інші ігноруються) і надсилає зворотно список з указанням прав доступу до наступних часових інтервалів, цьому списку підкорюються усі станції. Схема DAMA відноситься до схем з наявним резервуванням, коли кожний інтервал резервується явно.

Системи з використанням R–ALOHA можуть використовуватися у двох основних режимах [3].

Режим без резервування (стан спокою).

1. Виділений інтервал часу розбивається на невеликі під інтервали резервування.

2. Ці підінтервали використовуються для резервування інтервалів передачі повідомлень.

3. Після запиту резервування користувач очікує підтвердження і розподілення інтервалів.

Режим з резервуванням.

1. Якщо не використовується резервування, то часовий інтервал розбивається на M+1 інтервалів.

2. Перші M інтервалів використовуються для передачі повідомлень. Останній інтервал розбивається на під інтервали, які використовуються під час резервування або передачі запитів.

3. Передавачі передають пакети даних тільки у виділених їм елементах M-інтервалів.

Приклад використання протоколу наведено на рис.1.14 [3].

У стані спокою час з метою резервування розбивається на невеликі підінтервали. Після резервування система конфігурується так, що після перших M=5 інтервалів передачі повідомлень слідують V=6 підінтервалів резервування, подалі ця процедура повторюється. На рис.1.14 продемонстровано процес відправлення запиту і отримання підтвердження. Для наведеного прикладу передавальній станції необхідно зарезервувати три інтервали часу за умови, що кількість інтервалів M=5, а кількість під інтервалів V=6. У підтвердженні супутника містяться інструкції відносно розміщення першого пакету даних. Управління розподілено, тому усі користувачі отримують сигнал з супутника і, відповідно, інформацію про резервування і розподіл часу.

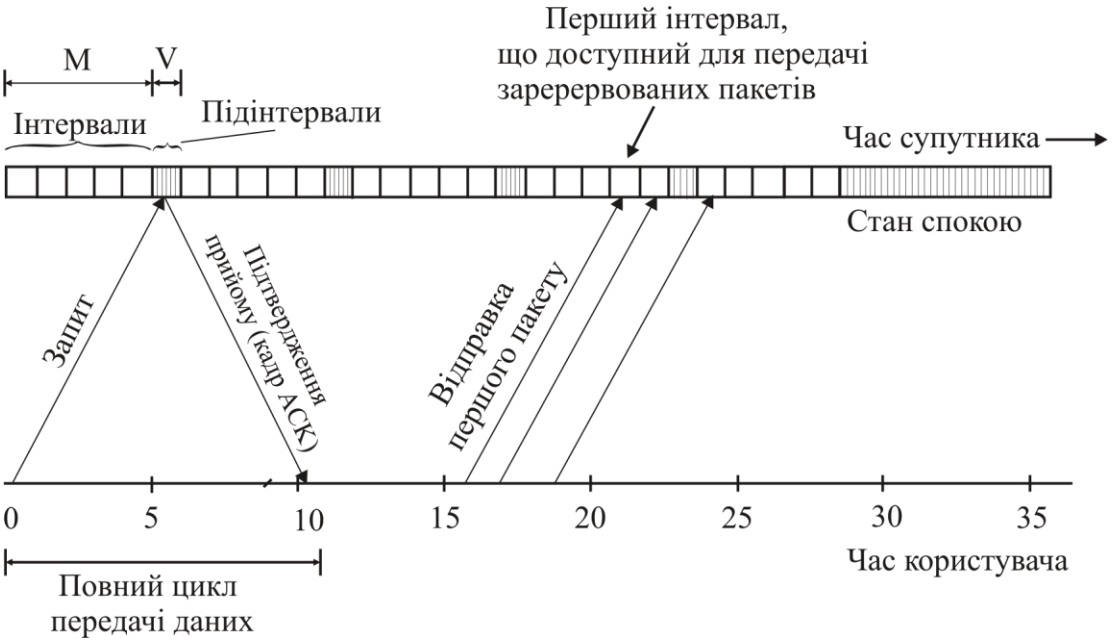

Рисунок 1.14 – Приклад реалізації алгоритму ALOHA з використанням резервування.

Тому у сигналі підтвердження супутника знаходиться уся інформація, яка міститься у повідомленні про виділення першого часового інтервалу. Як показано на рис.1.14 впродовж наступного інтервалу часу станція передає другий пакет. Далі користувачу відомо, що наступний інтервал складається з шести під інтервалів, призначених для резервування, тому передача інформаційних пакетів впродовж цього інтервалу не відбувається. Третій (останній) пакет відсилається впродовж четвертого інтервалу, якщо резервування не відбувається, то система повертається до стану спокою. Оскільки управління здійснюється розподілено, усі користувачі отримують від супутника інформацію і відповідні синхронізуючі імпульси.

1.5.2 Порівняння продуктивності протоколів S-ALOHA і R-ALOHA

Як правило, якість цифрової системи з використанням будь-якого виду цифрової модуляції оцінюють залежністю коефіцієнта бітової помилки від параметра Eb/N0 (відношення енергії, що приходиться на один біт до

спектральної щільності шуму). Застосування такого критерію є досить ефективним, оскільки Eb/N0 – це практично нормоване відношення сигнал/шум.

Відповідно нормовані криві дозволяють порівнювати продуктивність різних схем модуляції.

Для аналізу систем множинного доступу також використовується подібний показник, а саме – залежність середньої затримки від нормованої пропускної здатності [3, 4].

На рис.1.15 наведена ідеальна залежність затримки від пропускної здатності.

Для нормованих значень пропускної здатності $0 \le \rho < 1$ час затримки рівняється нулю, при $\rho = 1$ значення затримки нескінченно зростає. Поряд з ідеальною залежністю наведена типова залежність, а також напрям у якому відбувається збільшення продуктивності.

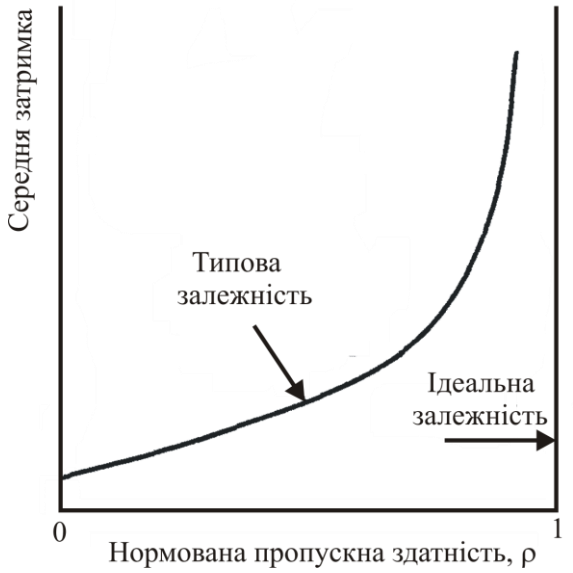

Рисунок 1.15 - Залежність середньої затримки від нормованої пропускної здатності

На рис.1.16 порівнюються залежності часу затримки від нормованої пропускної здатності для алгоритмів S–ALOHA і R–ALOHA.

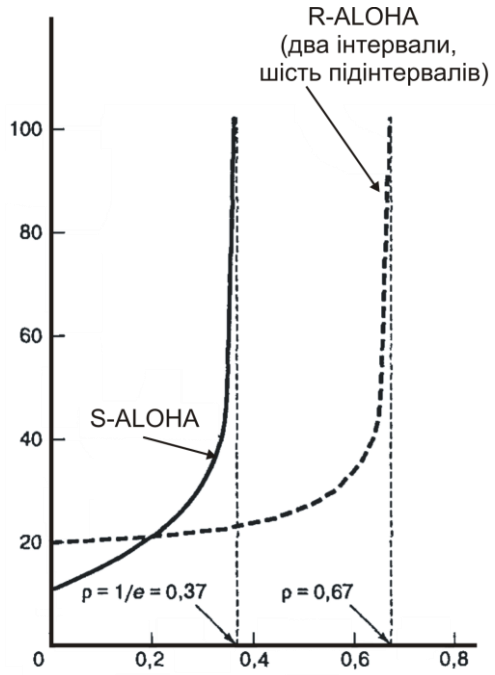

Рисунок 1.16 – Порівняльні характеристики протоколів S–ALOHA і R–ALOHA

Формат повідомлень, що відповідають рис.1.16 – два інтервали передачі даних і шість підінтервалів резервування. Час затримки цих двох протоколів порівнюють з ідеальною кривою. Для пропускної здатності $\rho<0,2$ середній час затримки для системи S–ALOHA менший порівняно з R–ALOHA. У той же час для значень ρ в інтервалі $0,2\leq\rho<0,67$ протокол R–ALOHA виглядає кращим за S–ALOHA через суттєво менше значення часу затримки.

Тобто, при мало інтенсивному обміні даними перевагу має протокол S–ALOHA, оскільки він не вимагає службових витрат, необхідних для резервування підінтервалів як у випадку протоколу R–ALOHA.

Але, при $\rho>0,2$ конфліктні ситуації і повторна передача даних в системі S–ALOHA призводять до того, що час затримки зростає швидше порівняно з R–ALOHA (і необмежено зростає при $\rho=0,37$). При більш високих значеннях пропускної здатності $0,2\leq\rho<0,67$ службові витрати повністю окупаються і забезпечують менш швидке зростання затримки при

збільшенні ρ. При використанні R–ALOHA час затримки нескінченно зростає при ρ=0,67.

Схема з резервуванням відрізняється від попередньої схеми DAMA тим, що етап резервування відбувається не на основі конкурентного доступу, а за звичайною фіксованою схемою TDMA. Кожному пристрою призначається часовий міні-інтервал, впродовж якого він повідомляє буде передавати дані чи ні. Тому на початку кожного циклу передачі базова станція передає пакет, який розбитий на N інтервалів, в кожному з яких зазначено зарезервовано канал або ні. Після цього слідують N-k інтервалів для даних. Такий метод гарантує для кожної станції, що зарезервувала канал, визначену пропускну здатність.

Інші станції можуть передавати дані впродовж інтервалів, які ніхто не резервував, але вже на умовах конкурентного доступу і без гарантії доставки пакетів.

1.5.3 Схема з резервуванням пакетів PRMA

Протокол множинного доступу з резервуванням пакетів (PRMA, Packet Reservation Multiple Access) є прикладом алгоритму зі схованим резервуванням, оскільки інтервали резервуються неявно, центральний пристрій на початку кожного циклу розсилає список з розподілом часових інтервалів. Саме ж резервування відбувається за іншою схемою. Припустимо, що якомусь з пристроїв необхідно передати дані, але при цьому він не зарезервував часовий інтервал. Цей пристрій регулярно отримує список з зарезервованими інтервалами. Наприклад, у такому списку указано, що третій, п’ятий і восьмий інтервали не зарезервовані, тобто вільні. Пристрій за випадковим законом приймає рішення в якому інтервалі можна передавати дані. Припустимо, що прийнято рішення про передачу у п’ятому інтервалі, якщо передача пройшла успішно, то користувач отримує про це підтвердження, базова станція резервує цей канал для нового пристрою і

вносить його у свій список. Якщо ж запит не дійшов до базової станції, то користувач знову повинен спробувати передати дані в одному з вільних інтервалів [2, 3, 5].

2 МОДЕЛЮВАННЯ ПРОТОКОЛІВ МНОЖИННОГО ДОСТУПУ

2.1 Обґрунтування базового алгоритму програмного комплексу

По-перше, визначимося з основними загальними припущеннями, на яких ґрунтується і які є необхідними для комп'ютерного моделювання протоколів множинного доступу.

Узагальнену структурну схему системи з пакетною передачею даних з використанням точки доступу, що пропонується для моделювання, зображено на рис.2.1.

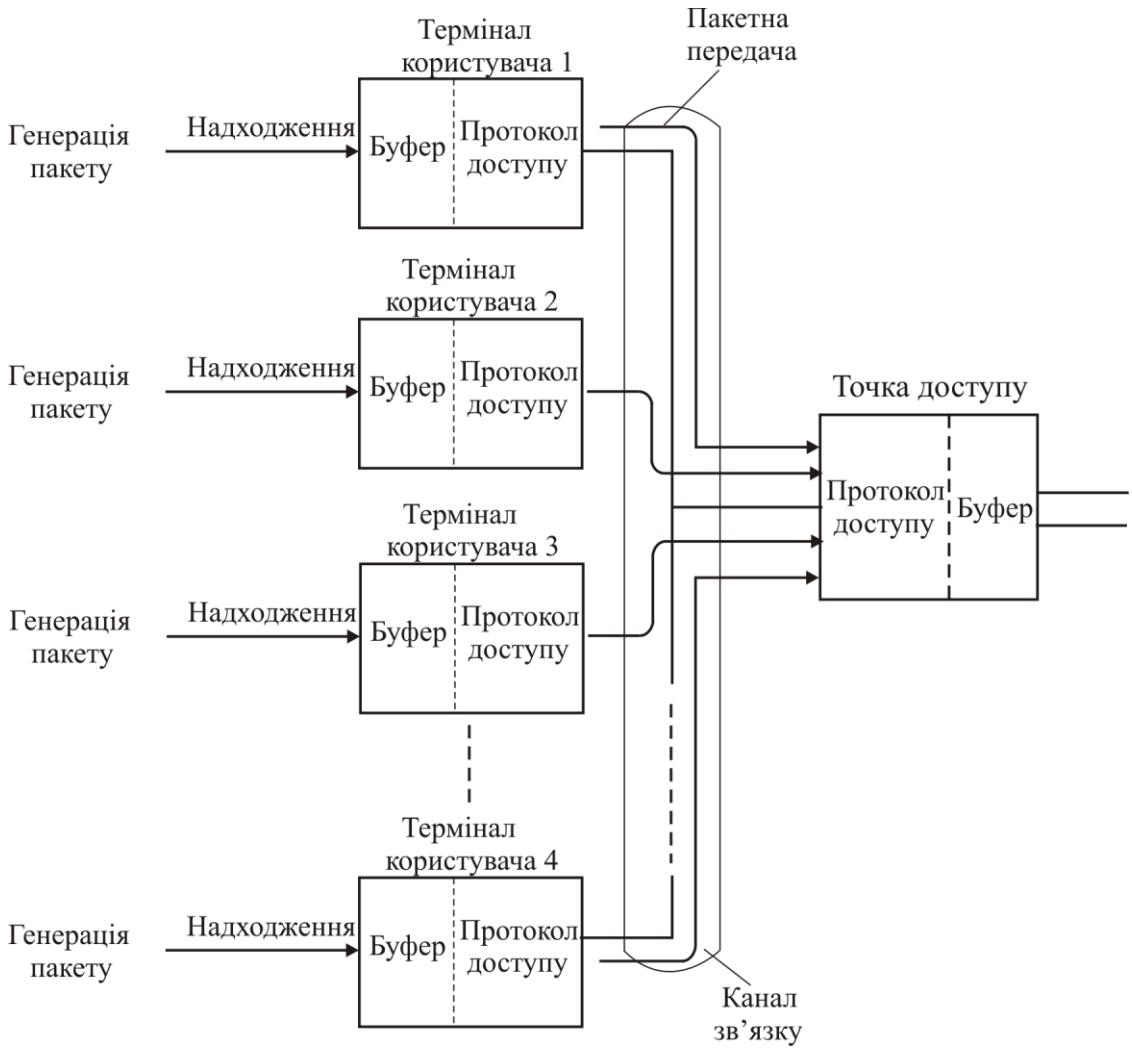

Рисунок 2.1 – Узагальнена схема телекомунікаційної системи з пакетною передачею

Припустимо, що характеристики терміналів усіх користувачів однакові. До того ж, будемо вважати, що кожен термінал має буфер. Коли відбувається генерація відповідним користувачем пакета, то він зберігається у буфері. Потім пакети, що зберігалися у буфері передаються відповідно до надходження пакетів у буфер. Тобто, буфер працює за алгоритмом FIFO (першим прийшов – перший вийшов). Сам буфер може підрозділятися на два типи: буфер з нескінченою пам’яттю і буфер з кінцевою пам’яттю.

Якщо використовується буфер з кінцевою пам’яттю і пам’ять заповнена, то пакет сформований у даного користувача втрачається. Такий варіант трактується як блокування виклику, але він відрізняється від спотворень пакета під час передачі до точки доступу. Окрім того, якщо кількість терміналів нескінчена, то таку модель називають моделлю з нескінченою кількістю джерел-терміналів.

З іншого боку, модель для якої кількість користувачів обмежена, ще називають моделлю з кінцевою кількістю джерел–терміналів.

2.1.1 Канал зв’язку

Суттєва різниця між провідними і безпровідними мережами полягає саме у каналі зв’язку. Визначимо основні ознаки і відмінності провідного і безпровідного каналів зв’язку.

Для провідних мереж ніякого спотворення сигналу у спільному середовищі (каналі зв’язку) не відбувається і потужність сигналів, що надходять до точки доступу від терміналів користувачів не змінюється. Саме з цього фундаментального положення здійснюється оцінка роботи протоколу доступу для провідної мережі

Для безпровідних систем зв’язку характеристики середовища (каналу зв’язку) є варіабельними у часі.

По–перше необхідно враховувати втрати розповсюдження, які залежать від відстані між терміналом і точкою доступу, а також враховувати

ефект затінення, який виникає через наявність перешкод на шляху розповсюдження сигналу.

Втрати розповсюдження і затінення в програмному комплексі пропонується моделювати з наступних міркувань.

Для втрат розповсюдження пропонується розглядати монотонне зменшення прийнятого у точці доступу сигналу під час збільшення відстані між терміналом і точкою доступу. Математично, звичайно, втрати розповсюдження, тобто зменшення потужності сигналу, подають через коефіцієнт пропорційності $\gamma^{-\alpha}$, де γ – медіанне значення прийнятого сигналу (для великомасштабних завмирань) і α – коефіцієнт затухання. Як правило, в залежності від місцевості значення α знаходиться у межах від 2 до 5 [8].

Окрім того, сигнал, що передається, поширюється в умовах багатопроменевого розповсюдження радіохвиль і надходить до точки прийому за різними шляхами. При цьому під час розповсюдження він підлягає впливу від таких фізичних ефектів як дифракція, перевідбиття і розсіювання. В результаті прийнятий сигнал у точці прийому набуває флуктуацій за амплітудою, фазою та кутом надходження. Цей ефект від багатопроменевого розповсюдження отримав назву федінга. Ці завмирання сигналу трактують як дрібномасштабні флуктуації.

Якщо провести усереднення рівня сигналу на інтервалі декілька десятків довжини хвилі, то отримане значення трактують як медіанне для дрібномасштабних завмирань. Причому це середнє значення також підлягає додатковим флуктуаціям через наявність перешкод, будівель ,пагорбів і т. ін., і такі флуктуації у дрібномасштабному сенсі отримали назву затінення. Математично затінення описується логарифмічно-нормальним законом зі стандартним значенням дисперсії 6…7 дБ [8].

2.1.2 Генерація пакетів

Припускаємо, що генерація пакетів кожним терміналом користувача відбувається випадково і незалежно. Вважається, що за таких умов процес генерації пакетів підлягає Пуасонівському розподілу. Відповідно можна відзначити основні вимоги під час генерації пакетів:

– незалежність, тобто генерація пакету повністю не залежить від попереднього процесу генерації;

– постійність, під якою розуміють однакову ймовірність з'явлення пакету для кожного часового слоту при моделюванні;

– рідкість з'явлення пакетів, яку трактують для малого часового інтервалу, а саме, вважатимемо, що ймовірність генерації більш двох пакетів за дуже малий інтервал часу дуже мала.

Крім того, якщо кількість пакетів, що згенерована, підлягає Пуассонівському розподілу, то момент часу, для якого здійснюється генерація пакету також описується законом Пуассона.

2.1.3 Колізія

Як було визначено, колізія виникає, коли два або більше пакетів одночасно передаються у спільному середовищі (рис.2.2), де затемнені ділянки відповідають конфлікту декілька пакетів, що одночасно передаються.

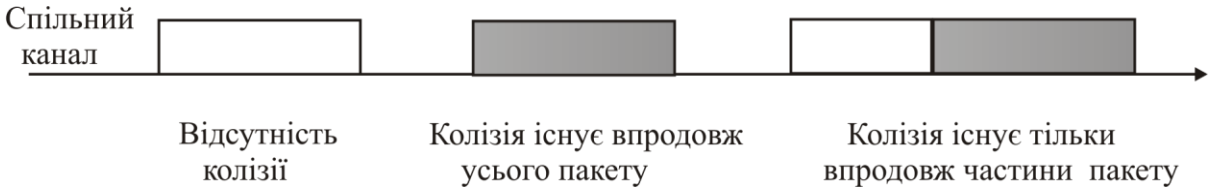

Рисунок 2.2 – Можливі варіанти колізій, які виникають під час пакетної передачі

Особливості обробки пакетів у випадку такого конфлікту для провідних і безпровідних систем наступні:

– для провідної мережі усі пакети, що формуються у спільному середовищі під час колізії спотворюються, оскільки рівень сигналів для усіх пакетів однаковий і, відповідно, пакет вважається втраченим – тобто для системи зв’язку передача пакету не здійснилася. Якщо ж колізія не виникає, то пакет вважається таким, як успішно доставлений до отримувана.

– для безпровідної мережі потужність прийнятого сигналу від кожного користувача залежить від розташування термінала і умов розповсюдження. Тому якщо під час колізії у каналі розповсюджується декілька пакетів, то цілком ймовірна ситуація, коли пакет від найближчого терміналу, тобто, з максимальною потужністю у точці прийому може інколи вважатися переданим, оскільки для нього спотворення мінімальні. Звичайно таку ситуацію з технічної точки зору трактують як ефект захоплення. З іншого боку, навіть якщо колізія не виникає, то пакет також може вважатися втраченим, якщо потужність прийнятого сигналу у точці доступу менша за деякий порогів рівень, при якому ще можливий достовірна передача інформації.

Для реальних комунікаційних мереж саме точка доступу вирішує вважати пакет від конкретного термінала успішно доставленим або ні, і результати рішення передаються до терміналу-джерела. Крім того, пакети які не вважаються успішно доставленими передаються знову через деякий часовий інтервал.

2.1.4 Трафік

У програмному комплексі під терміном трафік будемо розглядати повну кількість заново згенерованих пакетів, а також пакетів, що передавалися повторно за визначений інтервал часу, тобто повний інформаційний обсяг, який було введено у першому розділі. Подібно до

аналізу, що проведено у розділі 1, під час моделювання будемо аналізувати нормалізований трафік, який визначається за виразом (1.5), або вводячи загальний час передачі усіх пакетів $T_t=b\lambda$ для нормалізованого трафіка можна записати [4]:

$$G = \frac{T_t}{R}.$$

Якщо не відбувається генерації жодного пакету, то, очевидно, що G=0.

2.1.5 Пропускна здатність

Під пропускною здатністю у програмі приймається повна кількість пакетів, що успішно доставлені до точки доступу за визначений час. Також аналіз будемо проводити у термінах нормованої пропускної здатності, яку визначимо як

$$\rho = \frac{T_б \cdot n}{R},$$

де $T_б$ – кількість інформації (біт), що необхідна для передачі пакету,

n- кількість успішно переданих пакетів за визначений час.

Якщо ніякої генерації пакетів не відбулося, або усі передані пакети втрачені через колізії, то ρ набуває мінімального – нульового значення. Якщо ж усі пакети успішно доставлені до точки доступу, то ρ=1.

2.1.6 Середній час затримки передачі

Інтервал часу впродовж якого відбувається генерація пакету у терміналі користувача, передача його до точки доступу і прийом переданого пакету у точці доступу будемо трактувати як середню затримку передачі. Середня затримка передачі залежить від довжини пакету. Тоді нормалізовану до довжини пакету середню затримку позначимо як D. В принципі, для реальних телекомунікаційних систем, середній час затримки пакетів

залежить від поточного часу генерації пакету і передачі його терміналом користувача, відстані між точкою доступу і терміналом користувача і часу обробки сигналу у точці доступу.

2.1.7 Оцінка якості протоколів доступу

Якість протоколів доступу звичайно оцінюють за трьома введеними фундаментальними параметрами – нормованим інформаційним обсягом або нормованим трафіком, нормованою пропускною здатністю і нормованим середнім часом затримки передачі.

Для ідеального протоколу доступу повинно виконуватися наступне рівняння:

$$\rho = \begin{cases} G & (G < 1) \\ 1 & (G \geq 1) \end{cases}.$$

Але, як показано на рис.2.3, для реальних систем нормована пропускна здатність зростає до деякого порогового значення G під час збільшення нормованого трафіка, а потім пропускна здатність починає зменшуватися під час збільшення G.

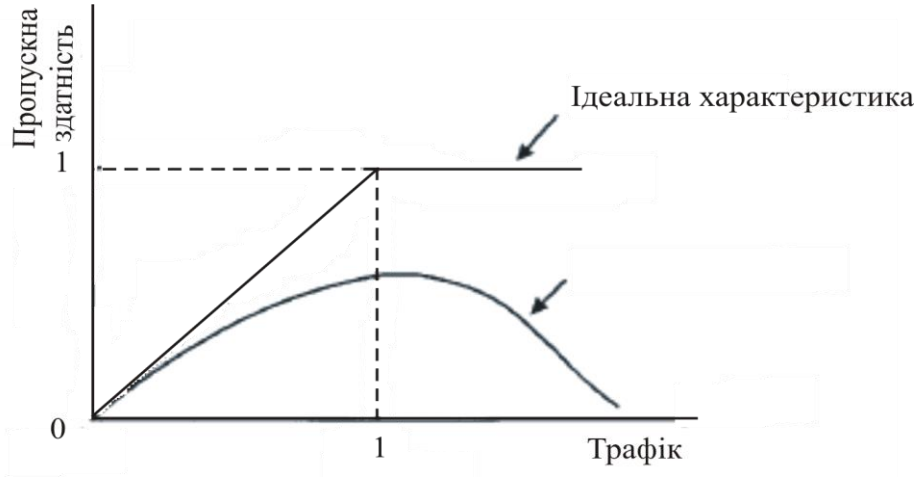

Рисунок 2.3 – Реальна і ідеальна залежності нормованої пропускної здатності від нормалізованого трафіка

Залежності середнього часу затримки і ідеалізованої кривої наведені на рис.2.4. Ідеалізована характеристика середнього часу затримки отримана за припущенням що відбувається ідеальне планування передачі усіх пакетів і ніякого часу на планування не витрачається.

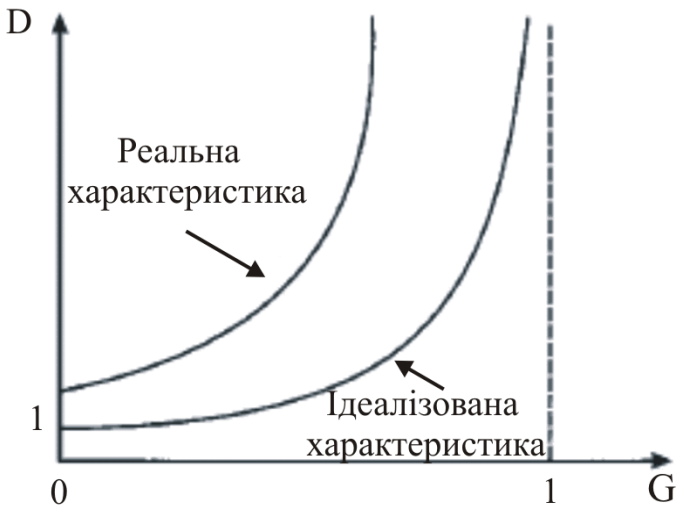

Рисунок 2.4 – Реальна і ідеальна залежності нормованого середнього часу затримки передачі від нормалізованого трафіка

Якщо нормована пропускна здатність більша за одиницю, середній час затримки D суттєво зростає і устромляється до нескінченності.

2.2 Базовий алгоритм програмного комплексу

Структурна схема алгоритму програмного комплексу наведена на рис.2.5 [4].

Рисунок 2.5 – Базовий алгоритм моделювання

Основною метою моделювання є визначення пропускної здатності і затримки передачі з метою порівняння різних протоколів доступу до каналу.

Як видно зі схеми, спочатку алгоритмом передбачається виконання двох незалежних задач: по-перше, це реалізація трафіка, що підлягає

пуасонівському розподілу і по-друге, визначення геометричного місця розташування терміналів користувачів і точки доступу у зоні обслуговування.

Далі необхідно розглянути умови, які відповідають каналам зв'язку провідних і безпровідних мереж. При моделюванні безпровідної мережі припускаємо, що втрати розповсюдження і затінення мають постійне значення.

Процес моделювання закінчується після того, як кількість успішно переданих пакетів досягне необхідного заданого значення. Застосовуючи декілька підпрограм можливо за базовим алгоритмом дослідити різні протоколи доступу з відповідними додатковими змінами.

2.3 Опис головної програми

Повний лістинг головної програми, а також необхідних підпрограм наведено у додатку А. Розглянемо основні процедури , які необхідно виконати у головній програмі. Спочатку охарактеризуємо усі змінні, що будемо використовувати у програмі.

Таблиця 2.1 Параметри і змінні, що використовуються у головній програмі

Позначення змінної	Фізичний сенс
Brate	Бітова швидкість (біт/секунда)
Srate	Символьна швидкість (символ/секунда)
Plen	Довжина пакету у символах
Ttime	Час передачі пакету (секунда)
Dtime	Нормалізована затримка розповсюдження
Alfa	Коефіцієнт затухання

Продовження таблиці 2.1

Sigma	Стандартне значення девіації для затінення
Capture	Наявність ефекту захоплення (0 – присутній, 1 – відсутній)
R	Радіус зони обслуговування
Bxy	Розташування точки доступу
Tcn	Коефіцієнт захоплення (децибели)
Mnum	Кількість терміналів користувачів
Mxy	Розташування терміналів користувачів
Mcn	Відношення сигнал/шум у точці доступу для терміналу, що знаходиться на границі зони (децибел)
Mplen	Довжина пакета у символах
Mstate	Стан терміналу користувача
Mgtime	Час генерації пакету у терміналі користувача (секунда)
Mtime	Час на зміну стану користувача (секунда)
Mstime	Час передачі пакету від терміналу
G	Трафік
Tint	Очікуване значення інтервалу генерації пакету (секунда)
Rint	Очікуване значення інтервалу повторної передачі (секунда)
Spnum	Кількість успішно переданих пакетів

Продовження таблиці 2.1

Spend	Кількість пакетів для закінчення моделювання
Splen	Кількість інформації в успішно переданих пакетах (символ)
Tplen	Кількість інформації для якої здійснювалася спроба передачі (символ)
Wtime	Час затримки передачі (секунда)

Структурно головну програму можна розділити на декілька функціональних блоків.

У першому блоці програми усі змінні, що використовуються як у головній програмі, так і в підпрограмах визначаються як глобальні змінні.. Це робиться з метою скорочення пам’яті, що необхідна для виконання з відповідним збільшенням швидкості моделювання.

Як глобальні змінні обираємо такі параметри системи зв’язку:

– по-перше, вводимо змінні, що характеризують стан користувачів **STANDBY** – ОЧІКУВАННЯ, **TRANSMIT** – ПЕРЕДАЧА, **COLLISION** – КОЛІЗІЯ, **PERMIT** – ДОЗВІЛ НА ПЕРЕДАЧУ;

– по-друге визначаються, як глобальні змінні, параметри системи зв’язку, що відповідають технічному завданню: символьна швидкість – **Srate,** довжина пакету – **Plen,** час передачі пакету **– Ttime**, час затримки розповсюдження – **Dtime**, кількість терміналів користувачів – **Mnum**, час передачі пакету – **Mstime**, стан терміналу користувача – **Mstate;**

– по-третє, задаються очікуване значення часу генерації нового пакету – **Tint** і

очікуване значення часу повторної передачі пакету **– Rint;**

– по-четверте, як глобальні змінні, розглядаються параметри, які характеризують якість протоколу множинного доступу: кількість успішно

переданих пакетів – **Spnum,** кількість інформації у символах в успішно переданих пакетах – **Splen,** кількість інформації у символах для якої здійснювалася спроба передачі – **Tplen,** середній час затримки передачі – **Wtime**.

Відповідний блок програми у термінах MATLAB набуває такого вигляду:

```
global STANDBY  TRANSMIT  COLLISION  PERMIT
global Srate  Plen  Ttime  Dtime
global  Mnum  Mplen Mstime  Mstate
global  Tint  Rint
global  Spnum  Splen  Tplen  Wtime
```

Визначаємо універсальні константи, які визначають процеси в мережі:

```
STANDBY    =0;
TRANSMIT   =1;
COLLISION  =2;
PERMIT     =3;
```

Для кожного протоколу доступу визначаємо своє ім’я підпрограми і в третьому блоці вводяться імена підпрограм для протоколів, що досліджуються. При цьому використовуємо для вибору підпрограм масив, оскільки за такою побудовою з використанням функції Mathlab feval можна легко додавати нові протоколи без ускладнення головної програми:

```
Protocol ={'paloha'  ...% Pure Aloha      : pno=1
           ' saloha'  ...% Slotted Aloha  : pno=2
           ' npcsma'  ...% Np-CSMA     : pno=3
```

В четвертому блоці визначаються параметри для моделювання відповідно до технічного завдання. Так, змінну **tcn** визначаємо як порогове

значення прийнятого сигналу у точці доступу, яке гарантує, що ніякого спотворення або помилки під час прийому не виникає. Тобто, **tcn** – це мінімально можливе відношення сигнал/шум, яке гарантує успішну передачі пакета. Приймаємо його рівним 10 дБ. В програмі трактуємо цю величину як коефіцієнт захоплення.

Змінну **mcn** вводимо як передану потужність сигналу від терміналу і яку задамо у програмі через відношення сигнал/шум у точці доступу за умови розташування терміналу користувача на границі зони обслуговування і коли в каналі проявляються втрати розповсюдження. Приймаємо **mcn**=30 дБ.

Змінна **pno** дозволяє вибрати необхідний протокол для моделювання з масиву відповідних протоколів.

Якщо ефект захоплення не розглядається (capture=0), то моделюється ідеальний канал провідної мережі. Якщо ж ефект захоплення включається до моделі (capture=1), то моделювання відповідає безпровідній мережі.

Загальну кількість пакетів, яку необхідно донести до точки доступу (тобто розглядати як успішно передані) і по завершенні якої процес моделювання можна вважати закінченим позначимо як **spend**. Приймаємо це значення рівним 1000.

Файл в якому будуть зберігатися результати моделювання позначимо як **outfile**.

Відповідний блок завдання параметрів на моделювання програми набуває такого вигляду:

```
brate  =512e3;
Srate  =256e3;
Plen=128;
Dtime= 0.01;
alfa  =3;
sigma  =6;
r=100 ;
bxy=(0,0,5);
tcn=10;
Mnum  =100;
mcn=30;
```

```
pno=1;
capture=0;
spend=1000;
outfile= 'test.dat'
```

За заданими у четвертому блоці параметрами у наступному п’ятому розраховуються час передачі пакета як відношення тривалості пакету (у символах) до символьної швидкості. Відношення сигнал/шум у точці доступу визначимо на підставі відомого співвідношення [8]:

$$P_{прм} = P_{пер} \cdot R^{-\alpha}$$

Для розрахунку відношення сигнал шум припускаємо, що усі термінали користувачів розташовані на висоті 0 м, точка доступу піднесена на висоту 5 м (змінна bxy(3)), а рівень вхідних шумів приймачів термінала користувача і точки доступу однаковий.

```
Ttime=Plen/Srate;
Npow=10^(mcn/10)*sqrt(r^2+bxy(3) ^2) ^alfa;
```

Усі параметри , що задані у блоці завдання параметрів зберігаємо у файлі ідентифікаторі **fid** :

```
 fid= fopen(outfile,'w');
fprinf (fid,'Protocol                          =%d\n',pno );
fprinf(fid,'Capture                             =%d\n',capture );
fprinf(fid,'Normalised_delay_time               =%f\n',Dtime );
fprinf(fid,'Bit_rate (bps)                      =%d\n',brate);
fprinf(fid,'Symbol_rate (sps)                   =%d\n',Srate );
fprinf(fid,'Length_of_Packet (sbl)              =%d\n',Plen);
fprinf(fid,'Number_of_mobile                    =%d\n',Mnum );
fprinf(fid,'Transmission_power (C/N)            =%f\n',mcn );
fprinf(fid,'Capture_ratio (dB)                  =%f\n',tcn );
fprinf(fid,'Number_of_Packet                    =%d\n',spend );
```

У сьомому блоці визначаємо розташування терміналів користувачів у зоні обслуговування з радіусом **r**. Реалізація розташування виконується за допомогою підпрограми **position**.

Припускаємо, що розташування усіх терміналів користувачів у зоні обслуговування за декартовою системою координат є випадковим. Таке припущення дозволяє задати затінення між терміналом користувача і точкою доступу випадковим значенням, що розподілено за нормальним законом:

```
mxy=position (r,Mnum,0);
randn('state',sum(100*clock));
mrnd=rand(1,Mnum);
```

У наступному блоці задається нормалізований трафік. Трафік G, що пропонується реалізувати під час моделювання, задаємо циклом за допомогою оператора **for**. Значення G повинно бути меншим за кількість терміналів користувачів. Якщо трафік перевищить кількість користувачів, то процес моделювання закінчується:

```
for G=[0.1:0.1: 2.0]
   if G>=Mnum
      break
   end.
```

Розраховується очікуваний час генерації пакета виходячи з кількості терміналів користувачів.

Якщо припустити ,що генерація пакетів відбувається за розподілом Пуассона, то ймовірність генерації n пакетів за час t може бути подана як [3,4]:

$$P(t) = \frac{e^{-\lambda t}(\lambda t)^n}{n!} \qquad (2.1)$$

Ймовірність того, що жодного пакета не буде згенеровано впродовж часового інтервалу від 0 до t визначиться як:

$$P(t) = e^{-\lambda t} \tag{2.2}$$

Тоді можна визначити ймовірність генерації першого пакету після часового інтервалу t як:

$$p(t) = 1 - e^{-\lambda t} \tag{2.3}$$

Тоді, у варіанті застосування такого розподілу для протоколу доступу, як поточний час t можна вважати час передачі пакету T_{time}, а параметр λ визначається очікуваним часом генерації пакету $\lambda = 1/T_{int}$. Відповідно (2.3) можна подати у виді:

$$p(t) = 1 - e^{-\frac{Ttime}{Tint}} \tag{2.4}$$

З іншого боку ймовірність передачі пакету через інтервал t можна визначити через повний нормалізований трафік і кількість терміналів користувачів як:

$$p(t) = \frac{G}{M_{num}}, \tag{2.5}$$

тобто можна записати рівність [4]:

$$p(t) = 1 - e^{-\frac{Ttime}{Tint}} = \frac{G}{M_{num}} \tag{2.6}$$

З отриманого рівняння визначається очікуваний час генерації пакету:

$$Tint = -\frac{Ttime}{\ln\left(1 - \frac{G}{M_{num}}\right)}. \tag{2.7}$$

Для моделювання необхідно визначити час генерації пакету. Згідно з (2.4) можна записати

$$x = 1 - e^{-\frac{t}{Tint}}, \tag{2.8}$$

де 0<x<1 - рівномірно розподілене випадкове число. З (2.7), остаточно для очікуваного часу генерації пакета визначаємо:

$$t = -Tint \cdot \ln(1 - x) \tag{2.9}$$

Потім час повторної передачі пакета встановлюється рівним очікуваному часу генерації пакета. Для реальних систем час повторної передачі пакета залежить від протоколу доступу що використовується. Наприклад, для протоколу ALOHA з виділенням часових інтервалів пакети пересилаються у межах 10 слотів.

Як було визначено, основною задачею моделювання є визначення залежності пропускної здатності і середнього часу затримки від значення повного інформаційного обсягу. Відповідно інтервал повторної передачі Rint також описується експоненціальним розподілом, як і час генерації пакетів, тому, приймаємо [4]:

Tint= -Ttime/ log (1-G/Mnum);
Rint=Tint;

У десятому блоці виконується ініціалізація змінних, які характеризують якість роботи протоколу доступу і використовуються під час моделювання:

Spnum=0;
Splen=0;
Tplen=0;

Wtime=0;

Визначається поточний час відповідно до обраної підпрограми моделювання визначеного протоколу доступу:

now_time=feval(char(protocol(pno)),-1);

У наступному блоці формується власне коренева програма, якою виступає цикл, що реалізовано оператором **while.** Конкретний протокол доступу моделюється відповідною підпрограмою.

Фундаментальні положення в процесі моделювання наступні. Стан усіх терміналів користувачів зберігається у змінній Mstate. Тоді під час зміни стану терміналу відбувається повернення до кореневої програми з наданням часу повернення:

next_time=feval(char(protocol(pno)),now_time);.

Якщо загальна кількість пакетів від терміналів користувачів, що передані до точки доступу успішно, перевищить визначену кількість, яка задана у змінній spend=1000, то процес моделювання для заданого трафіка закінчується:

```
if Spnum>=spend
  break
end.
```

У дванадцятому блоці розраховується кількість терміналів користувачів, що передають пакети до точки доступу:

idx=find(Mstate= =TRANSMIT | Mstate= =COLLISION);.

У наступному блоці проводиться оцінка пакетів, які успішно доставлені до точки доступу.

По-перше, таке моделювання проводимо для провідної мережі (коефіцієнт захоплення capture=0).

В попередньому блоці визначається саме випадок колізії, коли два і більше терміналів передають свої пакети. В такому випадку, оскільки, для провідної мережі це однозначно означає конфлікт з спотворенням пакетів, для змінної Mstate присвоюється значення COLLISION.

```
if capture = =0
    if length(idx)>1
       Mstate(idx)=COLLISOIN
   end.
```

Для безпровідної мережі змінна **capture** встановлюється рівною одиниці. За таких умов визначимо успішність доставки пакету до точки доступу. Як було відзначено, що проявлення ефекту захоплення проявляється у тому, що пакет від терміналу користувача, який у точці прийому має найбільший рівень потужності може підлягати подальшій обробці. Для оцінки потужності від кожного терміналу у точці прийому спочатку необхідно розрахувати відстань між точкою доступу і терміналом, що на цей момент передає пакет. Потім у точці доступу необхідно розрахувати відношення сигнал/шум для усіх пакетів від різних користувачів. З цього набору пакетів обирається пакет, який має найбільше значення відношення сигнал/шум. Для обраного пакету знову розраховується миттєве значення сигнал/шум, а сигнали від інших терміналів розглядаються як шум.

Якщо розраховане знамення сигнал/шум більше за порогове значення, вважається що дані пакету успішно передані до точки доступу і результат зберігається у змінній Mstate. Але, якщо розраховане значення сигнал/шум менше за порогове значення, то усі пакети вважаються втраченими через

колізію і результат колізії також зберігається у змінній Mstate. Тобто значення Mstate = TRANSMIT в процесі передачі означає успішну передачі пакету, у той час як Mstate = COLLSION свідчить про трату пакетів через конфлікт:

```
else
   if   length(idx)>1
        dxy=distance(bxy,mxy(idx,;),1);
        pow=mpow*dxy.^-alfa.*10. ^(sigma/10*mrnd(idx));
        [maxp no]=max(pow);
        if    Mstate(idx(no))== TRANSMIT
              if length(idx)==1
                    cn=10*log10(maxp);
              else
                    cn=10*log10(maxp/sum(sum(pow)-maxp+1));
              end
              Mstate(idx)== COLLISION
              if cn=tcn
              Mstate(idx(no)) = TRANSMIT
    else
              Mstate(idx)== COLLISION
     end
  end
end
```

Лічильник часу збільшується кожного разу, коли кожного терміналу користувач змінюється (тобто відбувається генерація нового пакету

```
now_time=next_time;.
```

По закінченні симуляції для заданого значення трафіку G результати моделювання – середній трафік, пропускна здатність і середня затримка передачі повинні висвітлюватися на екрані зі збереженням цих даних у файлі. Середній трафік визначається як відношення часу на передачу усіх пакетів до повного часу моделювання. Пропускна здатність визначається як відношення періоду впродовж якого пакети були успішно доставлені до повного часу моделювання [4].

За допомогою підпрограми **theorys** виводяться також значення пропускної здатності і середнього часу затримки передачі , що отримані в результаті теоретичного аналізу. Відповідний блок набуває такого вигляду:

```
traffic =Tplen/Srate/now_time;
ts = theorys(pno,traffic, Dtime);
fprintf(fid,′%f\t%f\t%f\t%f\t%f\t%f\t%f\n’,G,now_time...
,Splen/Srate,Tplen/Srate,Wtime,Tint,Rint);
fprintf(′G=%f\tS=%f\tTS=%f\n′,traffic,Splen/Srate/now_time,ts);.
```

По закінченню результатів моделювання для заданого значення трафіка G файл в якому зберігалися результати моделювання закривається і результати виводяться на екран дисплея

```
fclose(fid);
graph(outfile);.
```

2.4 Опис підпрограм, які необхідні для функціонування головної програми

2.4.1. Підпрограма розташування терміналів користувачів

Розташування точки доступу і терміналів користувачів у зоні обслуговування реалізується в підпрограмі position.m. Повний лістинг підпрограми наведено у додатку А.

Геометрична модель розташування терміналів користувачів і точки доступу, що реалізована у підпрограмі position подана на рис.2.6 [4].

Вхідними аргументами для підпрограми виступають радіус кругової зони обслуговування r, кількість терміналів користувачів n, що випадково розташовані у межах зони з радіусом r і h–висота. Центр зони розглядається як початок координат (0,0).

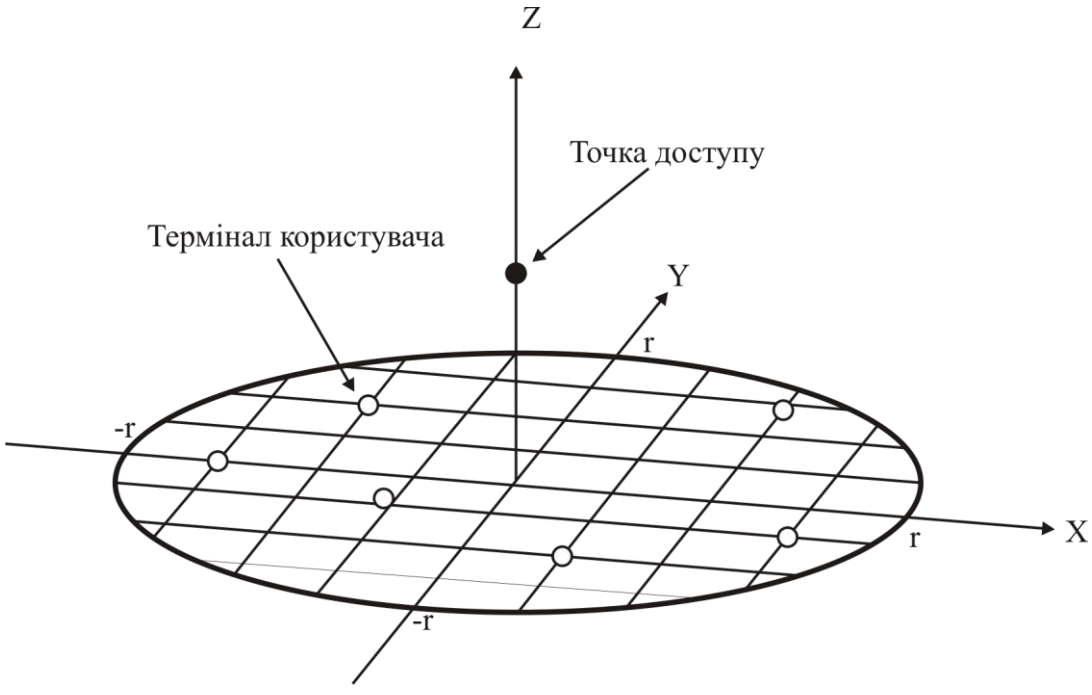

Рисунок 2.6 – Геометричне подання розташування терміналів користувачів у зоні обслуговування

Розташування усіх терміналів користувачів у межах зони повинно бути довільним. Висота кожного терміналу задається значенням параметра h. Якщо встановлено значення h=1, то висота розташування кожного терміналу обирається випадково у діапазоні 1…4. Вихідна інформація про розташування терміналів користувачів подається у вигляді матриці розміром n*3^.

2.4.2 Підпрограма розрахунку відстані між точкою доступу і терміналом користувача

Обчислення відстані між конкретним терміналом і точкою доступу реалізується у підпрограмі distance.m [4]. Вхідними аргументами для підпрограми виступають координати точки доступу – bstn, координати конкретного терміналу користувача – mstn і масштабний коефіцієнт sc1. Координати як точки доступу, так і терміналів користувачів задаються відповідними координатами у площинах x, y, z відповідно до рис.2.6. Якщо масштабний коефіцієнт sc1 рівняється одиниці, то відстань між точкою доступу і терміналом користувача визначається безпосередньо визначеними координатами. Якщо ж значення sc1 відмінно від одиниці, то відбувається збільшення відстані між точкою доступу і терміналом користувача у sc1 раз.

2.4.3 Підпрограма виводу результатів теоретичного аналізу

Для порівняння результатів моделювання і результатів теоретичного аналізу передбачається побудова графічних залежностей для кожного з протоколів у відповідності з результатами теоретичного аналізу, що проведено у першому розділі. Результати теоретичного аналізу моделюються у підпрограмі theorys.m.

Вхідними аргументами програми виступають номер протоколу – no, заданий трафік і нормалізована затримка передачі. Для no = 1, 2, 3, 4

виводяться результати для чистої схеми ALOHA, ALOHA з виділенням часових інтервалів (слотована ALOHA) CSMA і слотована схема ISMA. Задаючи значення g і a проводиться розрахунок теоретичного значення пропускної здатності.

2.4.4 Підпрограма виводу результатів моделювання

Вивід результатів моделювання відбувається за допомогою підпрограми graph.m.

Ця програма реалізує вивід графічних залежностей між трафіком і пропускною здатністю, а також між трафіком і середнім часом затримки передачі. Вхідним аргументом graph.m. виступає змінна filename, яка указує ім’я файла, в якому зберігаються результати моделювання.

2.5 Моделювання чистої схеми ALOHA

Як було показано у першому розділі для протоколу ALOHA ніякого планування передачі не відбувається. Перед початком передачі усі користувачі не мають ніякого уявлення про зайнятість каналу. Відповідно передача конкретним терміналом відбувається відразу після з’явлення інформації для передачі. Принцип роботи протоколу ALOHA, який реалізовано в програмному комплексі зображено на рис.2.7 [2,3,4].

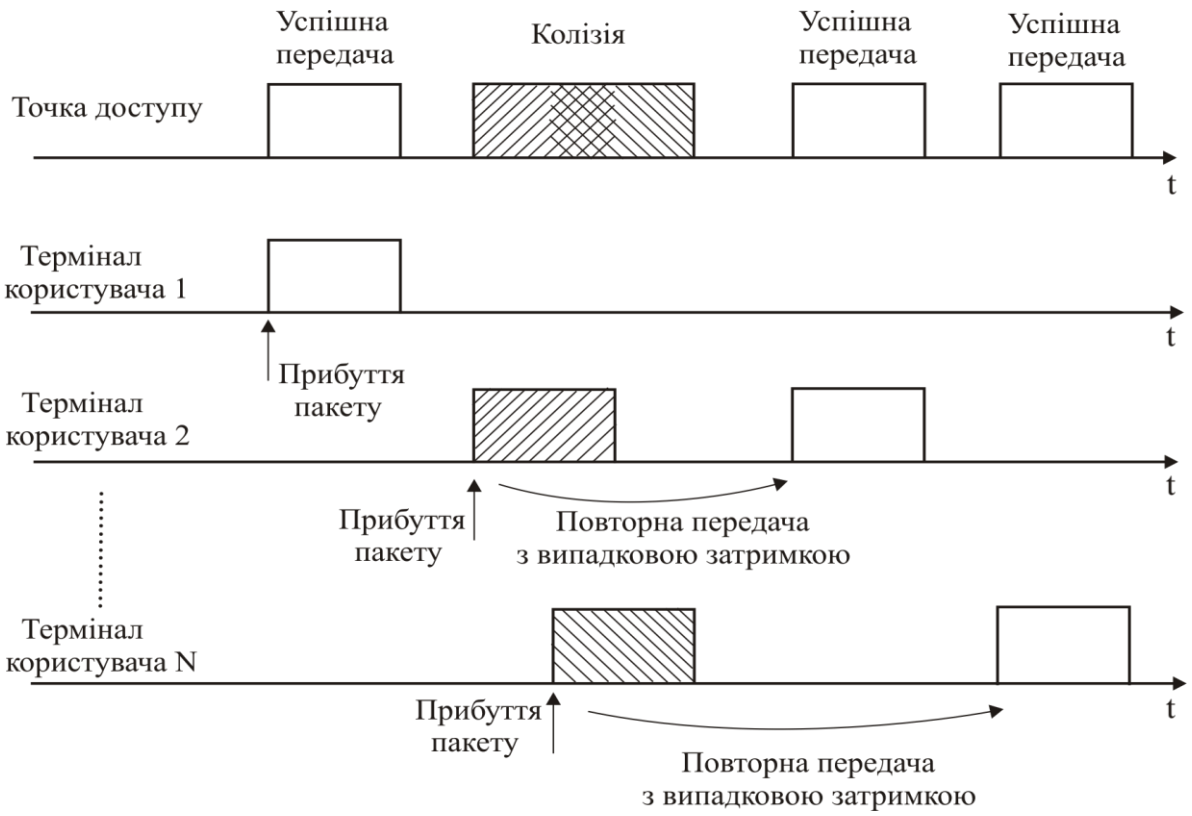

Рисунок 2.7 – Принцип роботи протоколу ALOHA

На рис.2.7 відображено також момент з’явлення колізії між другим і N–им користувачем і механізм повторної передачі з випадковою затримкою випадку виникнення колізії.

Більш детально механізм виникнення колізії зображено на рис.2.8. З аналізу рис.2.8 можна зробити висновок, що за умови фіксованої довжини кожного пакету і часу передачі пакету T, то пакет може вважатися успішно переданим до точки доступу, якщо жоден з інших користувачів не почне передачу пакета впродовж інтервалу 2T, тобто від моменту часу t_i-T до моменту часу t_i+T, як це показано на рис.2.9.

У 1 розділі показано, що за таких умов пропускна здатність визначається виразом (1.10).

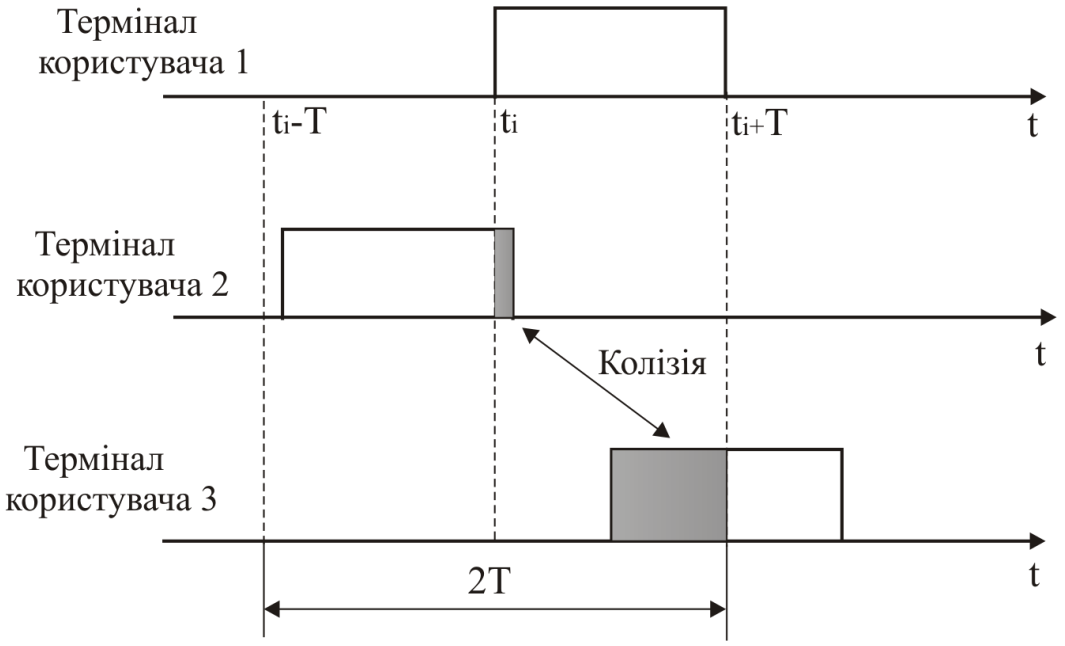

Рисунок 2.8 – Умови виникнення колізії

2.5.1 Підпрограма моделювання протоколу ALOHA

Моделювання роботи чистої схеми ALOHA реалізовано у підпрограмі paloha.m. Повний лістинг програми наведено у додатку Б. Вхідним аргументом програми виступає змінна now_time, яка характеризує поточний час. Вихідним параметром програми є змінна next_time, яка надає інформацію про час зміни статусу кожного з терміналів користувачів після виконання функцій протоколу ALOHA.

В таблиці 2.2 наведені параметри, які характеризують основні умови під час моделювання.

Таблиця 2.2 Умови моделювання протоколу ALOHA

Назва змінної	Фізичний сенс	Значення
r	Радіус зони обслуговування	100 м
bxy	Висота розташування точки доступу	5м

Продовження таблиці 2.2

Mnum	Кількість терміналів	100
Srate	Символьна швидкість	256 ксимвол/секунда
Plen	Довжина пакету	128 символів
alfa	Коефіцієнт затухання	3
sigma	Стандартна девіація для логарифмічно-нормального закону	6 дБ
mcn	Відношення сигнал/шум у точці доступу, коли термінал знаходиться на межі зони обслуговування	30 дБ
tcn	Коефіцієнт захоплення	10 дБ

Подібно до головної програми у підпрограмі paloha.m можна провести певну структуризацію, що дозволяє виділити в ній шість функціональних блоків.

У першому блоці аналогічно до головної програми вводяться глобальні змінні:

global STANDBY TRANSMIT COLLISION PERMIT
global Srate Plen
global Mnum Mplen Mstate
global Tint Rint
global Spnum Splen Tplen Wtime
persistent mgtime, mtime

У другому блоці відбувається ініціалізація стану усіх терміналів користувачів для поточного часу **now_time <0**. Саме в цьому блоці

відбувається розрахунок початку часу генерації першого пакету і завдання довжини пакету.

```
if now_time<0
    mgtime= -Tint*log(1-rand(1,Mnum));
    mtime =mgtime
    Mstate=zeros(1,Mnum);
    Mplen(1:Mnum)=Plen
   mtime(idx)=now_time+Mplen(idx)/Srate;
   next_time=min(mtime) ;
   return
end
```

У третьому блоці по закінченні сеансу пакетної передачі підраховується кількість успішно переданих пакетів, розраховується час затримки і визначається момент генерації нового пакету для усіх терміналів.

Причому, для кожного терміналу генерація нового пакету не починається до тих пір поки не відбудеться успішна передача пакету конкретним терміналом до точки доступу (пакет від кожного терміналу не досягне точки доступу).

```
    idx=find(ntime==now_time&Mstate==TRANSMIT);
    if length(idx)>0
    Spnum= Spnum+1;

    Splen= Splen+Mplen(idx);
    Wtime=Wtime+now_time-mgtime(idx)
    Mstate==STANDBY;

    Wtime=Wtime+now_time-mgtime(idx)
    mgtime(idx)= now_time-Tint*log(1-rand);

    mtime(idx)= mgtime(idx) ;
```

end

У четвертому блоці після закінчення сеансу пакетної передачі у разі невдалої спроби передачі пакету проводиться обчислення часу повторної передачі пакету для усіх терміналів, що прийняли участь у колізії.

```
idx=find(ntime==now_time&Mstate==COLLISION);
if length(idx)>0
    Mstate(idx)=STANDBY;
    Mtime(idx)=now_time-Rint*log(1-rand(1,length(idx)));
end
```

У п’ятому блоці визначаються усі термінали, які на поточний момент (змінні now_time) здійснюють передачу пакету. Відбувається зміна їх стану на режим передачі – TRANSMIT і проводиться розрахунок кінця передачі.

Потім підраховується кількість переданих пакетів.

```
idx=find(mtime==now_time);
if length(idx)>0
Mstate(idx)=TRANSMIT;
mtime(idx)=now_time+Mplen(idx)/Srate;
Tplen=Tplen+sum(Mplen(idx));
end
```

І, нарешті, у шостому блоці на підставі вибору мінімального значення **mtime**, визначається найближчий поточний час **next_time** для якого відбувається зміна статусу терміналу користувача

```
next_time=min(mtime);.
```

2.5.2 Результати моделювання

Результатом проведеного моделювання для усіх протоколів доступу є графічні залежності для пропускної здатності і середнього часу затримки як функції нормованого повного інформаційного обсягу – трафіка.

На рис.2.9 наведені залежності пропускної здатності від трафіка для протоколу ALOHA для ідеального провідного каналу (ефект захоплення не розглядається). На рис.2.10 наведені результати моделювання середнього часу затримки передачі для визначених умов.

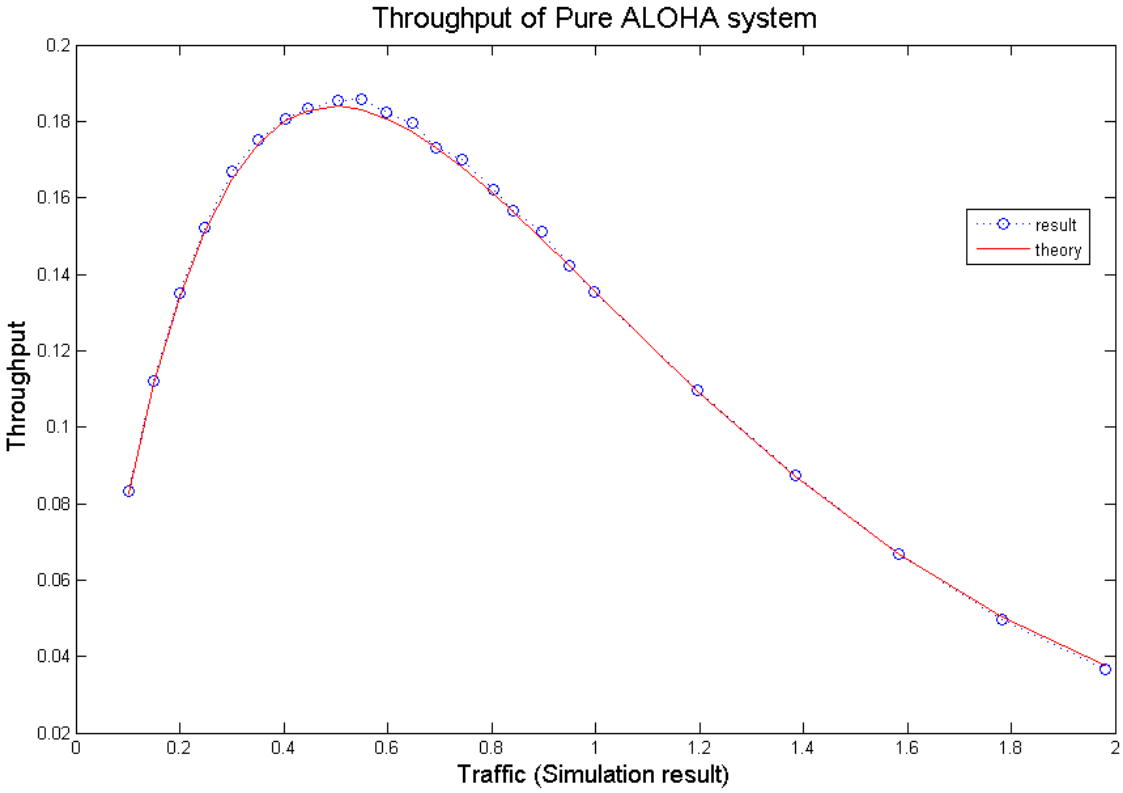

Рисунок 2.9 – Результати моделювання пропускної здатності для протоколу ALOHA провідної мережі (--теоретичний аналіз, % - експеримент)

Результати моделювання і теоретичного аналізу свідчать, що максимальна пропускна здатність обмежена значенням 18,5 %, яке досягається при значенні нормованого трафіка приблизно G= 0,5.

Графічна залежність середнього часу затримки для протоколу чистої ALOHA за результатами моделювання зображена на рис.2.10.

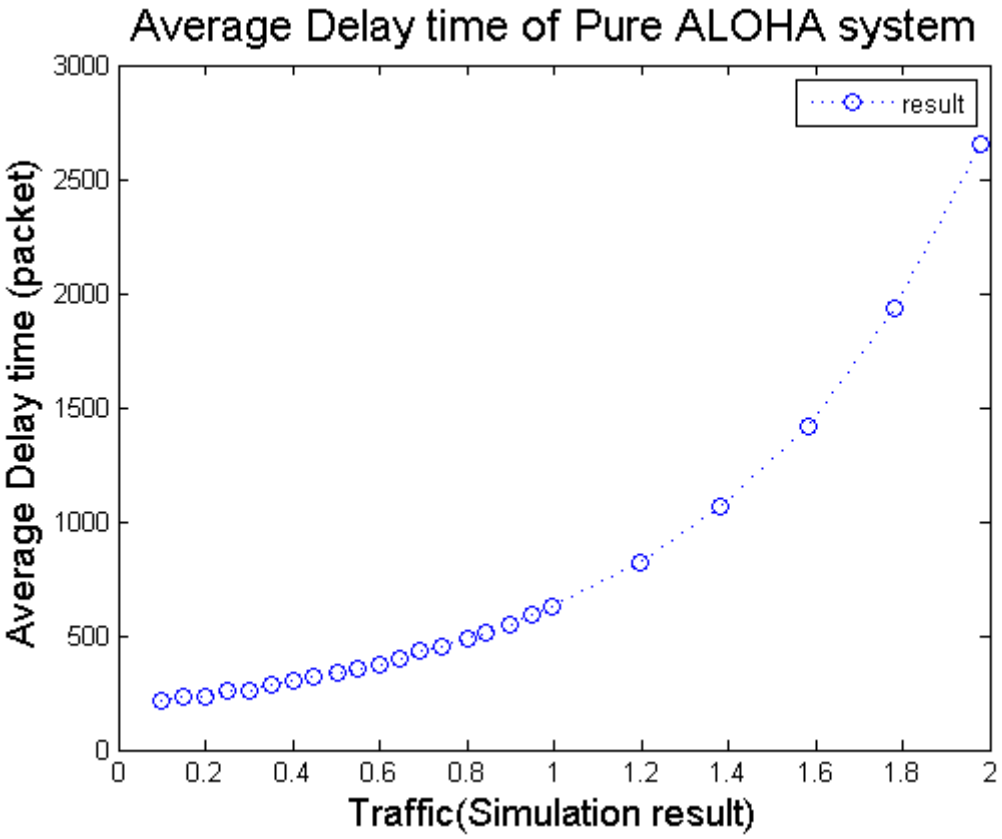

Рисунок 2.10 – Графічна залежність середнього часу затримки протоколу ALOHA для провідних мереж

Аналіз графіків свідчить про суттєве збільшення часу затримки, при збільшенні нормованого трафіка до значення G=2 (затримка досягає значення 3000 пакетів).

Порівняння результатів експерименту і теоретичного аналізу свідчать про адекватне моделювання роботи протоколу ALOHA для провідної мережі зв’язку.

Розглянемо роботу протоколу ALOHA з використанням ефекту захоплення. Такий варіант можливий тільки у безпровідній мережі. У такому разі точкою доступу аналізується потужність прийнятого сигналу від усіх терміналів і обирається сигнал з максимальною потужністю. Якщо рівень відношення сигнал/шум для цього терміналу більший за пороговий рівень,

який задається у програмі параметром tcn=10 дБ, то такий пакет вважається успішно переданим.

Результати моделювання пропускної здатності для протоколу ALOHA з використанням ефекту захоплення наведені на рис.2.11, рис.2.12.

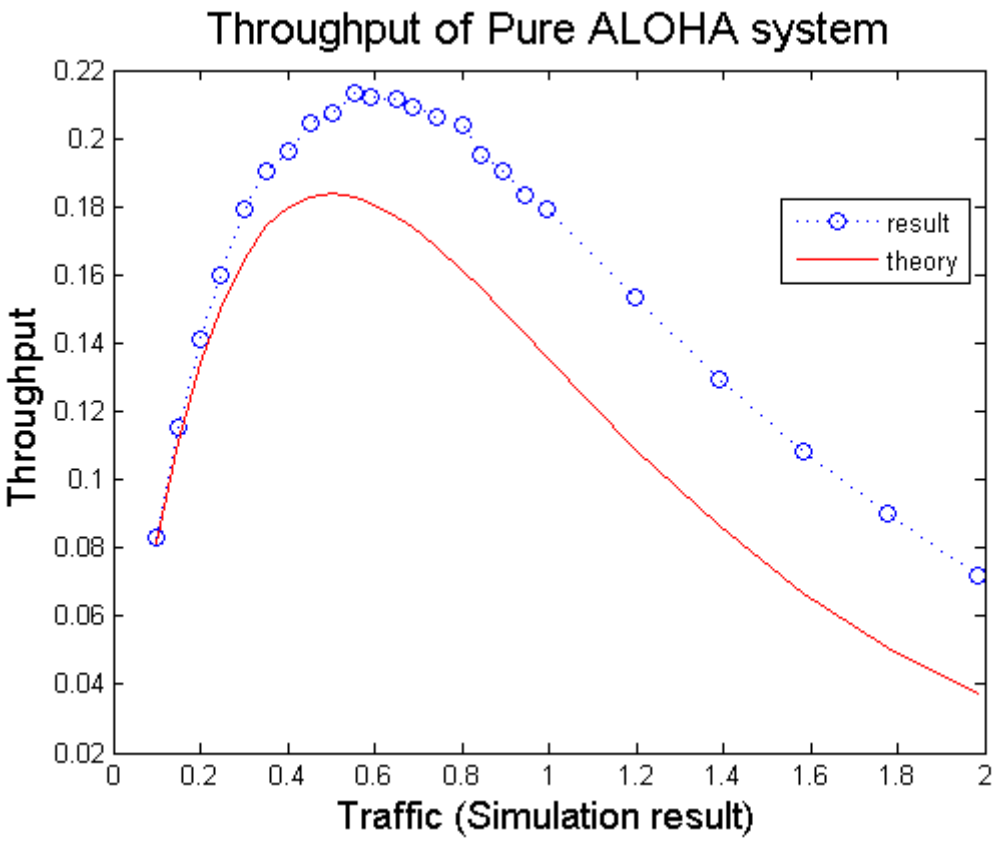

Рисунок 2.11 – Результати моделювання пропускної здатності для протоколу ALOHA безпровідної мережі (--теоретичний аналіз, % - експеримент)

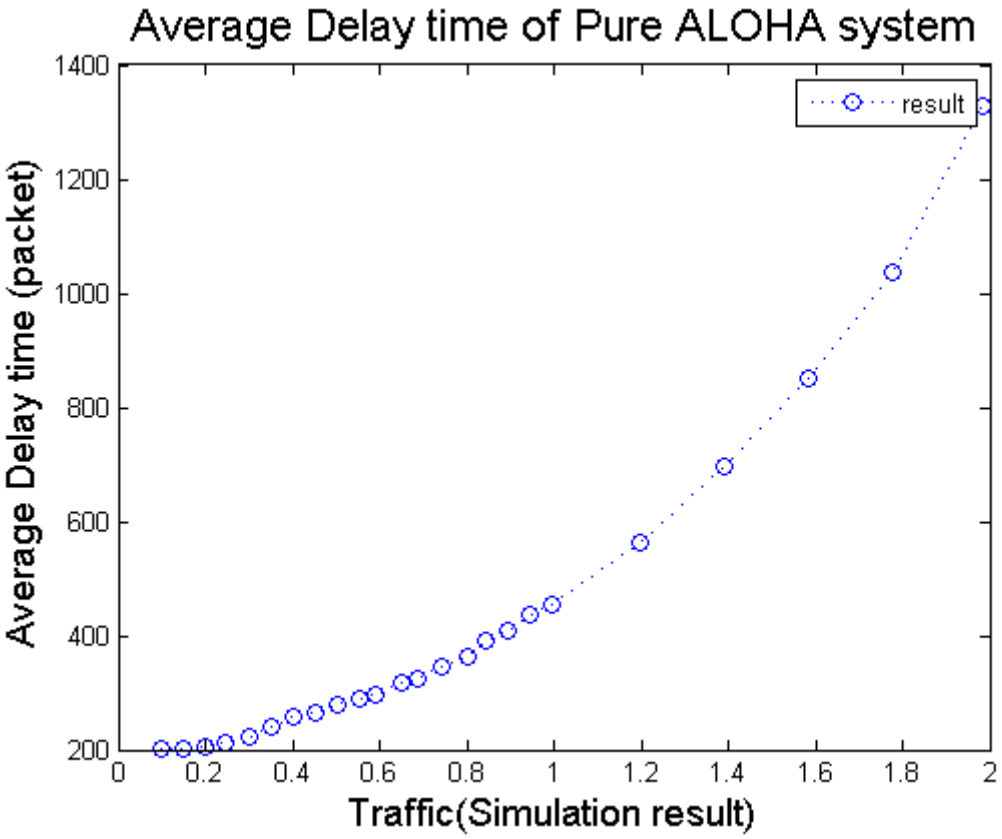

Рисунок 2.12 – Графічна залежність середнього часу затримки протоколу ALOHA для безпровідних мереж

З аналізу графіків для пропускної здатності, виходить, що максимальне значення пропускної здатності збільшується до 21, 5% при значенні нормованого трафіка G=0,55 (для теоретичної залежності максимум S=18,5% відповідає трафіку G=0,5). Середній час затримки з використанням захоплення зменшується при G=2 практично удвічі.

Аналіз отриманих результатів свідчить наступне:

– якщо ефект захоплення не розглядається, то пропускна здатність близька до теоретичного значення навіть для заданої кількості терміналів – 100 користувачів;

– у випадку ж використання захоплення, пропускна здатність каналу зв’язку стає більшою. Додатково також можна відзначити зменшення середнього часу затримки передачі.

Тому можна відзначити, оскільки для протоколу чистої схеми ALOHA колізії виникають досить часто, то використання ефекту захоплення дозволить збільшити пропускну здатність каналу зв’язку.

2.6 Моделювання протоколу ALOHA з виділенням часових інтервалів

Модифікація цього протоколу полягає у тому, що повідомлення можуть бути переданими тільки впродовж часового слоту, що розташований між двома синхронізуючими імпульсами. Причому передача пакету може відбуватися тільки на початку часового слоту. Відзначається, що кількість колізій з дотриманням такої роботи зменшується практично у два рази [3].

Принцип дії протоколу зображено на рис.2.13. Пакет згенерований у визначеному часовому слоті передається до точки доступу у наступному слоті. Для успішної передачі пакету до точки доступу кількість пакетів згенерованих в одному слоті не повинна перевищувати одиницю. Якщо в слоті формуються декілька пакетів, то виникає колізія.

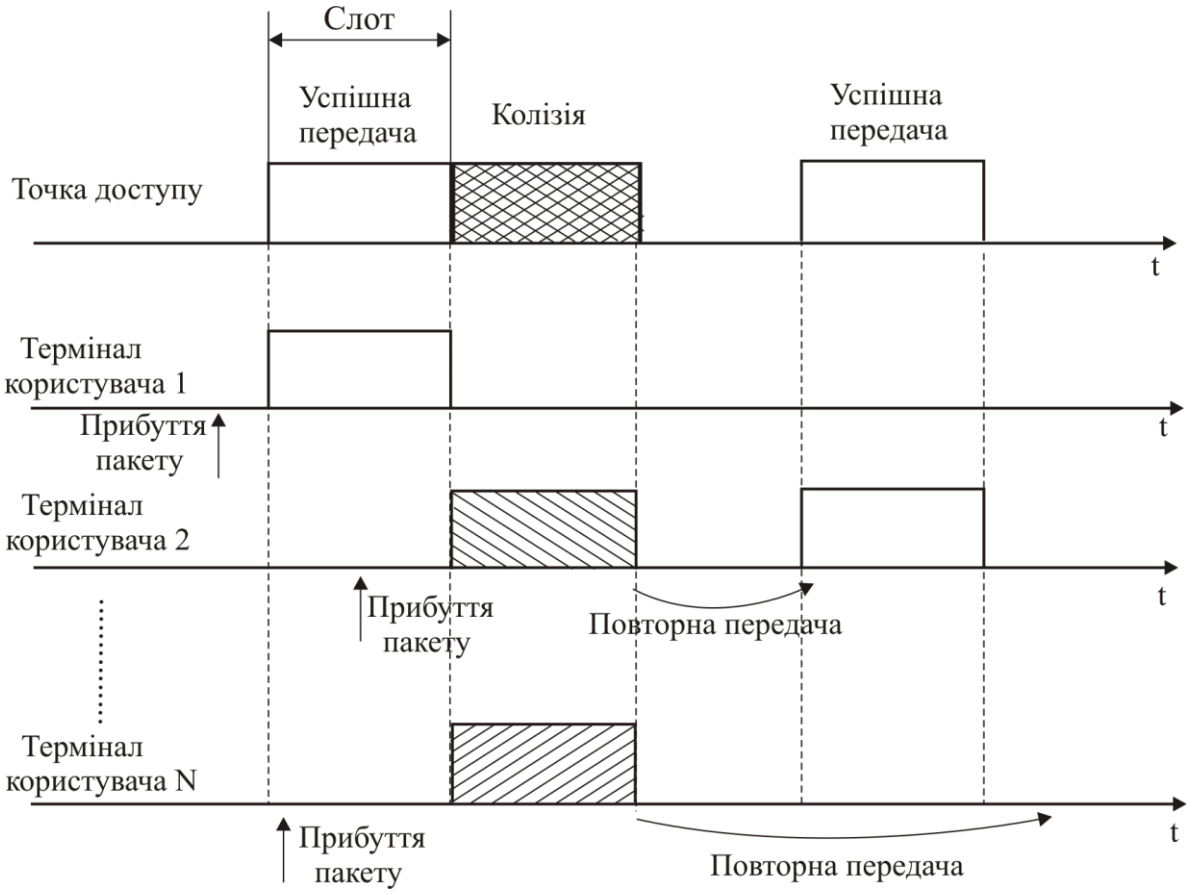

Рисунок 2.13 – Принцип роботи протоколу ALOHA з виділенням часових інтервалів

Більш детально механізм виникнення колізії зображено на рис.2.14

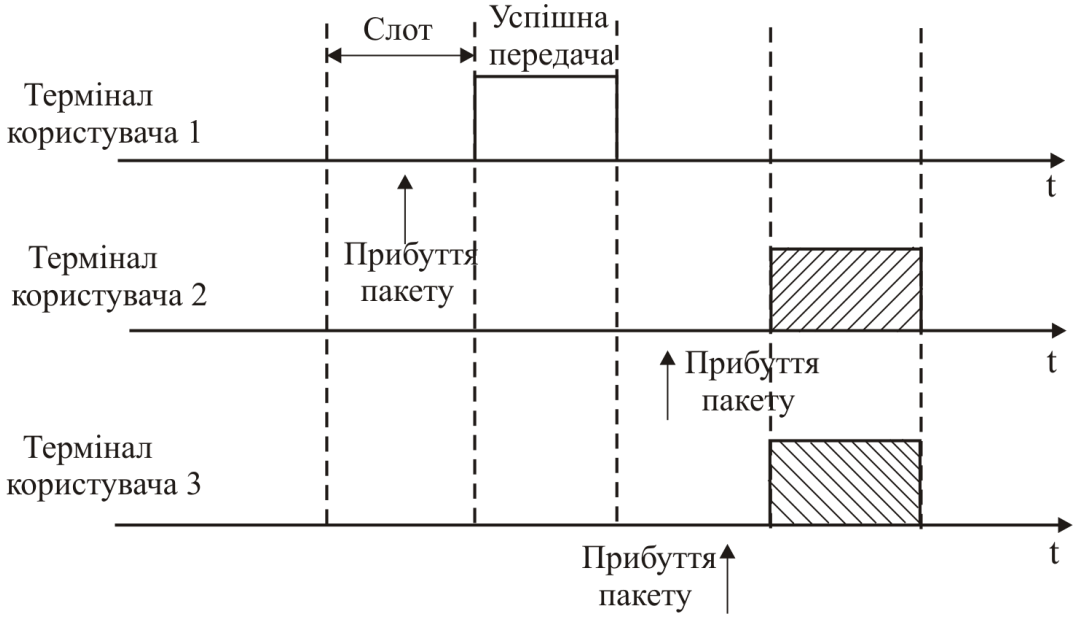

Рисунок 2.14 – Механізм виявлення колізій у протоколі ALOHA з виділенням часових інтервалів

Як було показано у параграфі 1.3.2, пропускна здатність протоколу S–ALOHA визначається виразом (1.11) і досягає максимуму ρ=0,368 при G=1.

2.6.1 Підпрограма моделювання протоколу S–ALOHA

Моделювання протоколу S–ALOHA реалізується за допомогою підпрограми saloha.m, повний лістинг якої наведено у додатку В. В головному підпрограма saloha.m повністю подібна до підпрограми моделювання чистої схеми ALOHA – paloha.m. Різниця, як було визначено вище, полягає у синхронізації передачі пакетів з формуванням часових слотів.

Результати моделювання у вигляді залежностей пропускної здатності і середнього часу затримки від нормованого трафіку для протоколу S–ALOHA наведені на рис.2.15, рис2.16. Як і при моделюванні протоколу чистої схеми ALOHA спочатку моделюється провідний канал зв’язку (ефект захоплення відсутній).

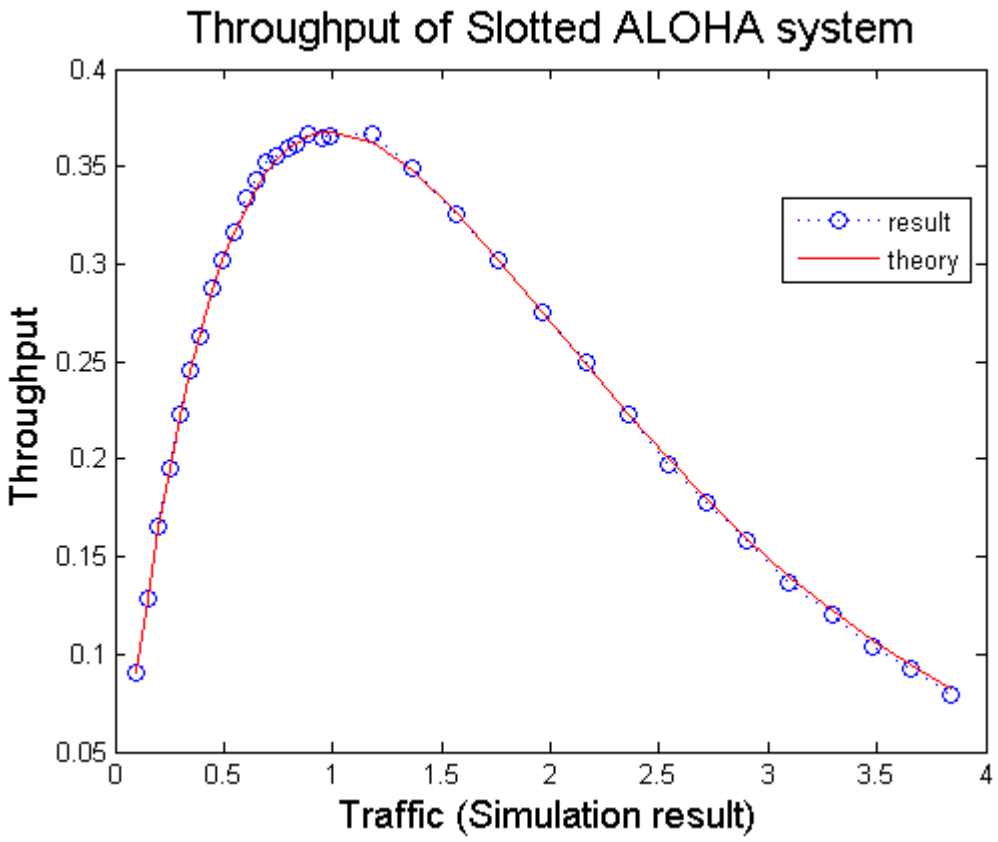

Рисунок 2.15 – Результати моделювання пропускної здатності для протоколу ALOHA провідної мережі (--теоретичний аналіз, %- експеримент)

Результати моделювання підтверджують збільшення пропускної здатності для протоколу S–ALOHA порівняно з протоколом чистої схеми ALOHA.

Максимальне значення пропускної здатності протоколу S–ALOHA за результатами моделювання склало S=0,367 при значенні нормованого трафіка G=1,1 порівняно з S=0,185 при значенні G=0,5 протоколу чистої схеми ALOHA. Тобто протокол S–ALOHA реалізує практично удвічі більшу пропускну здатність для безпровідної мережі. Аналогічний висновок можна зробити і про суттєве зменшення значення середнього часу затримки для S–ALOHA (рис.2.15 і рис.2.16).

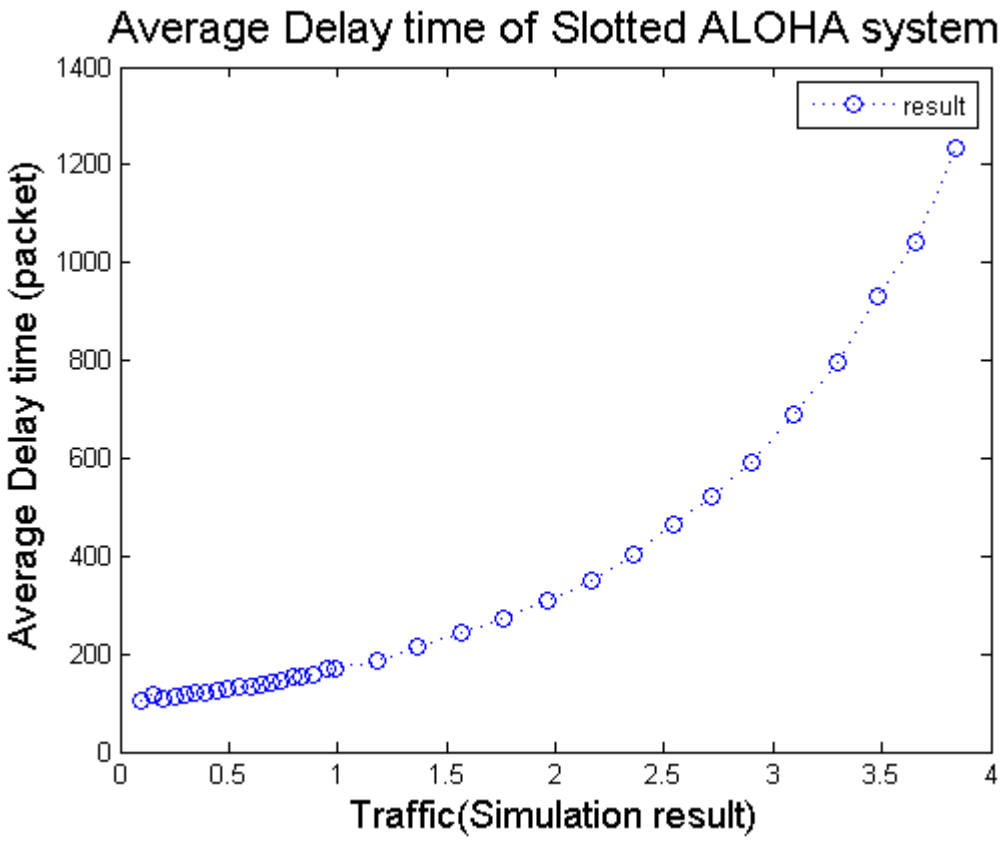

Рисунок 2.16 – Графічна залежність середнього часу затримки протоколу S–ALOHA для провідних мереж

Проведемо моделювання роботи S–ALOHA для безпровідних мереж. Для цього в головній програмі встановимо коефіцієнт захоплення capture=1. Результати моделювання наведені на рис.2.17 і рис.2.18.

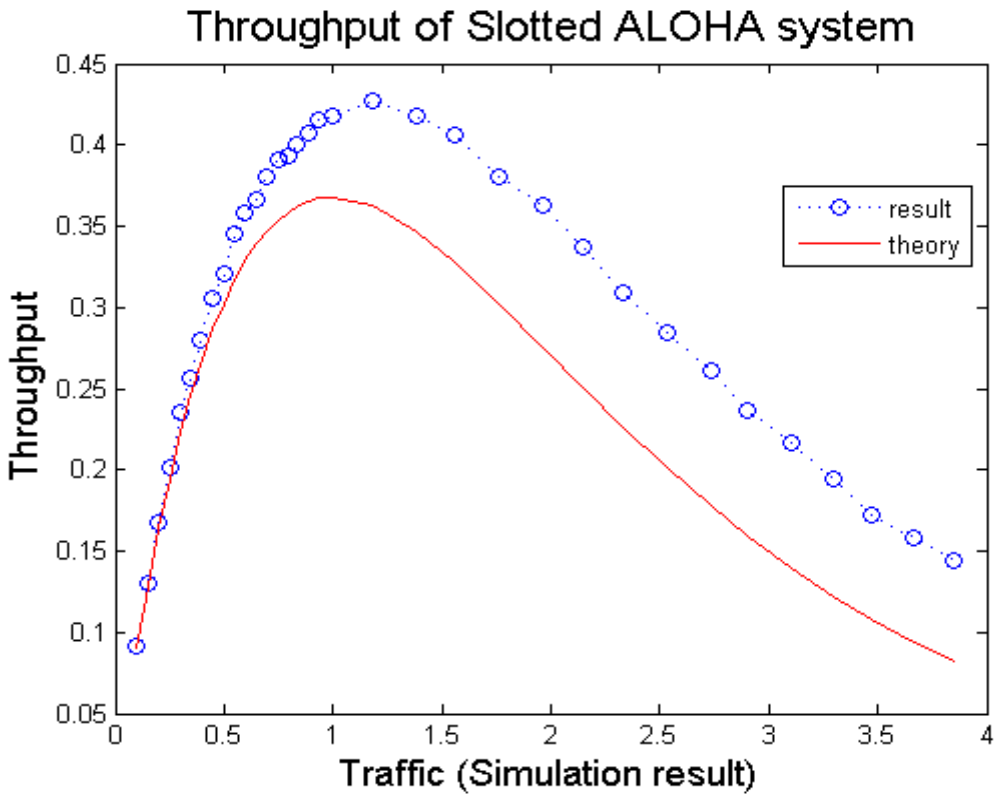

Рисунок 2.17 – Результати моделювання пропускної здатності для протоколу S–ALOHA безпровідної мережі (--теоретичний аналіз, %- експеримент)

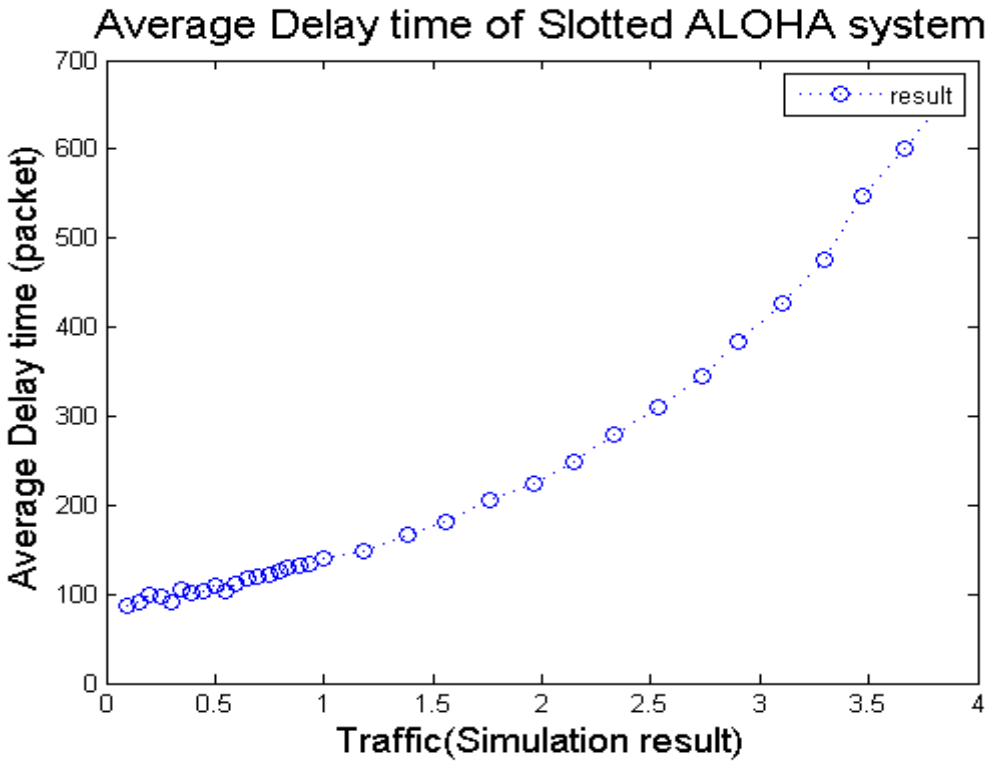

Рисунок 2.18 – Графічна залежність середнього часу затримки протоколу S–ALOHA для безпровідних мереж

Як і для чистої схеми ALOHA можна відзначити проявлення ефекту захоплення на характеристики провідної і безпровідної мереж зв’язку, яке проявляється у збільшенні пропускної здатності і зменшенню часу середньої затримки під час використання ефекту захоплення у безпровідній мережі починаючи зі значення нормованого трафіка G=1.

2.7 Протокол множинного доступу з детектуванням несучої CSMA

Власне назва протоколу пояснюється тим фактом, що усі термінали користувачів контролюють наявність несучого коливання у каналі зв’язку. Саме з виявлення несучого коливання термінал користувача може встановити наявність передачі інформації іншими користувачами, оскільки при пакетній передачі термінал користувача формує несуче коливання тільки на період передачі пакету.

Якщо несуча у каналі виявлена, то на цей момент канал вважається зайнятим, якщо ж несуча не виявлена, то канал вважається вільним. Тобто, протокол CSMA фактично визначає порядок організації передачі пакетів як результат детектування несучої.

Якщо несуча виявлена і канал вважається зайнятим, то необхідного передбачити заходи для усунення колізій. Протокол ненаполегливого методу CSMA є одним з протоколів, що дозволяє уникнути колізій.

Для цього протоколу під час генерації власних пакетів термінал користувача починає процедуру детектування несучої. Якщо канал вільний, тобто несуча не виявлена, то починається термінова передача пакету до точки доступу. Якщо ж канал виявляється зайнятим, то термінал користувача припиняє процедуру детектування несучої і, через деякий час повторює процес детектування несучої. каналу.

Цей час очікування і є ключовим фактором для реалізації у системі зв’язку високої пропускної здатності.

В принципі сам факт детектування у протоколі не дозволяє повністю уникнути колізії. Однією з виникнення колізії при прослуховуванні несучої є так звана затримка розповсюдження.

Дійсно, в реальних телекомунікаційних системах під час передачі пакету через канал конкретним терміналом інші термінали користувачів сприймають несуче коливання у спільному каналі не миттєво, а через деякий час, який і трактується як затримка розповсюдження. Якщо інші термінали почнуть передачу пакетів саме впродовж часу розповсюдження, то неминуче виникне колізія у точці доступу (рис.2.19) [4]. Затримка часу розповсюдження залежить від відстані між терміналами користувачів.

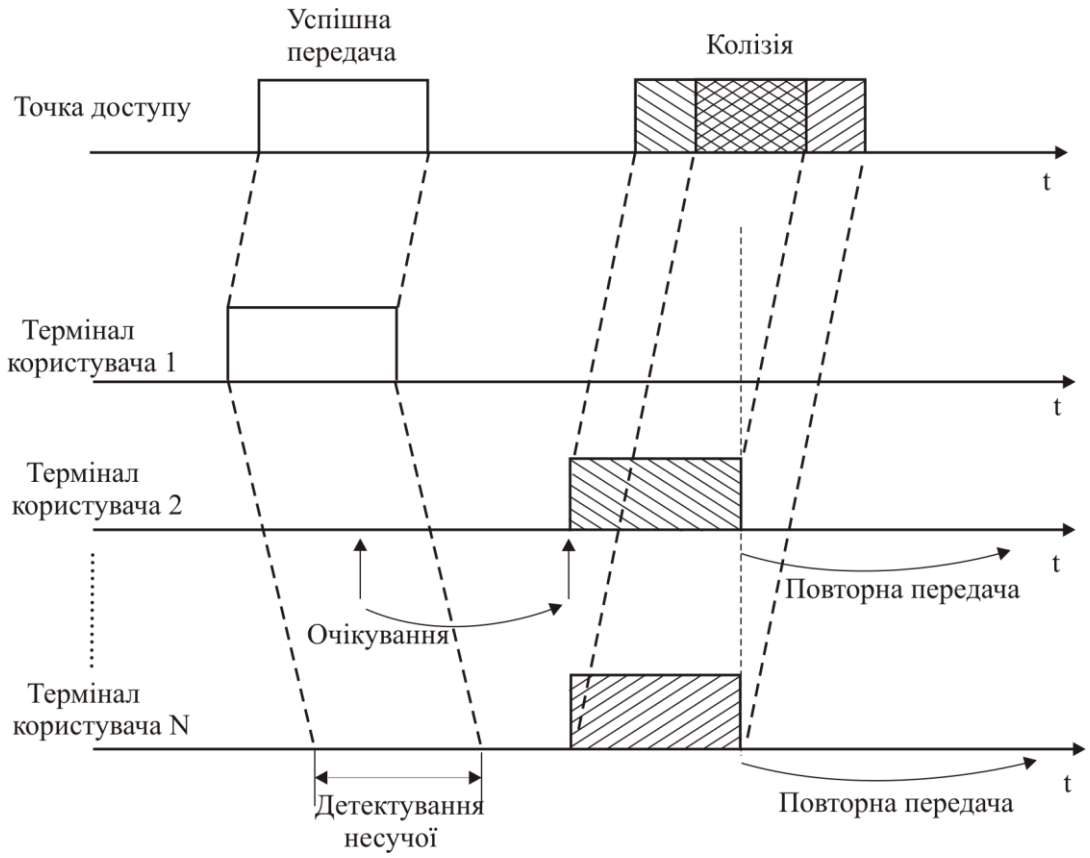

Рисунок 2.19 - Принцип роботи протоколу ненаполегливого методу CSMA

Механізм виявлення колізії більш детально зображено на рис.2.20

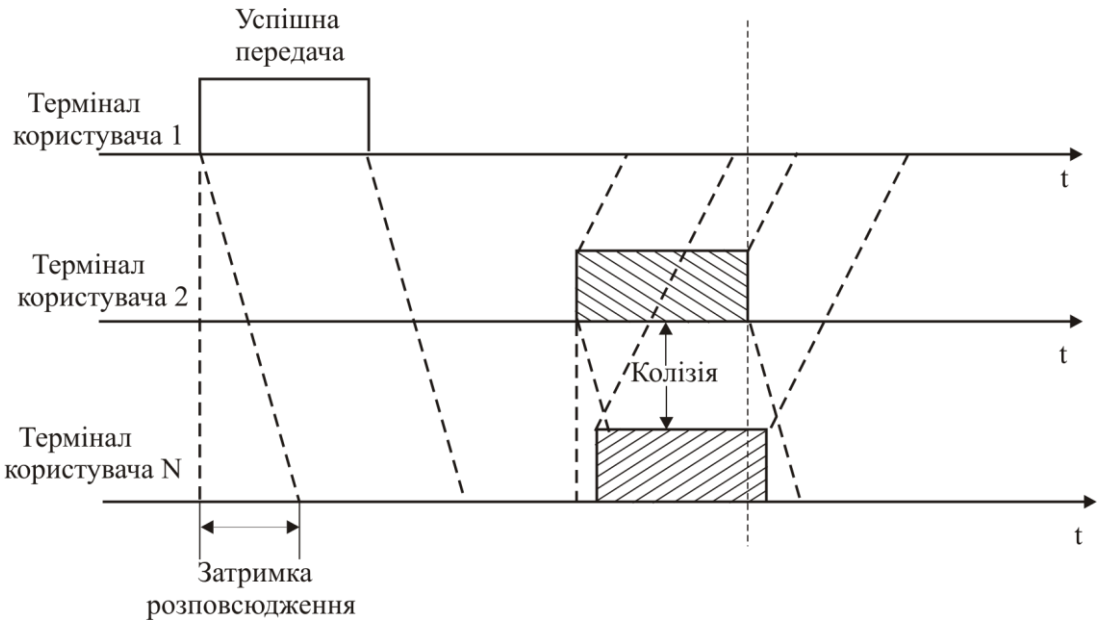

Рисунок 2.20 – Механізм виникнення колізії для протоколу ненаполегливого методу CSMA

У більшості випадків припускається що час затримки розповсюдження однаковий для системи зв’язку і, відповідно, під час пакетної передачі від точки доступу і терміналом формується нормалізований час затримки (затримка нормалізована до періоду). Але, у безпровідній системі процес детектування несучої є не завжди можливим для деяких терміналів навіть під час передачі пакетів, оскільки між терміналами можливе існування певних перешкод (рис. 2.21). Ця проблема відома як проблема схованих терміналів [2,4,5,7].

Рисунок 2.21 – Проблема схованих станцій

Пропускна здатність через трафік визначається як [4]

$$\rho = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}, \tag{2.10}$$

де а – нормалізований час затримки.

Цей вираз для пропускної здатності відповідає ідеальному середовищу передачі і відсутності схованих станцій

2.7.1 Підпрограма моделювання методу CSMA

Моделювання протоколу CSMA реалізовано у підпрограмі npcsma.m. Ця підпрограма в основному подібна до підпрограми моделювання чистої схеми ALOHA – paloha.m. Підпрограму npcsma.m структурно можна поділити на п’ять функціональних блоків подібних до розглянутих у параграфі 2.5.1. Різниця полягає у тому, що перед передачею пакету кожним терміналом виконується детектування несучої. Алгоритм детектування реалізовано у підпрограмі carriersense.m [4]. Якщо канал не зайнятий, то відбувається негайна передача пакету до точки доступу. Якщо ж канал зайнятий , то планується час для передачі пакету. Уся інформація щодо часу передачі пакетів для усіх терміналів користувачів зберігається у глобальній змінній Mstime.

```
idx=find(ntime==now_time&Mstate==STANDBY);
if length(idx)>0
    Tplen=Tplen+sum(Mpleh(idx)) ;
    for ii=1:length(idx) ;
    jj=idx(ii) ;
  if carriersense(jj,now_time)==0
          Mstate(jj)=TRANSMIT;
          Mstime(jj)= now_time;
```

```
                mtime(jj)= now_time+Mplen(jj)/Srate;
        else
      mtime(idx)= now_time-Rint*log(1-rand);

        end
    end
end
```

Повний лістинг підпрограми carriersense.m наведено у додатку Г. У цій підпрограмі до змінної Mstime, яка визначає час передачі пакету додається затримка розповсюдження,що залежить від відстані між терміналами користувачів. Після цього відбувається детектування несучої усіма терміналами. Якщо виявлена несуча. То стан каналу встановлюється як “зайнято” (result=1).

Якщо ж несучу не виявлено, то стан каналу встановлюється як “вільний” (result=0).

2.7.2 Результати моделювання для схеми CSMA

Залежності пропускної здатності і середнього часу затримки наведені на рис.2.22 і рис.2.23 відповідно.

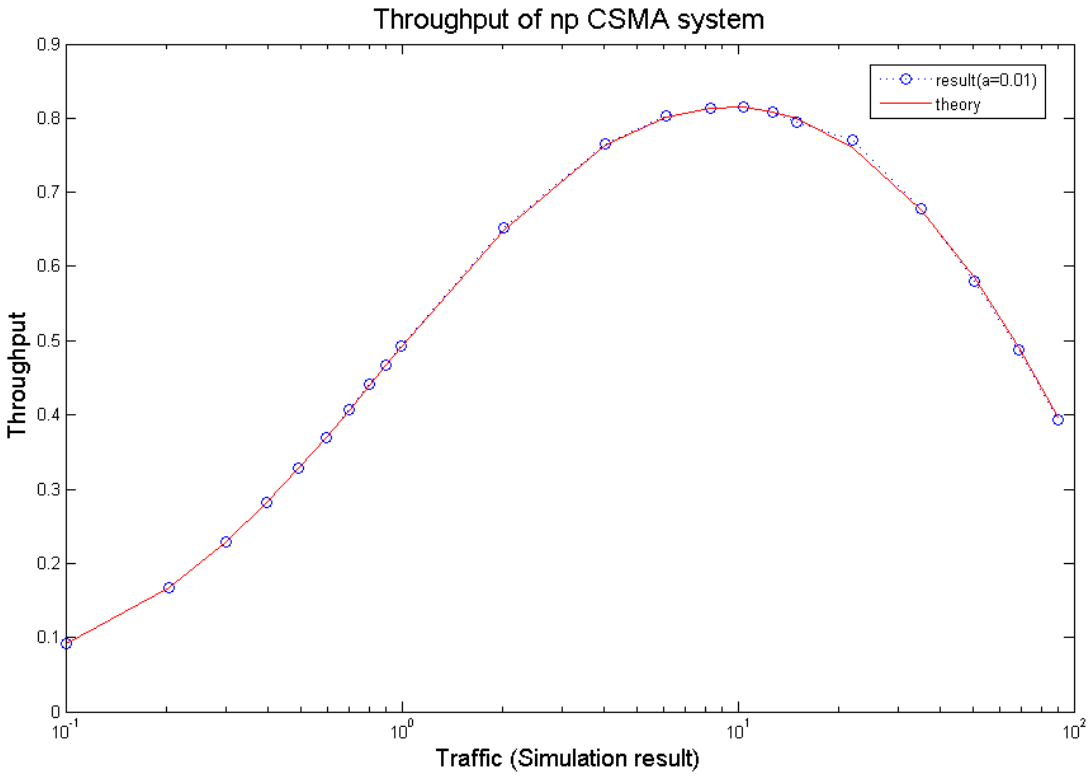

Рисунок 2.22 – Результати моделювання пропускної здатності для протоколу NP–CSMA провідної мережі (--теоретичний аналіз, %- експеримент)

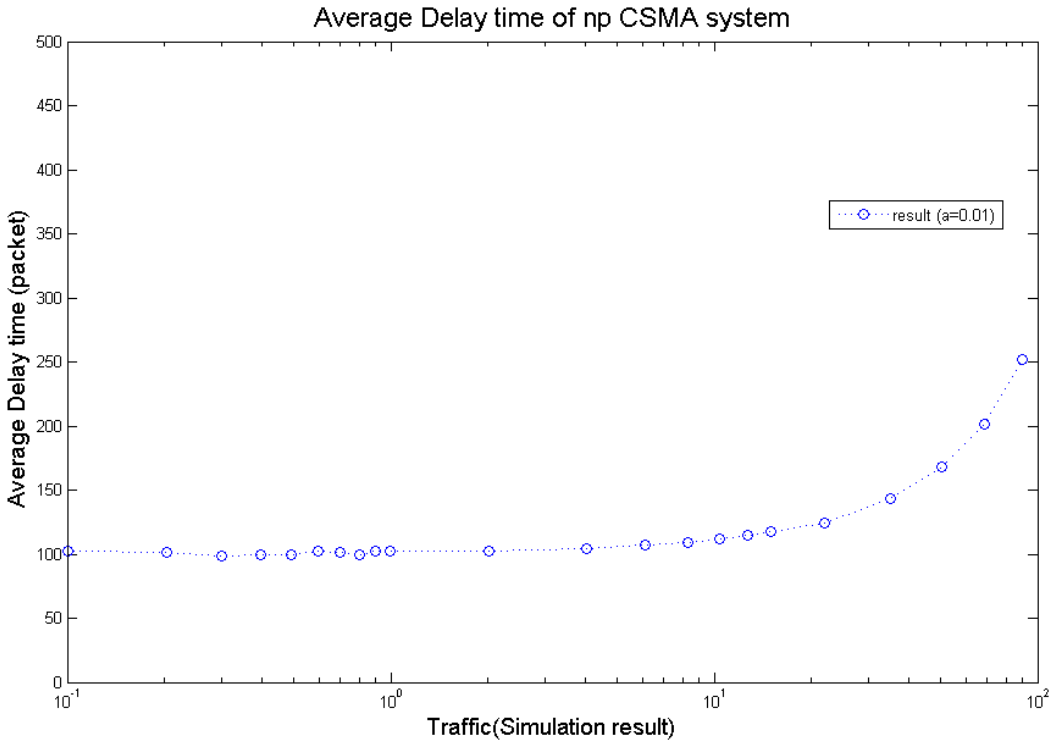

Рисунок 2.23 – Графічна залежність середнього часу затримки протоколу NP–CSMA провідної мережі

Використання ефекта захоплення для методу NP–CSMA продемонстровано на рис.2.24 і рис.2.25.

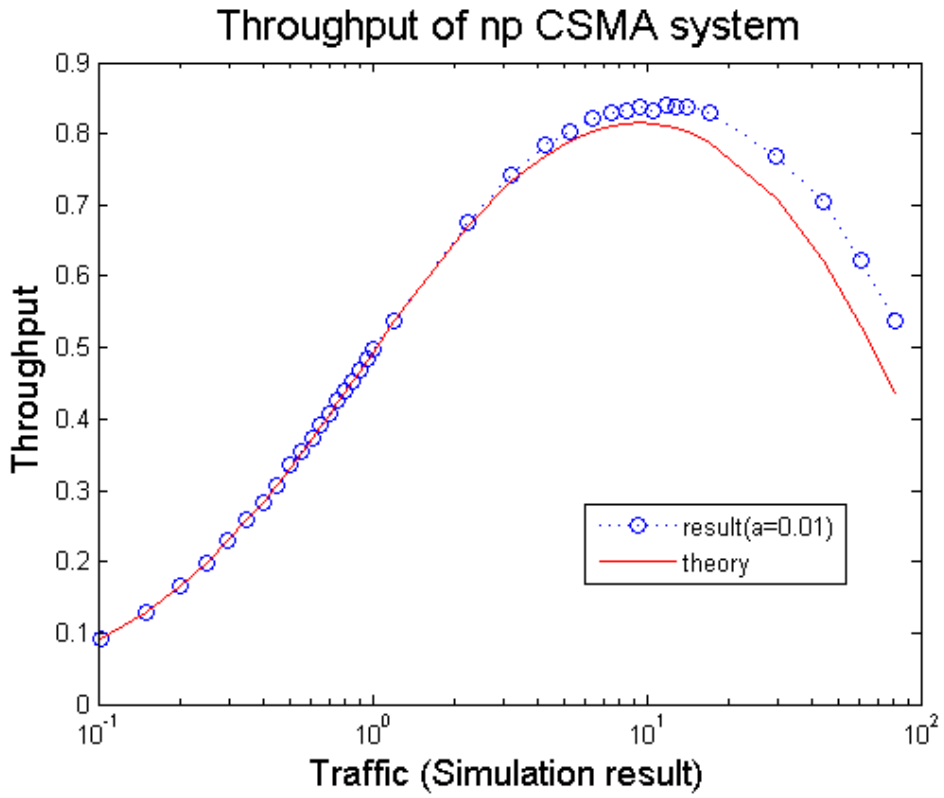

Рис.2.24 - Результати моделювання пропускної здатності для протоколу NP–CSMA безпровідної мережі (--теоретичний аналіз, %- експеримент)

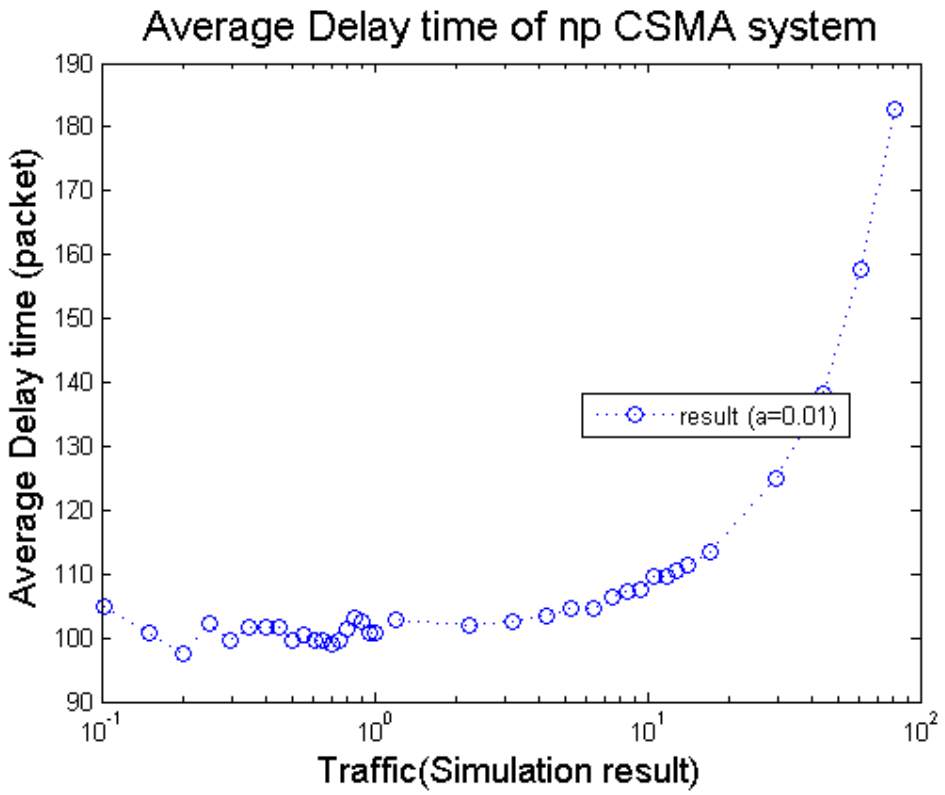

Рис.2.25 - Графічна залежність середнього часу затримки протоколу NP–CSMA для безпровідних мереж

Але, необхідно відзначити, що продемонстровані переваги методу NP-CSMA спостерігаються не завжди. З аналізу виразу (2.10) для пропускної здатності виходить, що характеристики протоколу залежать від нормалізованого часу затримки каналу (параметр а). Аналіз залежності (2.10) свідчить, що пропускна здатність зменшується під час збільшення часу затримки у каналі.

Тому для демонстрації цієї залежності змінимо у головній програмі час затримки зі значення Dtime=0,01 до значення Dtime=0,2. Результати моделювання для нового значення часу затримки у каналі наведені на рис.2.26, рис.2.27.

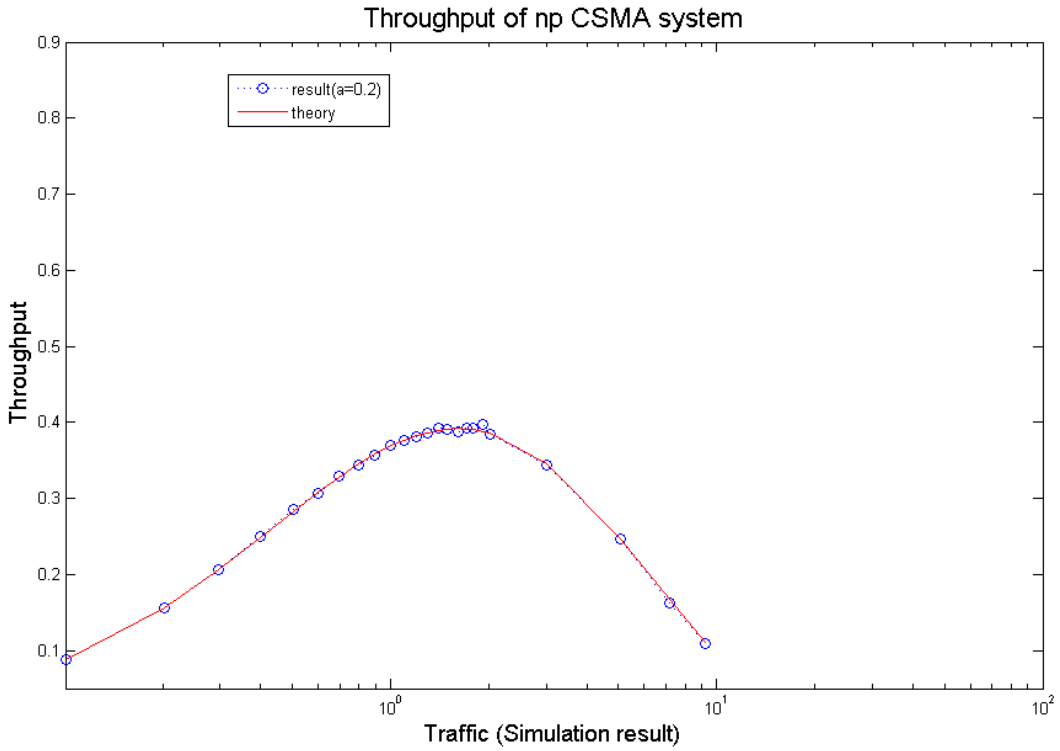

Рисунок 2.26 – Результати моделювання пропускної здатності для протоколу NP–CSMA провідної мережі при значенні затримки a=0,2 (--теоретичний аналіз, %- експеримент)

Використання ефекта захоплення для методу NP–CSMA продемонстровано на рис. 2.28 і рис.2.29.

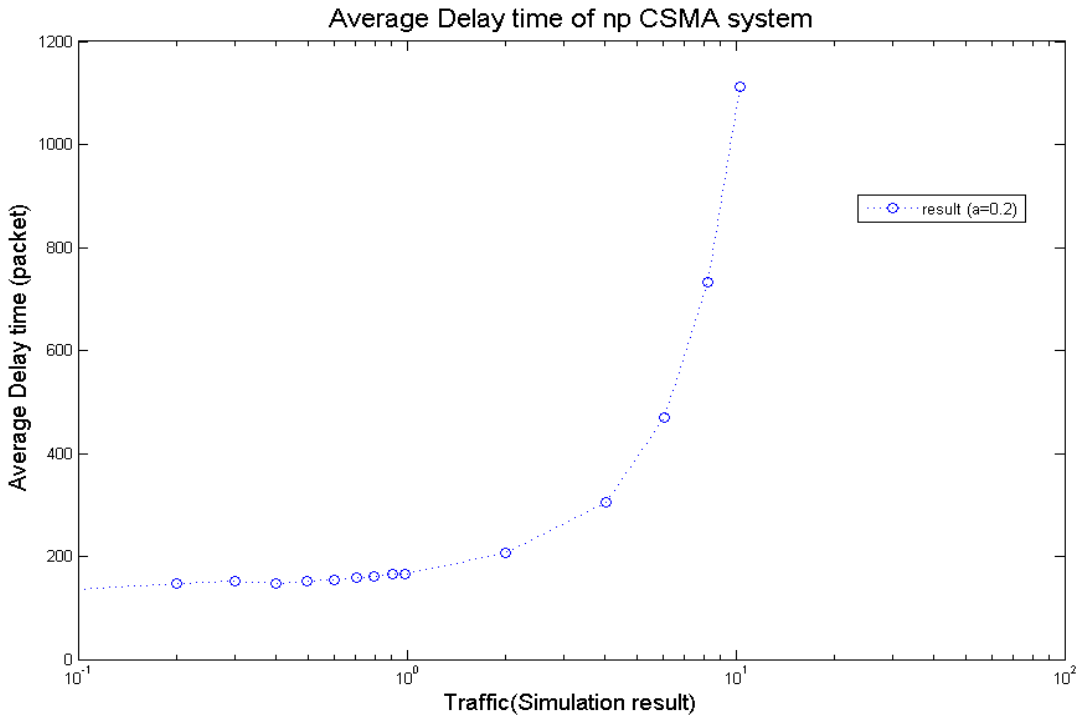

Рисунок 2.27 – Графічна залежність середнього часу затримки протоколу NP–CSMA провідної мережі при значенні затримки a=0,2.

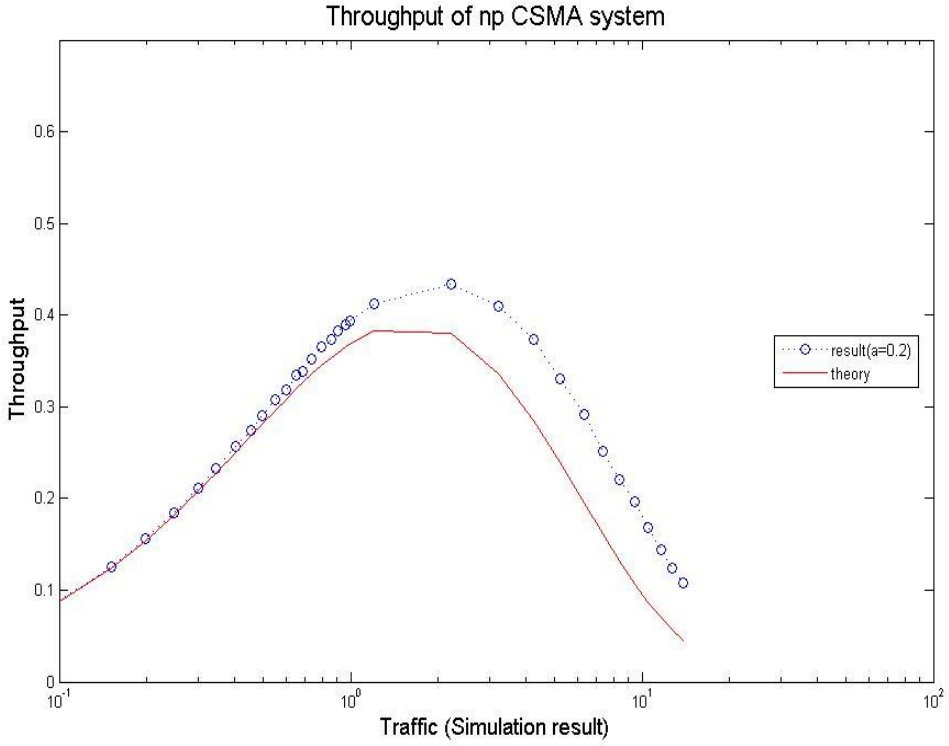

Рисунок 2.28 – Результати моделювання пропускної здатності для протоколу NP–CSMA безпровідної мережі при значенні затримки a=0,2 (--теоретичний аналіз, %- експеримент)

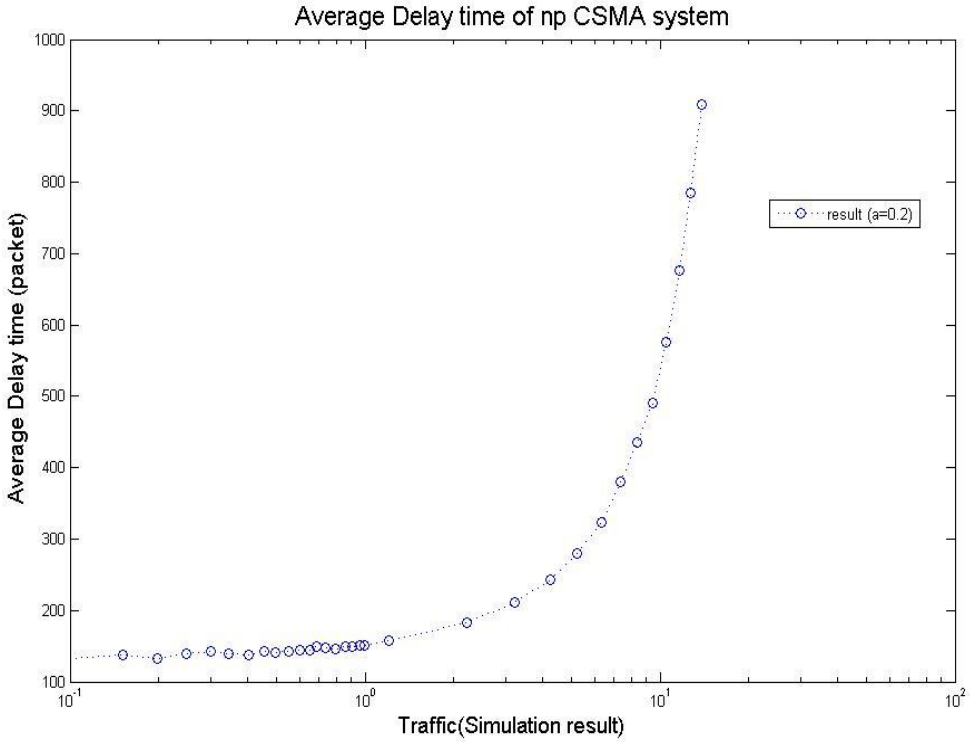

Рисунок 2.29 – Графічна залежність середнього часу затримки протоколу NP–CSMA безпровідної мережі при значенні затримки a=0,2.

Як видно з графіків до досягнення екстремуму криві без захоплення і з використанням захоплення практично збігаються, але після досягнення екстремуму ефект захоплення і,відповідно, безпровідна мережа забезпечує більші значення пропускної здатності.

Аналіз графіків також свідчить, що максимум пропускної здатності виявився залежним від нормалізованого часу затримки. Якщо значення a невелике, то максимальна пропускна здатність для схеми CSMA більша за пропускну здатність чистої схеми ALOHA і S–ALOHA. Але для великих значень **a** характеристика наближається до характеристики чистої схеми ALOHA. Це можна пояснити тим фактом, що інші термінали користувачів транслюють свої пакети впродовж достатньо великого часу затримки розповсюдження навіть якщо термінал передає свій пакет після детектування несучої. Як наслідок, виникає колізія. Застосування ефекту захоплення переданий пакет від конкретного користувача може бути успішно

доставленим через різницю у потужності пакетів різних користувачів. Відповідно пропускна здатність зростає.

2.8 Протокол методу множинного доступу ISMA.

Стандартний протокол CSMA зменшує ймовірність колізій завдяки механізму детектування несучої від інших користувачів. Але CSMA не може уникнути колізії коли два термінали знаходяться у межах недоступності через наявність перешкод між ними. Два таких термінали розглядаються як сховані одне від одного станції. Один з методів, який дозволяє вирішити проблему схованих станцій є протокол ISMA.

Вирішується це питання в протоколі ISMA наданням інформації до користувачів про зайнятість або вивільнення каналу самою точкою доступу Принцип роботи протоколу ISMA продемонстровано на рис.2.30 [4].

Рисунок 2.30 – Концепція протоколу ISMA

Пропускна здатність через трафік визначається як [4]

$$\rho = \frac{dG^{-dG}}{1 + d - e^{-dG}} \tag{2.11}$$

де *d* – нормалізована затримка розповсюдження.

Для ISMA, якщо точка доступу приймає пакети від користувача, то для усіх інших терміналів користувачів надсилається інформація про зайнятість каналу. В протилежному випадку, коли прийому будь-якого пакету точкою доступу не відбувається то вона передає сигнал звільнення каналу. Коли кожний термінал користувача отримує сигнал про звільнення каналу, то він повинен прийняти рішення передавати йому пакет до точки доступу або ні.

Коли термінал приймає сигнал про зайнятість каналу, то його передача пакету затримується (придушується). Принципово протокол ISMA можна розглядати як метод CSMA без проблеми схованих станцій. Але час затримки розповсюдження для ISMA удвічі більший порівняно з CSMA. Дійсно, оскільки усі термінали користувачів детектують сигнал від точки доступу, то точка доступу повинна спочатку прийняти сигнал від конкретного терміналу користувача і тільки після прийому надіслати сигнал зайнятості каналу для усіх терміналів-користувачів. Для протоколу CSMA усі користувачі детектують сигнал тільки від усіх інших користувачів. Такий алгоритм і зумовлює для ISMA подвоєння затримки передачі. Якщо інші термінали транслюють свої пакети під час затримки передачі, то виникає колізія у точці доступу, як це показано на рис.2.31.

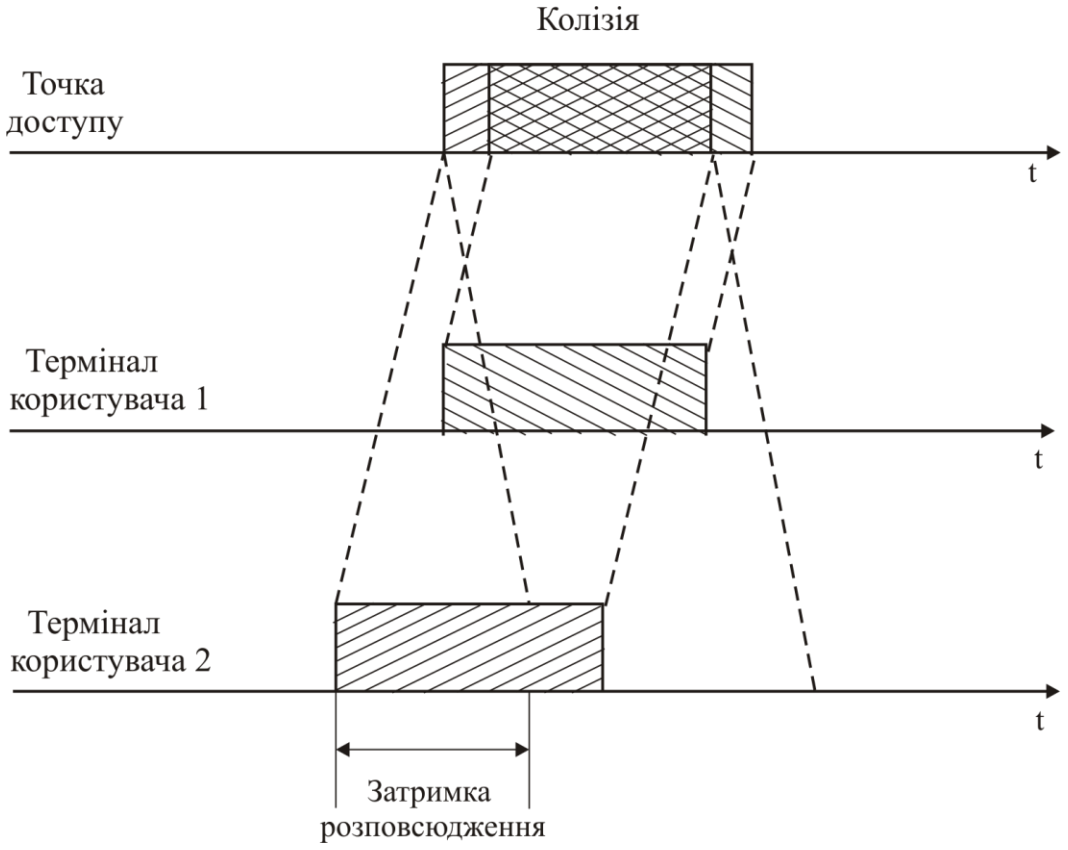

Рисунок 2.31 – Виникнення колізії для протоколу ISMA

Нормалізація часу затримки відбувається до часу необхідного для передачі одного пакету. Окрім того, для ISMA також вводять поняття прямого каналу (від точки доступу до терміналів користувачів) і зворотного каналу (від терміналів користувачів для точки доступу)

Для моделювання обрано протокол ненаполегливого ISMA з виділенням часових інтервалів-слотів. Принцип дії протоколу продемонстровано на рис.2.32 [4].

Тривалість слоту обирається рівним тривалості одного пакету. Коли кожен з користувачів генерує свій пакет відбувається детектування несучої. Якщо приймається сигнал про вивільнення каналу, то термінал користувача передає пакет у наступному часовому слоті.

Якщо ж термінал користувача приймає сигнал про зайнятість каналу, то передача пакету не відбувається, а здійснюється перехід в режим

очікування наступного слоту, який обирається випадково,і вже в ньому поновлює процедуру детектування.

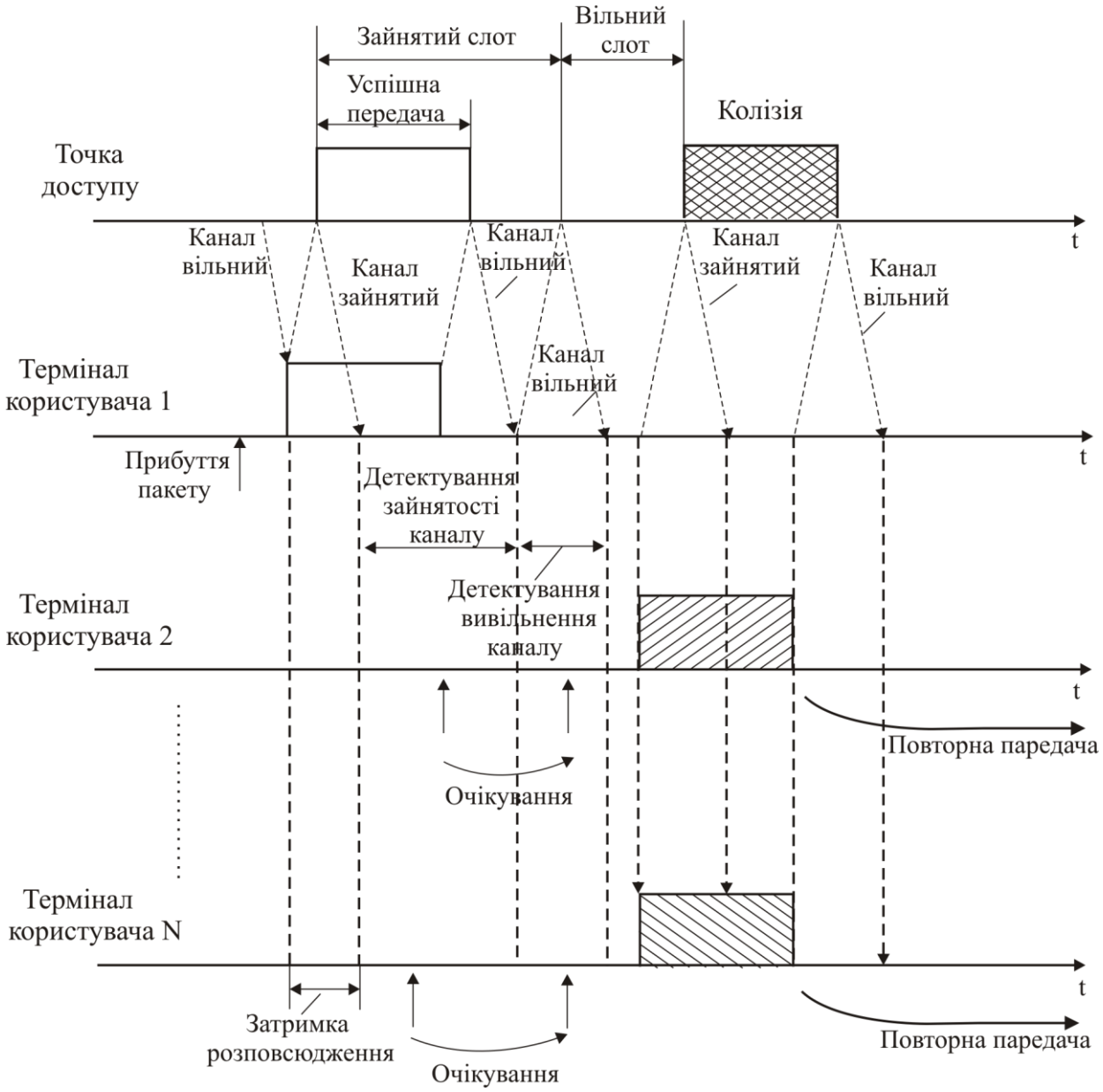

Рисунок 2.32 – Принцип роботи протоколу ненаполегливого методу ISMA

Для точки доступу часовий слот, в якому транслюється сигнал зайнятості до усіх терміналів користувачів називають зайнятим слотом. Навпаки, часовий слот, в якому передається сигнал про вивільнення каналу називають слотом вивільнення.

Коли точка доступу прийняла пакети від усіх користувачів, то вона інформує усіх користувачів про майбутній час для передачі пакетів. Але, якщо точка доступу не прийняла будь-якого пакету, то вона також інформує користувачів про майбутній час передачі.

2.8.1 Підпрограма моделювання протоколу ISMA

Моделювання запропонованого алгоритму реалізовано у підпрограмі snpisma.m, повний лістинг якої наведено у додатку Д.

Структурно підпрограму можна розділити на сім функціональних блоків. Перші чотири блоки і сьомий блоки повністю тотожні аналогічним за призначенням блокам підпрограми npcsma.m.

У п’ятому блоці підпрограми snpisma.m термінали користувачів, які генерують пакети або очікують передачі своїх пакетів на поточний момент часу виконують процедуру прихованого детектування. Якщо канал виявляється вільним, відбувається оновлення змінної now_time – поточного часу на час наступної передачі пакету. Але якщо канал зайнятий зайнятий, то визначається час для реалізації повторного детектування.

2.8.2 Результати моделювання

Результати моделювання пропускної здатності і середнього часу затримки передачі для значення нормалізованої затримки розповсюдження d=0,01 наведені на рис.2.33 і рис.2.34 відповідно.

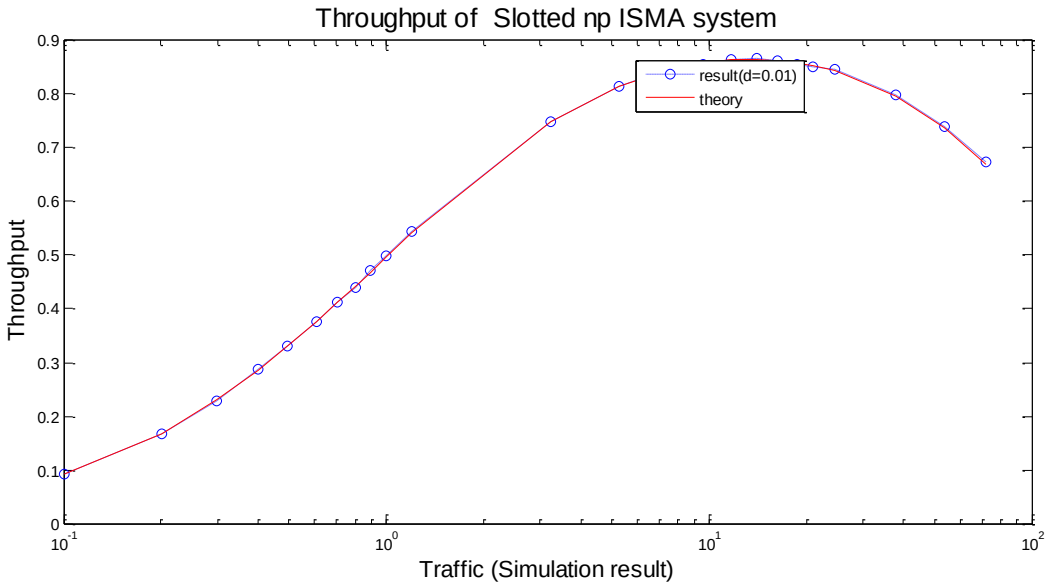

Рисунок 2.33 – Результати моделювання пропускної здатності для протоколу ISMA провідної мережі при значенні нормалізованої затримки розповсюдження d=0,01 (--теоретичний аналіз, %- експеримент)

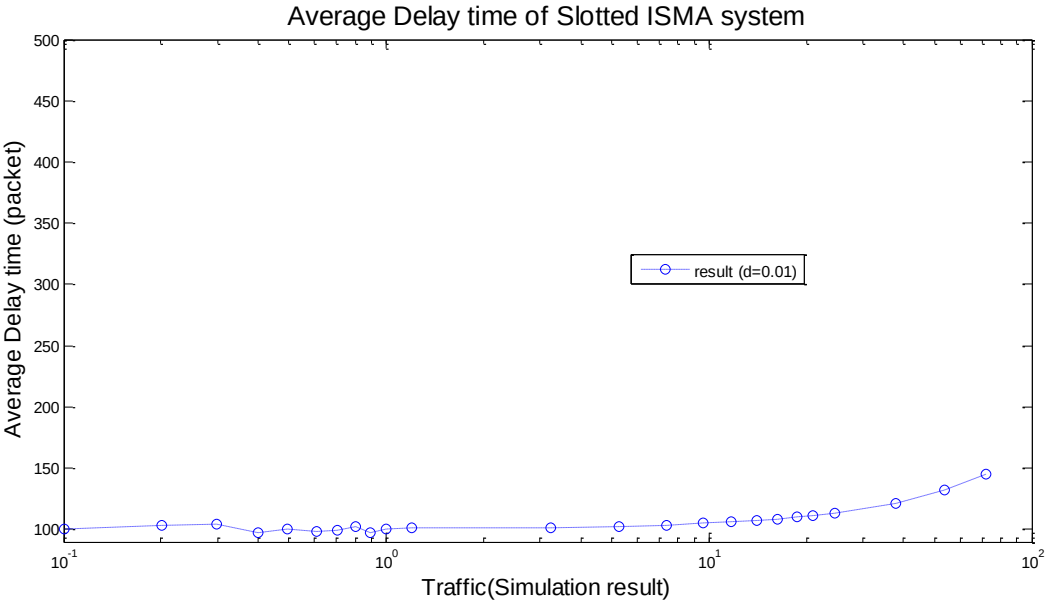

Рисунок 2.34 – Графічна залежність середнього часу затримки протоколу ISMA провідної мережі при значенні нормалізованої затримки розповсюдження d=0,01.

Використання ефекта захоплення для методу ISMA продемонстровано на рис. 2.35 і рис.2.36.

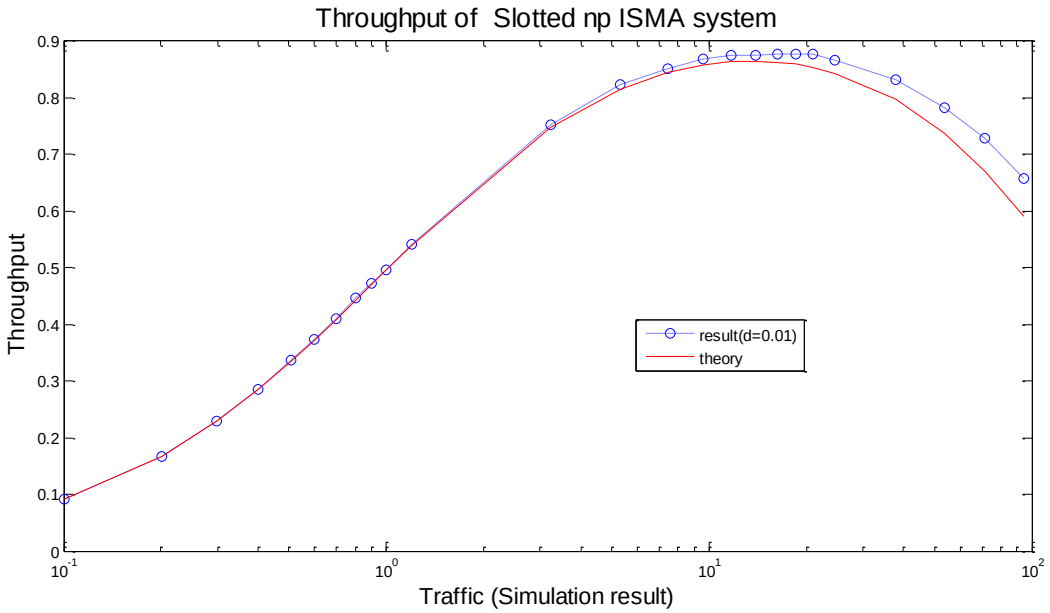

Рисунок 2.35 – Результати моделювання пропускної здатності для протоколу ISMA безпровідної мережі при значенні нормалізованої затримки розповсюдження d=0,01.

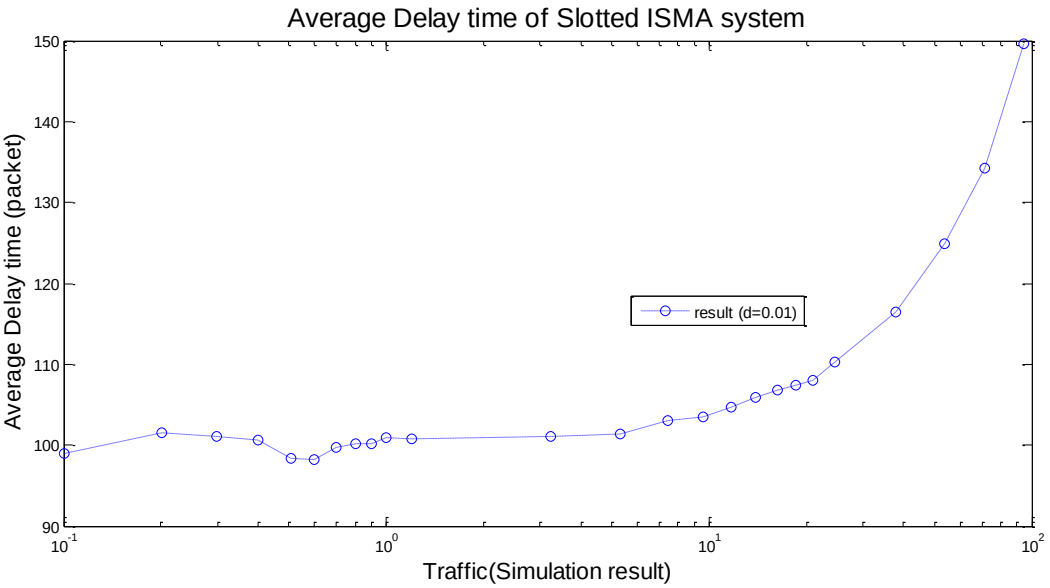

Рисунок 2.36 – Графічна залежність середнього часу затримки протоколу ISMA безпровідної мережі при значенні нормалізованої затримки розповсюдження d=0,01.

Результати моделювання пропускної здатності і середнього часу затримки передачі для значення нормалізованої затримки розповсюдження d=0,2 наведені на рис.2.37 і рис.2.38 відповідно.

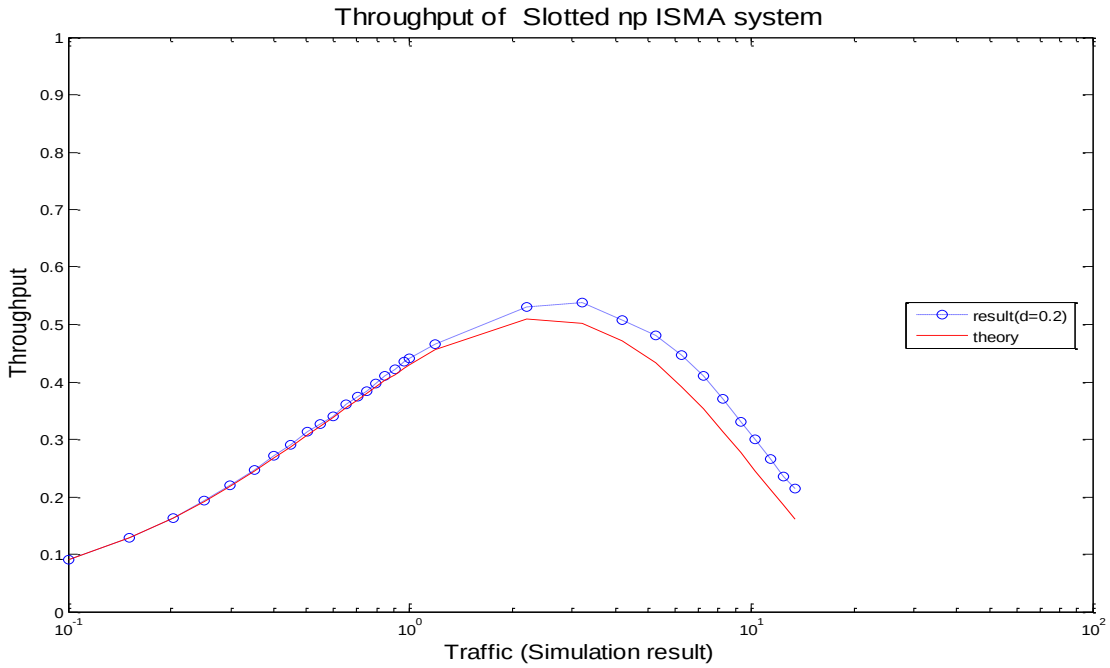

Рис.2.37 – Результати моделювання пропускної здатності для протоколу ISMA провідної мережі при значенні нормалізованої затримки розповсюдження d=0,2.

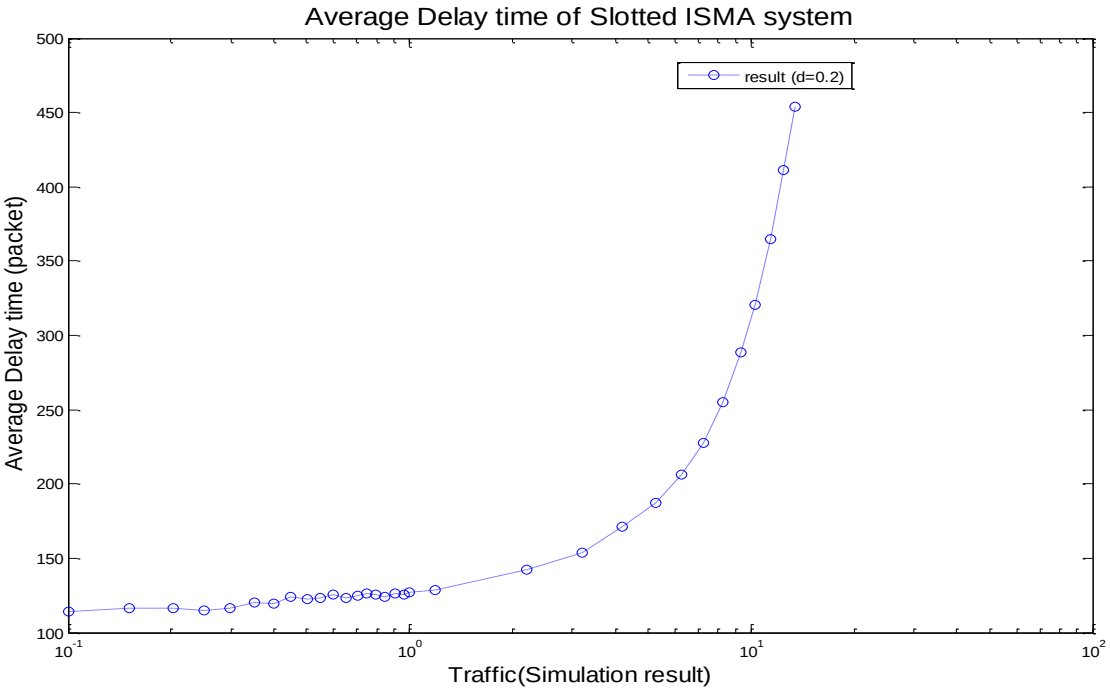

Рис.2.38 – Графічна залежність середнього часу затримки протоколу ISMA провідної мережі при значенні нормалізованої затримки розповсюдження d=0,2.

Використання ефекта захоплення для методу ISMA продемонстровано на рис. 2.39 і рис.2.40.

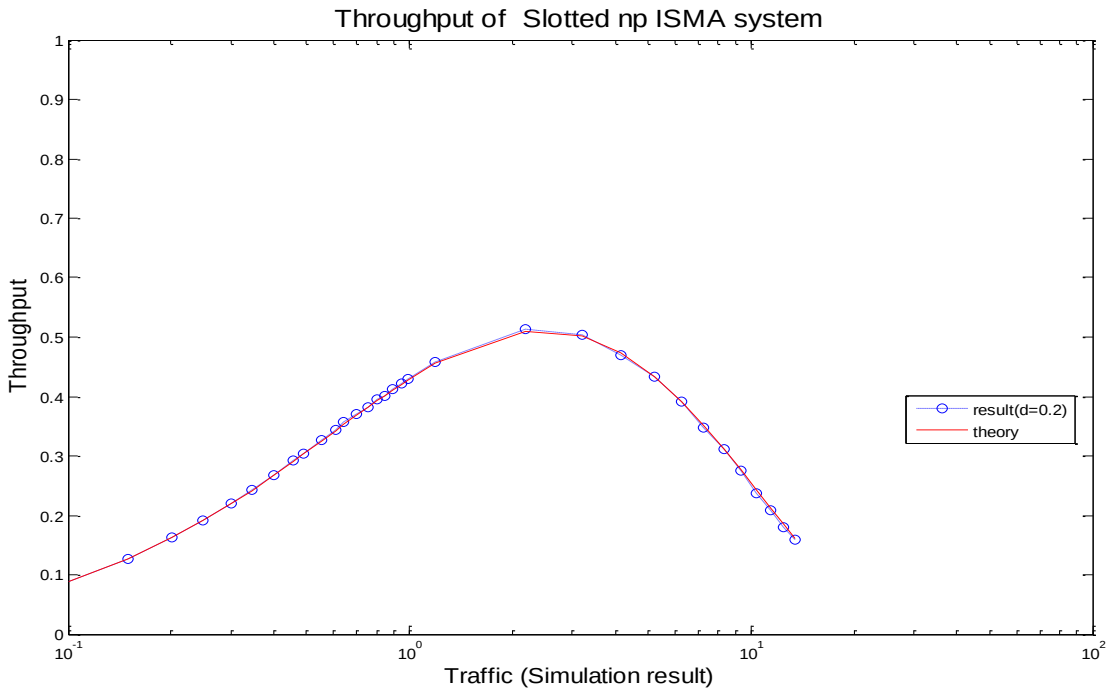

Рис.2.39 – Результати моделювання пропускної здатності для протоколу ISMA безпровідної мережі при значенні нормалізованої затримки розповсюдження d=0,2.

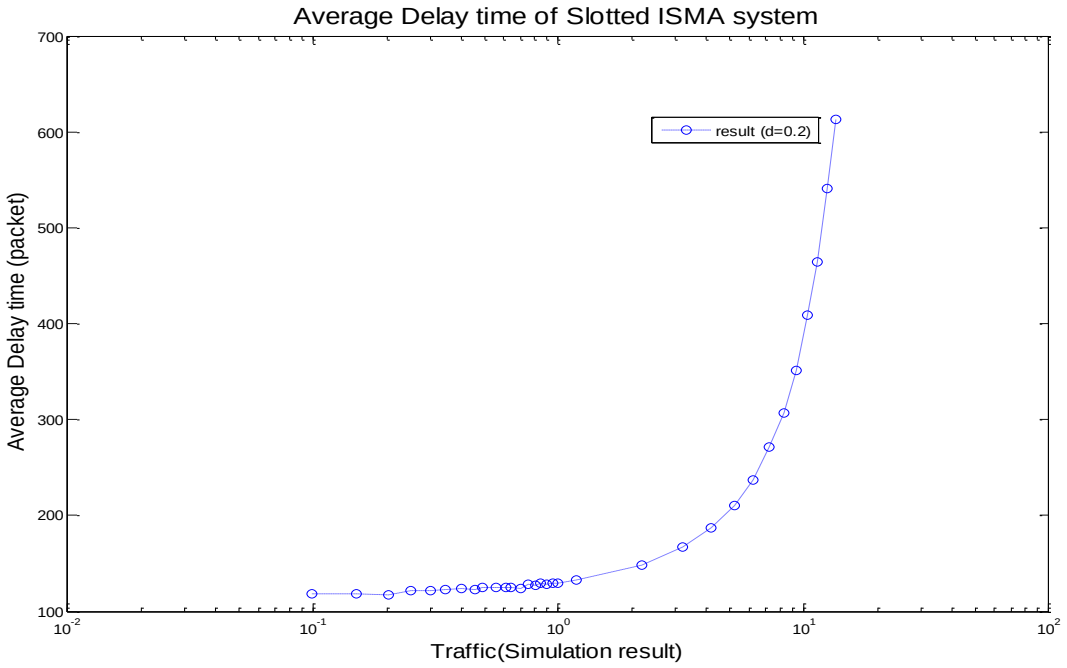

Рис.2.40 – Графічна залежність середнього часу затримки протоколу ISMA безпровідної мережі при значенні нормалізованої затримки розповсюдження d=0,2.

Як видно з наведених графіків, максимальна пропускна здатність протоколу ISMA залежить від нормалізованого часу затримки розповсюдження. Окрім того, можна також відзначити збільшення пропускної здатності при використанні ефекту захоплення, оскільки частину пакетів можна розглядати як успішно прийняті у точці доступу через суттєво різні потужності від різних користувачів у точці доступу і відповідно виживання найбільш “потужних” пакетів.

3 ЕКОНОМІЧНІ РОЗРАХУНКИ

3.1 Тенденції розвитку ринку бездротового зв’язку

Телекомунікаційний ринок є одним з найбільш перспективних та швидко зростаючих напрямків галузі зв’язку України. На даний час система телекомунікацій в Україні знаходиться на шляху швидкого розвитку, що в цілому орієнтоване на вхід української системи зв'язку в світову, як рівноправного партнера. Однією з галузей зв'язку, що має бурний розвиток, є мобільний зв'язок. Щороку відбувається злиття та поглинання одних мобільних операторів іншими, а самі мобільні оператори розширюють спектр послуг, які вони надають, з метою отримання більшої частки на ринку. Традиційні методи моделювання розвитку даного ринку ускладнені постійною появою нових технологій, що кардинально змінюють характер розвитку ринку [9].

З кожним роком зростає кількість користувачів мобільним зв’язком, це означає збільшення обсягу передавання інформації, а отже збільшення навантаження на технічну частину, що обслуговує абонентів. Цю проблему вирішують цифрові методи модуляції.

Більш складні за алгоритмом роботи цифрові методи модуляції (у порівнянні з аналоговими методами) вимагають ускладнення апаратурної (технічної) реалізації системи. Саме цифрові методи модуляції використовуються у більшості сучасних системах мобільного зв’язку.

Темою дипломного проекту є «Моделювання протоколів множинного доступу в безпроводових мережах». Ця тема охоплює знання, які формують загальну інформацію про протоколи множинного доступу та їх призначення, як вони застосовуються в безпроводових мережах, засоби проектування, конструювання та матеріалізації відповідних технічних процесів та явищ у конкретних об’єктах та системах, які стосуються теми дипломного проекту.

Взагалі, безпроводова мережа – це тип комп'ютерної мережі, що застосовує бездротове з'єднання для передачі даних і підключення до мережевих вузлів. Безпроводові мережі зв'язку апаратних пристроїв дозволяють мобільним користувачам організувати взаємодію апаратних пристроїв, що забезпечує роботу в нестаціонарних умовах. Безпроводова мережа доступу дуже проста в установці, її можна налаштувати і запустити через кілька хвилин після включення робочої станції оператора.

Основними операторами є Київстар, Vodafone Україна та lifecell, які разом займають понад 97,5% ринку мобільного зв'язку України. На рис. 3.1 і рис.3.2 подані тенденції розвитку стільникового зв'язку України [10].

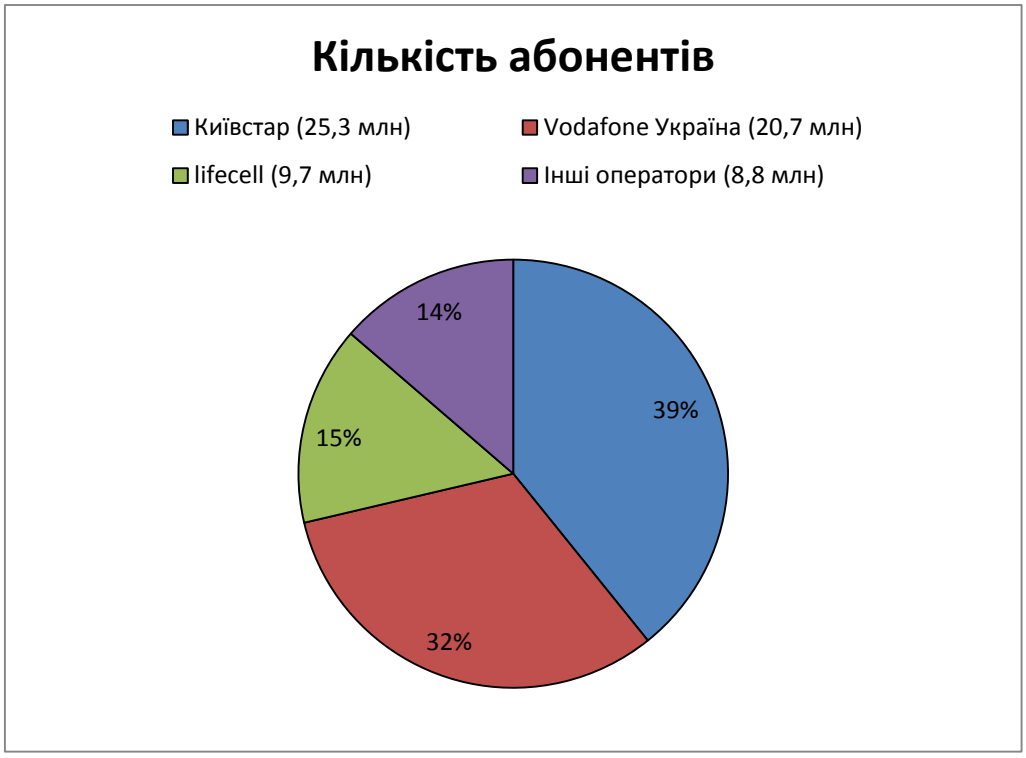

Рисунок 3.1 – Структура ринку стільникового зв'язку України

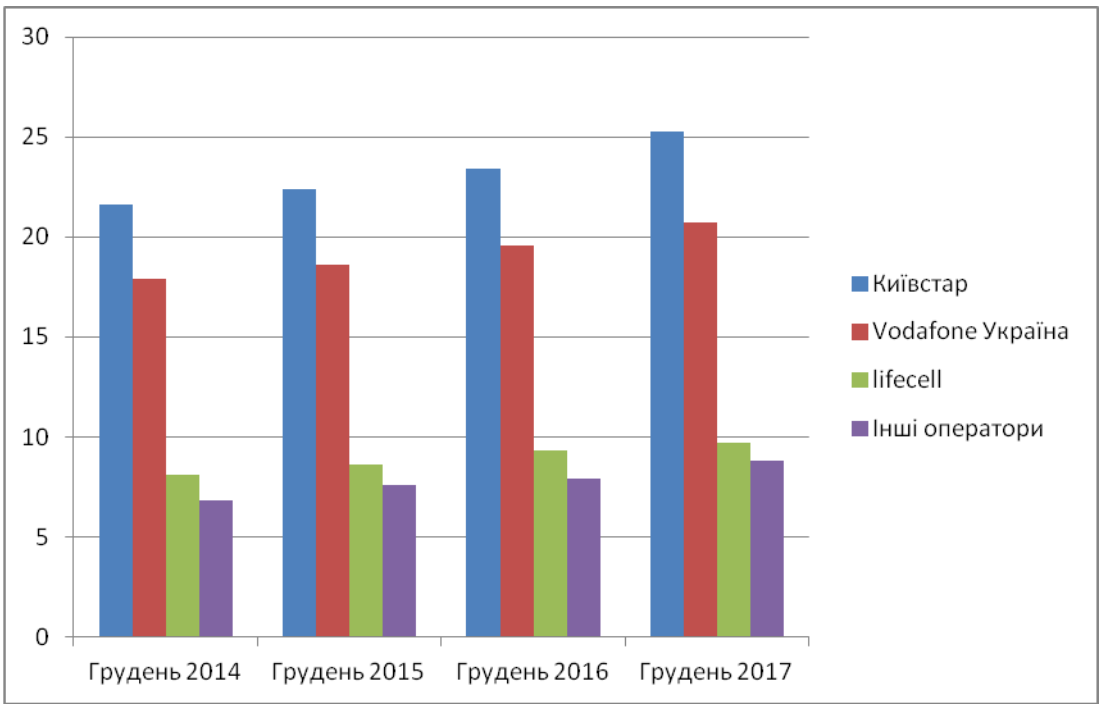

Рисунок 3.2 – Динаміка зросту кількості абонентів стільникового зв’язку в Україні

Проблема представленого дослідження має актуальний характер в сучасних умовах. Про це свідчить активність досліджень і нових розробок у цьому напрямку.

Питання дослідження цифрових методів модуляції, а саме створення спеціального програмного забезпечення для формування сигналів вивчалося недостатньо. Загалом, матеріал викладений у навчальних посібниках, носить загальний характер, у той час як у різних статтях та публікаціях за даною тематикою розглядаються більш вузькі питання, що стосуються заданої теми. Проте потребується більш детальніше врахувати сучасні умови при дослідженні проблематики заданої теми.

Висока значимість та недостатня практична розробленість визначають безсумнівну новизну даного дослідження, а отже й підвищують ступінь його значущості для нових технологій у сфері зв’язку.

3.2 Визначення трудомісткості та тривалості роботи

Основною умовою раціонального планування дослідження є скорочення строків виконання при мінімальних витратах трудових, матеріальних та грошових ресурсів. Для цього необхідно вирішити наступні питання: визначення трудомісткості та тривалості; складання календарного графіка виконання; визначення витрат на проведення і ефективність дослідження.

Комплекс науково – дослідницьких робіт може бути поділений на етапи. Для кожного етапу необхідно вказати його найменування, виконавців, трудомісткість і тривалість робіт. В даній роботі беруть участь один молодший науковий співробітник і один старший науковий співробітник. Результати розподілу наведені в таблиці 3.1.

Через те, що важко встановити трудомісткість виконання робіт, у зв'язку з елементами незвичайності, в процесі виконання більшості науково-дослідницьких робіт, використовується ймовірнісний метод. При цьому використовують дві або три вірогідних оцінки часу. Ці оцінки є вихідними для розрахунку очікуваного часу виконання роботи за формулою 3.1:

$$t_{оч} = \frac{3 \cdot t_{min} + 2 \cdot t_{max}}{5} \quad (3.1)$$

де $t_{оч}$ – очікувана оптимальна оцінка часу виконання роботи, днів;

t_{min} – мінімально необхідний час на виконання роботи при найбільш сприятливих умовах, днів;

t_{max} – максимальні витрати часу на виконання роботи за несприятливих умов, днів.

Таблиця 3.1 – Оцінка довготривалості та трудомісткості етапів робіт

№	Етапи роботи	Часова оцінка, дн.			Дис-пер-сія	Виконавці		Трива-лість, днів
		t_{min}	t_{max}	$t_{оч}$		Спеціальність	Кіл–сть, чол.	
1	2	3	4	5	6	7	8	9
1	Отримання технічного завдання	1	2	2	0,2	Молодший науковий співро-бітник	1	2
2	Огляд літературних джерел	3	7	5	0,8	Молодший науковий співробітник	1	5
3	Аналіз основних принципів організації	2	4	3	0,4	Молодший науковий співро-бітник	1	3
4	Підготовчий (техніко-економічне обґрунтування) етап	14	20	17	1,2	Молодший науковий співро-бітник	1	14
5	Написання програми	13	15	14	0,4	Старший науковий співро-бітник	1	14
6	Аналіз результатів програми	13	19	16	1,2	Старший науковий співро-бітник	1	11
7	Вибір та купівля необхідного обладнання та матеріалів	2	4	3	0,4	Молодший науковий співро-бітник	1	3
8	Експериментальні дослідження	20	22	21	0,6	Молодший науковий співро-бітник	1	21

Продовження таблиці 3.1

1	2	3	4	5	6	7	8	9
9	Аналіз отриманих даних, коригування програми	5	7	6	0,4	Старший науковий співро-бітник, Молодший науковий співро-бітник	2	6
10	Висновки та пропозиції	8	10	9	0,4	Старший науковий співро-бітник	1	7
11	Складання та обговорення технічного звіту	2	2	2	0,0	Старший науковий співро-бітник	1	2
12	Впровадження результатів	2	2	2	0,0	Молодший науковий співро-бітник	1	2
	Усього	85	114	100	–	–	–	90

Ступінь правильності визначення перевіряється розрахунком дисперсії – різниці між мінімальною та максимальною оцінками часу, що визначається за формулою (3.2):

$$\sigma = \frac{t_{\max} - t_{\min}}{5} \tag{3.2}$$

Розраховані значення для кожного етапу занесені у табл. 3.1.

Дана дипломна робота повинна виконуватися поетапно, у лінійній послідовності, так без отримання необхідних результатів дослідів не можна виконувати наступний пункт. Використовуючи дані табл. 3.1, збудуємо лінійний календар (рис. 3.3):

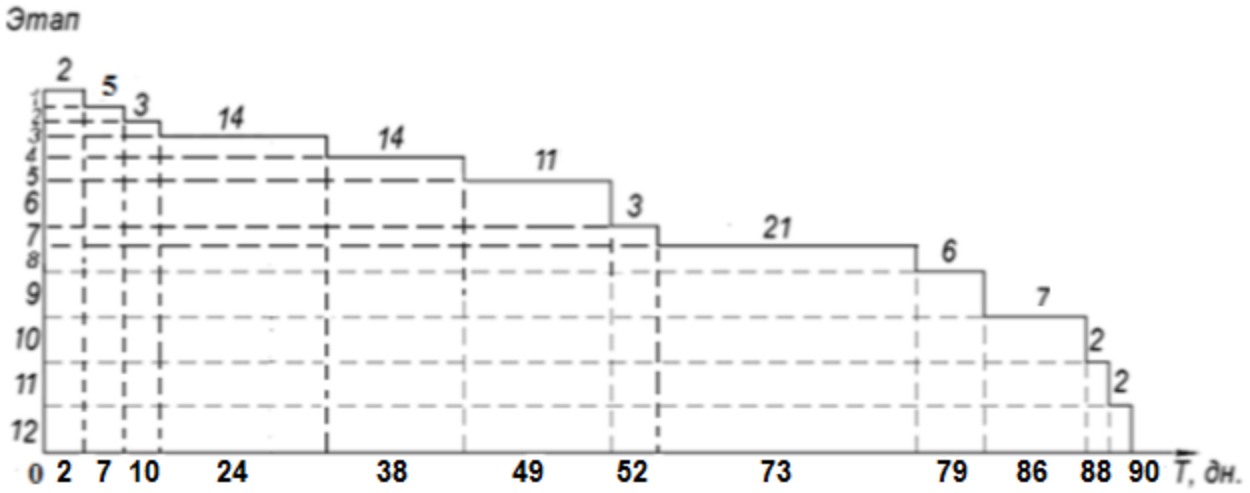

Рисунок 3.3 – Лінійний календарний графік

3.3 Розрахунок кошторису витрат на практичну реалізацію магістерської роботи

До складу витрат на реалізацію проекту враховується вартість усіх ресурсів, необхідних для проведення комплексу робіт. Проте в даному випадку, при роботі над заданою темою дипломного проекту розрахунок багатьох статей ускладнений через невизначеність, яка виражається в тому, що заздалегідь невідомо необхідну кількість деяких матеріалів, деталей, послуг, а також величини витрат.

Вирішенням даного питання є використання методики збільшених розрахунків. Дана методика передбачає по перше первинний розрахунок основної заробітної плати, а вже після цього – процентних частин інших статей витрат на реалізацію проекту.

Статті, витрати за якими можуть бути розраховані більш точно, розраховуються за звичайною методикою.

З метою визначення витрат на реалізацію проекту складено кошторис витрат (табл. 3.2).

Таблиця 3.2 – Кошторис витрат на реалізацію проекту

Статті витрат	Умовне позначення	Сума	
		грн.	частка, %
Матеріали, покупні вироби і напівфабрикати (за відрахуванням відходів, що реалізуються)	М	1117,6	2,16
Спеціальне устаткування для реалізації проекту	СУ	21000	40,7
Основна і додаткова заробітна плата виробничого персоналу	ЗП	14337,54	27,79
Відрахування на соціальне страхування (від суми основної і додаткової заробітної плати)	ОТЧ	3154,26	6,11
Накладні витрати	НВ	11972,96	23,24
Усього витрат на реалізацію проекту	-	51582,36	100

3.3.1 Розрахунок вартості матеріалів

До статті витрат на матеріали включаються вартість основних та допоміжних матеріалів, необхідних для розробки проекту. За період проведення науково-дослідницьких робіт співробітниками будуть використані наступні матеріали (табл. 3.3).

Таблиця 3.3 – Розрахунок вартості матеріалів

Матеріал	Марка, ГОСТ, ДСТУ, ТУ	Кількість	Ціна за одиницю, грн/шт.	Витрати за матеріали	Частка, %
Папір А4	UNI Office A4	500	0,15	75	63,7
Папір А2	Xerox A2	4	3	12	10,2
Папір А1	Xerox A1	5	5	25	21,25
Транспортно-заготівельні витрати	–	–	–	5,6	4,85%
Усього	–	–	–	117,6	

3.3.2 Спеціальне устаткування

У цій статті враховуються витрати на оренду, доставку і монтаж лабораторних установок, вимірювальних та регулювальних пристроїв, приладів, випробувальної апаратури тощо (табл. 3.4).

Балансова вартість обчислювальної техніки становить 10000 грн. за один комп'ютер. Для проведення науково – дослідницької роботи використовується 2 комп'ютера.

Таблиця 3.4 – Витрати на спеціальне устаткування

Перелік устаткування	Марка, ГОСТ, ДСТУ, ТУ	Кількість	Ціна за одиницю, грн.	Собівартість експлуатації, грн. / год.
Разом	Комп’ютер	2	10000	20000
Транспортно-заготівельні витрати	–	–	–	1000
Всього	–	–	–	21000

3.3.3 Розрахунок заробітної плати

Витрати на основну заробітну плату складаються з планового фонду заробітної плати всіх категорій працівників, зайнятих в розробці проектованого пристрою.

Розрахунок заробітної плати ведеться на основі даних про трудомісткість (табл. 3.1). Результати розрахунків зведені в табл. 3.5.

Додаткову заробітну плату приймаємо рівною 10% від основної заробітної плати. Розрахунок основної та додаткової заробітної плати наведено в табл. 3.6.

Таблиця 3.5 – Розрахунок основної заробітної плати

Посада виконавця	Кіль-сть людей	Місячний оклад, грн	Середньоденна зар.плата, грн.	Кількість робочих днів	Сума зар. плати, грн.
Старший науковий співробітник	1	4500	150	40	6000
Молодший науковий співробітник	1	3200	106.66	56	5972.96
Усього	2	–	–	–	17972,96

Таблиця 3.6 – Основна та додаткова заробітна плата

Спеціальність виконавця	Додаткова заробітна плата, грн.	Сума основної та додаткової заробітної платні, грн
Старший науковий співробітник	1200	7200
Молодший науковий співробітник	1194,58	7137,54
Усього	2394,58	14337,54

3.3.4 Відрахування на соціальне страхування

Відрахування на соціальне страхування й в інші фонди визначаються в розмірі 22 % від суми основної та додаткової заробітних плат.

Таким чином, відрахування на соціальне страхування становить:

$$Відр = (ЗП_{осн} + ЗП_{доп}) \cdot 0,22 \quad (3.3)$$

де $ЗП_{осн}$ – основна заробітна плата, грн.;

$ЗП_{доп}$ – додаткова заробітна плата, грн.

$$Відр = 14337,54 \cdot 0,22 = 3154,26 \text{ грн}$$

3.3.5 Накладні витрати

До накладних витрат відносять витрати на загальне управління та загальногосподарські потреби (на заробітну плату апарату управління, канцелярські витрати та інше), на утримання і експлуатацію будівель і споруд. Накладні витрати включаються у вартість проведення роботи непрямим шляхом – у відсотках від основної заробітної плати співробітників.

Накладні витрати становлять 80-100% від основної заробітної плати співробітників, що в нашому випадку становить:

$$НВ=17972,96 \cdot 1,0=17972,96 \text{ грн}$$

3.3.6 Бальна оцінка економічної ефективності проекту

Наукові дослідження, прямий підрахунок економічної ефективності яких неможливий, оцінюють за допомогою бальної системи.

Бальна оцінка проводиться за наступними показниками:

– важливість розробки $К_1$=1, обирається з табл. 3.7;

Таблиця 3.7 – Шкала для оцінки важливості розробки $К_1$

№ з/п	Показник	Бали
1	Ініціативна робота, що не є частиною комплексної програми, або завданням відомчих органів	1
2	Робота, виконувана за договором про науково-технічну допомогу	3
3	Робота представляє частину відомчої програми	5
4	Робота представляє частину відомчої комплексної програми	7
5	Робота представляє частину міжнародної комплексної програми	8

– можливість використання результатів розробки $К_2$=8 (табл. 3.8);

Таблиця 3.8 – Шкала оцінки можливості використання результатів розробки $К_2$

№ з/п	Показник	Бали
1	У даному підрозділі	1
2	У даній організації	3
3	У багатьох організаціях	5
4	У масштабах країни	8

– теоретична значимість і рівень новизни дослідження $К_3$=2 (табл. 3.9);

Таблиця 3.9 – Шкала оцінки теоретичної значимості й рівня новизни дослідження $К_3$

№ з/п	Показник	Бали
1	Аналіз, узагальнення й класифікація відомої інформації. Подібні результати були відомі в досліджуваній області	2
2	Одержання нової інформації, що доповнює знання про сутність досліджуваних процесів, не відомі в досліджуваній області	3
3	Одержання нової інформації, що змінює уявлення про сутність досліджуваних процесів, не відомої раніше	5
4	Створення нових теорій, методик	6
5	Одержання інформації, що сприяє формуванню напрямків, не відомих раніше	8

– складність розробки $К_4$=5 (табл. 3.10).

Таблиця 3.10 – Шкала оцінки показників складності дослідження $К_4$

№ з/п	Показник	Бали
1	Робота виконується одним підрозділом, витрати менш 10000 грн.	1
2	Робота виконується одним підрозділом, витрати 10000-50000 грн.	3
3	Робота виконується одним підрозділом, витрати 50000-100000 грн.	5
4	Робота виконується за участю багатьох підрозділів, витрати 100000-500000 грн.	7
5	Робота виконується декількома організаціями, витрати понад 500000 грн.	8

Загальна оцінка встановлюється за добутком коефіцієнтів:

$$Пс=К_1 \cdot К_2 \cdot К_3 \cdot К_4, \quad (3.4)$$

$$П_с=1 \cdot 8 \cdot 2 \cdot 5=80 \text{ балів.}$$

Питомий ефект на кожний бал – 1 000 грн.

Загальний ефект від розробки складає:

$$Е=Пс \cdot 1000, \quad (3.5)$$

$$Е=80 \cdot 1000=80\ 000 \text{ грн}$$

Економічна ефективність від реалізації дипломного проекту визначається за допомогою коефіцієнта ефективності, що характеризує частку загального ефекту від розробки, що приходиться на одну грн. витрат (собівартості НДР) :

$$К_В=Е/К_{ндр}, \quad (3.6)$$

$$К_В=80000/51582,36=1,55.$$

В даному розділі було проведено аналіз і обґрунтування економічної ефективності науково – дослідницької роботи. Розраховано, що для проведення дослідження необхідно близько 90 днів. При цьому сумарні витрати на дослідження становлять 51582,36 грн., з них:

– заробітна плата – 14337,54 грн., що становить 27,79 % від загальної кількості витрат;

– накладні витрати – 11972,96 грн. (23,24%);

– спеціальне обладнання для реалізації проекту – 21000 грн. (40,7 %);

– відрахування на соціальне страхування 3154,26 грн. (6,11%);

– витратні матеріали, куповані вироби і напівфабрикати – 1117, грн. (2,16%).

Обґрунтованість ефективності дослідження підтверджується розрахованим коефіцієнтом економічної ефективності, який становить – 1,55.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

За Законом України «Про охорону праці», охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

Для управління охороною праці створюються відповідні служби і призначаються компетентними органами посадові особи, які забезпечують вирішення конкретних питань охорони праці. На підприємстві з кількістю працюючих 50 і більше осіб роботодавець створює службу охорони праці відповідно до типового положення, що затверджується спеціально уповноваженим центральним органом виконавчої влади з питань нагляду за охороною праці. На підприємстві з кількістю працюючих менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку. На підприємстві з кількістю працюючих менше 20 осіб для виконання функцій служби охорони праці можуть залучатися сторонні спеціалісти на договірних засадах, які мають відповідну підготовку.

За порушення законодавства про охорону праці, невиконання розпоряджень посадових осіб органів державного нагляду за охороною праці юридичні та фізичні особи, які відповідно до законодавства використовують найману працю, притягаються органами державного нагляду за охороною праці до сплати штрафу у порядку, встановленому законом.

4.1 Аналіз потенційних небезпек

Оскільки тема дипломного проекту «Моделювання протоколів множинного доступу в безпроводових мережах» передбачає роботу у приміщенні обладнаному персональними комп’ютерами з візуальними

дисплейними терміналами, необхідно розглянути заходи щодо забезпечення безпеки, виробничої санітарії, гігієни праці та пожежної безпеки приміщень з персональними комп’ютерами.

При аналізі технологічних процесів та обладнання, що використовується, згідно ГОСТ 12.0.003-74 (1999) «Опасные и вредные производственные факторы. Классификация», виявляються небезпечні виробничі фактори, які при впливі на працюючих можуть призвести до погіршення умов праці або травматизму. Робоче місце представляє собою набір різноманітної комп’ютерної техніки з візуальними дисплейними терміналами та периферійні пристрої. Небезпека у ході робот буде присутньою при використанні джерел живлення, підключенні та відключенні приладів за допомогою вилок, розеток, перехідних пристроїв, подовжувачів.

Потенційні небезпеки фізичного характеру:

– ураження електричним струмом через несправність електрообладнання, підвищене значення напруги в електричному ланцюзі або недотримання вимог безпеки при його експлуатації, що може призвести до травми або летального результату;

– ураження статичним струмом, призводить до отримання неприємних відчуттів людиною та до виходу з ладу приладів;

– вплив електромагнітного випромінювання через підвищеній рівень електромагнітних випромінювань, що призводить до розладу центральної нервової системи та захворювань серцево-судинної системи.

Потенційні небезпеки психофізіологічного характеру:

– недотримання режиму роботи за ПК розумове перенапруження, перенапруження аналізаторів та емоційні перевантаження за, що призводять до підвищення стомлюваності, зниження уваги і, як наслідок, до можливості травмування працівника.

Потенційні небезпеки, пов’язані із порушенням санітарно гігієнічних вимог:

– погіршення самопочуття людини через підвищену чи знижену температури повітря робочої зони, внаслідок з’являються порушення обмінних процесів в організмі та виникають різні гострі і хронічні простудні захворювання відповідно;

– потрапляння в легені і на слизові оболонки пилу, через підвищену запиленість повітря робочої зони, що провокує появу алергічних захворювань органів зору та дихання;

– зорове стомлення і біль в очах, через недостатню освітленість робочої зони, які призводять до зниження уваги і можливості травмування;

– пошкодження органів слуху та роздратування підвищеним рівнем шуму на робочому місці внаслідок чого відбувається зниження гостроти слуху, порушується функціональний стан серцево-судинної та нервової систем.

Потенційні небезпеки, пов’язані з порушенням правил пожежної безпеки:

– ризик для здоров'я та життя персоналу, через недотримання правил протипожежної безпеки, що може призвести до травм, летального результату та матеріальних втрат;

Потенційні небезпеки, пов’язані з проявом наслідків надзвичайних ситуацій:

– отримання травм і матеріальних втрат, через неправильну поведінки персоналу при НС.

4.2 Заходи по забезпеченню техніки безпеки

Під час проектування систем електропостачання, монтажу силового електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог ПВЕ, ПТЕ, ПБЕ, СН 357-77 «Инструкция по проектированию силового осветительного оборудования промышленных предприятий», затверджених Держбудом, ГОСТ 12.1.006,

ГОСТ 12.1.030 «ССБТ. Электробезопасность. Защитное заземление, зануление», ГОСТ 12.1.019 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты», ГОСТ 12.1.045, ВСН 59-88 Держкомархітектури «Электрооборудование жилых и общественных зданий. Нормы проектирования», Правил пожежної безпеки в Україні, цих Правил, а також розділів СНіП, що стосуються штучного освітлення та електротехнічних пристроїв, та вимог нормативно-технічної та експлуатаційної документації заводу-виробника ЕОМ.

Для виключення ураження електричним струмом передбачено:

– організаційні заходи: проведення навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;

– технічні заходи: встановлення аварійного резервного вимикачу, який може повністю вимкнути електричне живлення приміщення, окрім освітлення, використовується підключення до мережі пристроїв за допомогою справних штепсельних з’єднань і електророзеток заводського виготовлення; проведено електромережу штепсельних розеток для живлення пристроїв уздовж стін приміщення, по підлозі поряд за стінами приміщення, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання; відповідність усіх пристроїв вимогам чинних в Україні стандартів нормативних актів з охорони праці, а також пристрої закордонного виробництва додатково відповідають вимогам національних стандартів держав – виробників і мають відповідну позначку на корпусі, в паспорті або іншій експлуатаційній документації; використання захисного заземлення та занулення згідно «Правил устрою електроустановок» («ПУЕ»).

Для виключення ураження статичним струмом та впливу електромагнітного поля застосовуються:

– організаційні заходи: проведення навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;

– технічні заходи: екранування джерела стендового харчування, згідно з ГОСТ 12.4.124-83 «Засоби захисту від статичної електрики. Загальні технічні вимоги»; використання покриття технологічних підлог з одношарового полівінілхлоридного антистатичного лінолеуму, для зниження величини виникаючих зарядів статичної електрики в робочому приміщенні; загальне і місцеве періодичне зволоження повітря.

Загальні заходи з техніки безпеки:

– перед початком роботи перевірка справності усіх приладів на робочому місці, очищення екрана відео терміналу від пилу та інших забруднень;

– після закінчення роботи відключення від електричної мережі усіх приладів, а також у разі виникнення аварійної ситуації негайне відключення усіх приладів від електричної мережі;

– дотримання режиму роботи з ПК та іншими приладами.

4.3 Заходи по забезпеченню виробничої санітарії та гігієни праці

Виробнича санітарія - система організаційних заходів і технічних засобів, що запобігають або зменшують дію шкідливих виробничих факторів на працюючих.

До шкідливих виробничих факторів відносяться:

– підвищена або знижена температура, вологість і рухливість повітря;

– підвищена запиленість і загазованість повітря;

– відсутність чи недолік природного світла; недостатня освітленість робочої зони; знижена контрастність об'єктів порівняно з фоном; прямі відблиски (прожекторне освітлення територій виробництв, світло фар

автотранспорту) і відображені відблиски (від пролитої води та інших рідин на поверхні територій виробництв);

– підвищена пульсація світлового потоку;

– підвищений рівень шуму, вібрації, ультра- та інфразвуку; підвищена напруга в електричному ланцюзі, замикання якої може відбутися через тіло людини; підвищений рівень статичної електрики.

Приміщення з ВДТ та ПЕОМ повинні бути обладнані системами опалення, кондиціювання повітря або припливно–витяжною вентиляцією відповідно до СНіП 2.04.05-91 «Опалення, вентиляція і кондиціонування».

Параметри мікроклімату, іонного складу повітря, вміст шкідливих речовин на робочих місцях, оснащених відео терміналами, відповідають вимогам пункту 2.4 СН 4088-86 «Санитарные нормы микроклимата производственных помещений», ГОСТ 12.1.005-88 «ССБТ Общие санитарно-гигиенические требования к воздуху рабочей зоны», СН 2152-80 «Санитарно-гигиенические нормы допустимых уровней ионизации воздуха производственных и общественных помещений» (табл.4.1 і табл.4.2).

Таблиця 4.1 – Норми мікроклімату у приміщенні

Пора року	Категорія робіт згідно ГОСТ 12.1-005-88	Температура повітря, град.С,	Відносна вологість повітря, %	Шкідливість руху повітря, м/с
		Оптимальна	Оптимальна	Оптимальна
Холодна	легка -1 а	22 – 24	40 – 60	0,1
	легка -1 б	21 – 23	40 – 60	0,1
Тепла	легка -1 а	23 – 25	40 – 60	0,1
	легка -1 б	22 – 24	40 – 60	0,2

Таблиця 4.2 - Рівні іонізації повітря приміщень

Рівні	Кількість іонів в 1 см куб. повітря	
	+ n	- n
Мінімально необхідні	400	600
Оптимальні	1500 – 3000	3000 – 5000
Максимально допустимі	50000	50000

Пил може здійснювати на людину фіброгенну дію, при якій в легенях відбувається розростання сполучних тканин, що порушує нормальну будову та функцію органу.

Основним напрямком в комплексі заходів по боротьбі з пилом є попередження її створення або надходження у повітря робочих приміщень. Найважливіше значення в цьому напрямку мають заходи технологічного характеру. Технологічні процеси, відповідні ГОСТ 12.1.005–88 «Загальні санітарно–гігієнічні вимоги до повітрю робочої зони», по можливості, проводяться таким чином, щоб освіта пилу було повністю виключено, або, принаймні, зведено до мінімуму. З цією метою потрібно максимально замінювати сухі порошать матеріали вологими, пастоподібними, розчинами і обробку їх вести вологим способом. При неможливості повного виключення пилоутворення, необхідно, шляхом відповідної організації технологічного процесу і використання відповідного технологічного обладнання, не допускати виділення пилу в повітря робочих приміщень. Це досягається, головним чином, шляхом організації безперервного технологічного процесу в повністю герметичній або, принаймні, максимально закритій апаратурі і комунікаціях.

Організація робочого місця користувача відео терміналу та ЕОМ повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ГОСТ 12.2.032 «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования», характеру та особливостям трудової діяльності.

Площа, виділена для одного робочого місця з відео терміналом або персональною ЕОМ, повинна складати не менше 6 м^2, а обсяг – не менше 20 м^3. Робочі місця з відео терміналами відносно світлових прорізів повинні розміщуватися так, щоб природне світло падало збоку, переважно зліва.

При розміщенні робочих місць з відео терміналами та персональними ЕОМ необхідно дотримуватись таких вимог:

– робочі місця з відео терміналами та персональними ЕОМ розміщуються на відстані не менше 1 м від стін зі світловими прорізами;

– відстань між бічними поверхнями відео терміналів має бути не меншою за 1,2 м;

– відстань між тильною поверхнею одного відео термінала та екраном іншого не повинна бути меншою 2,5 м;

– прохід між рядами робочих місць має бути не меншим 1 м.

Конструкція робочого місця користувача відео термінала (при роботі сидячи) має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; передпліччя – вертикально; лікті – під кутом 70-90^{o} до вертикальної площини; зап'ястя зігнуті під кутом не більше 20^{o} відносно горизонтальної площини, нахил голови –15–20^{o} відносно вертикальної площини.

Висота робочої поверхні столу для відео термінала має бути в межах 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400 мм, глибина – 800-1000 мм.

Для зниження статичного напруження м'язів рук необхідно застосовувати стаціонарні або знімні підлокітники довжиною не менше 250 мм, шириною – 50-70 мм, що регулюються по висоті над сидінням у межах 230±30 мм та по відстані між підлокітниками в межах 350-500 мм.

Екран відео термінала та клавіатура мають розташовуватися на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахуванням розміру алфавітно-цифрових знаків та символів. Відстань від екрана до ока працівника повинна складати:

– при розмірі екрану по діагоналі 35/38 см (14" /15") – 600-700 мм;

– при розмірі екрану по діагоналі 43 см (17") – 700-800 мм;

– при розмірі екрану по діагоналі 48 см (19") – 800-900 мм;

– при розмірі екрану по діагоналі 53 см (21") – 900-1000 мм.

Клавіатуру слід розміщувати на поверхні столу або на спеціальній,

регульованій за висотою, робочій поверхні окремо від столу на відстані 100-300 мм від краю, ближчого до працівника. Кут нахилу клавіатури має бути в межах 5-15'.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрану відео термінала, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля: по висоті 900-1300 мм, по глибині 400 – 500 мм.

При потребі високої концентрації уваги під час виконання робіт з високим рівнем напруженості суміжні робочі місця з відео терміналами та персональними ЕОМ необхідно відділяти одне від одного перегородками висотою 1,5-2 м.

Приміщення з ЕОМ повинні мати природне і штучне освітлення відповідно до ДБН В.2.5-28-2006 «Природне та штучне освітлення». Природне світло повинно проникати через бічні світло прорізи, зорієнтовані, як правило, на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5%. Розрахунки КПО проводяться відповідно до ДБН В.2.5-28-2006. Вікна приміщень з відео терміналами повинні мати регулювальні пристрої для відкривання, а також жалюзі, штори, зовнішні козирки тощо.

Штучне освітлення приміщення з робочими місцями, обладнаними відео терміналами ЕОМ загального та персонального користування, має бути обладнане системою загального рівномірного освітлення. У виробничих та адміністративно–громадських приміщеннях, де переважають роботи з документами, допускається вживати систему комбінованого освітлення (додатково до загального освітлення встановлюються світильники місцевого освітлення). Відношення яскравості екрану комп’ютера до яскравості оточуючих його поверхонь не повинно перевищувати у робочій зоні 3:1.

При розташуванні відео терміналів ЕОМ за периметром приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями.

Для забезпечення нормованих значень освітлення в приміщеннях з відео терміналами ЕОМ загального та персонального користування необхідно очищати віконне скло та світильники не рідше ніж 2 рази на рік, та своєчасно, проводити заміну ламп, що перегоріли.

Таблиця 4.3 - Норми освітленості в кабінетах і класах з ПК

Характеристика роботи	Робоча поверхня	Площина	Освітленість, лк	Примітка
Робота переважно з екранами дисплеїв ПК (50% та більше робочого часу)	Екран	В	200	не вище
	Клавіатура	Г	400	не нижче
	Стіл	Г	400	не нижче
Робота переважно з документами (з екранами дисплеїв ПК менше 50% робочого часу)	Екран	В	200	не вище
	Клавіатура	Г	400	не нижче
	Стіл	Г	500	не нижче
	Дошка	В	500	не нижче
Проходи основні	Підлога	Г	100	

Примітка. В - вертикальна площина, Г - горизонтальна площина. Загальне освітлення має бути виконане у вигляді суцільних або переривчатих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників. Допускається застосовувати світильники таких класів світлорозподілу:

– світильники прямого світла – П;

– переважно прямого світла – Н;

– переважно відбитого світла – В.

Приведемо розрахунок штучного освітлення для приміщення, розміри якого: довжина 5м, ширина 3м, висота 3м.

Розрахунок освітленості виконаємо методом коефіцієнта використання. Цей метод використовується для розрахунку загального рівномірного висвітлення горизонтальних поверхонь виробничих приміщень при відсутності затемнень.

Розрахунок освітлення методом коефіцієнта використання виконується по формулі:

$$\Phi = \frac{E \cdot S \cdot k \cdot z}{N \cdot \eta}, \quad (4.1)$$

де Φ – необхідний світловий потік ламп у кожнім світильнику, лм;

E – нормативна мінімальна освітленість, лк;

k – коефіцієнт запасу;

S – освітлювана площа, м^2;

z – коефіцієнт мінімальної освітленості, величина якого знаходиться в межах від 1,1 до 1,5 (при оптимальних відносинах відстані між світильниками до розрахункової висоти для ламп розжарювання і ДРЛ z=1,15 і для люмінесцентних ламп z = 1,1);

N – число світильників у приміщенні;

η – коефіцієнт використання світлового потоку.

Приймаємо: E=400 лк; k=1,5; z=1,1.

Освітлювана площа приміщення визначається по формулі:

$$S = A \cdot B, \quad (4.2)$$

де S – освітлювана площа;

A – довжина приміщення, м;

B – ширина приміщення, м.

Отримуємо $S = 5 \cdot 3 = 15$ м^2.

Розміщення світильників у приміщенні при системі загального висвітлення залежить від розрахованої висоти їхнього підвісу h, що звичайно задається розмірами приміщень.

Найбільш вигідне співвідношення відстані між світильниками до розрахункової висоти підвісу:

$$\lambda = \frac{L}{h}, \tag{4.3}$$

де L – відстань між рядами або сусідніми світильниками у ряду, м;

h – висота підвісу світильника над робочою поверхнею, м.

Для люмінесцентних ламп при косинусоїдальному типові кривої вибираємо $\lambda = 1{,}04$

Знаходимо розрахункову висоту підвісу по наступній формулі:

$$h = H - h_{‰} - h_p, \tag{4.4}$$

де H – висота приміщення, м;

$h_{‰}$ – висота звису світильника (від перекриття), м;

h_p – висота робочої поверхні над підлогою, м.

Приймаємо: Н=3,9 м, $h_{‰}$=0,7 м, h_p=0,8 м.

Тоді h=3,9– 0,7 – 0,8=2,4 м.

Відстань між світильниками визначаємо з формули (4.5):

$$L = \lambda \cdot h, \tag{4.5}$$

$L = 2{,}4 \cdot 1{,}04 = 2{,}5$ м

Визначаємо кількість світильників для установки в приміщенні:

$$N = \frac{S}{L^2}, \tag{4.6}$$

$$N = \frac{15}{2{,}5^2} = 2{,}4 \approx 3, \text{ шт.}$$

Для визначення коефіцієнта використання η знаходимо індекс приміщення *i*:

$$i = \frac{A \cdot B}{h \cdot (A + B)}, \tag{4.7}$$

де A і B – відповідно довжина і ширина приміщення, м;

h – розрахункова висота підвісу, м.

Отримуємо:

$$i = \frac{5 \cdot 3}{2{,}4 \cdot (5 + 3)} = 0{,}78.$$

Отримане значення і округляємо до найближчого табличного значення і приймаємо i = 0,78.

Оцінюємо коефіцієнти відображення поверхонь приміщення: стелі – ρ_i, стін – ρ_n, робочої поверхні – ρ_p. Приймаємо: ρ_i = 70%, ρ_n = 50%, ρ_p = 30%.

За отриманим значенням i і ρ визначаємо величину коефіцієнта використання світлового потоку для обраного світильника.

Вибираємо світильник типу ПВЛМ-Д, для якого η=73%. По формулі (4.1) визначаємо необхідний світловий потік ламп у кожнім світильнику:

$$\Phi = \frac{400 \cdot 15 \cdot 1.5 \cdot 1.1}{3 \cdot 0.73} = 4520{,}55 лм.$$

З довідкової літератури вибираємо необхідну лампу. Тип обраної лампи – ЛБ-30, $Ф_Л$=2180 лм. У приміщенні встановлюємо 3 світильники по 2 лампи у кожному, розміщені вони в один ряд.

Шум у певних умовах може мати значний вплив на здоров'я та поведінку людини. Шум може викликати роздратування і агресію, артеріальну гіпертензію (підвищення артеріального тиску), тиннитус (шум у вухах), втрату слуху.

Рівні звукового тиску в октавних смугах частот 250-4000 Гц не повинні перевищувати значень ,встановлених Санітарними нормами допустимих рівнів шуму на робочих місцях № 3223-85 «Санітарні норми допустимих рівнів шуму на робочих місцях» і ГОСТ 12.1.003-88 «Шум. Загальні вимоги безпеки».

Зниження шуму і вібрації, що впливають на людину, здійснюється наступними заходами:

– застосуванням звукоізолюючих пристроїв, для ізоляції шумних агрегатів;

– вибором раціонального режиму праці і відпочинку, скороченням часу перебування в галасливих умовах.

Рівні ультрафіолетового випромінювання не повинні перевищувати допустимих відповідно до СН № 4557-88 «Санітарні норми ультрафіолетового випромінювання у виробничих приміщеннях», затверджених Міністерством охорони здоров’я та ДСанПІН 3.3.2-007-98.

Гранично допустима напруженість електростатичного поля на робочих місцях не повинна перевищувати рівнів, наведених в ГОСТ 12.1.045 «ССБТ. Електромагнітні поля. Допустимі рівні на робочих місцях і вимоги до проведення контролю», СН № 1757–77 «Санітарно-гігієнічні норми допустимої напруги електростатичного поля» та ДСанПІН 3.3.2–007–98.

Потужність експозиційної дози рентгенівського випромінювання на відстані 0,05 м від екрана та корпуса відео термінала при будь-яких положеннях регулювальних пристроїв відповідно до Норм радіаційної безпеки України (НРБУ-97), затверджених постановою державного санітарного лікаря Міністерства охорони здоров’я України від 18.08.97 № 58, не повинна

перевищувати $7{,}74\times10^{-12}$ А/кГ, що відповідає еквівалентній дозі 0,1 мбер/год. (100 мкР/год.).

4.4 Заходи з пожежної безпеки

Пожежна безпека – це стан об’єкту, при якому виключається можливість пожежі, а у випадку її виникнення виключається дія на людей небезпечних факторів пожежі та забезпечується захист матеріальних цінностей.

Відповідно до Закону України «Про пожежну безпеку» пожежна безпека повинна забезпечуватися шляхом проведення організаційних, технічних та інших заходів, спрямованих на попередження пожеж, забезпечення безпеки людей, зниження можливих майнових втрат і зменшення негативних екологічних наслідків у разі їх виникнення, створення умов для швидкого виклику пожежних підрозділів та успішного гасіння пожеж.

Система активного пожежного захисту – це комплекс організаційних заходів і технічних засобів по боротьбі з пожежами і запобіганню дії на людей небезпечних чинників пожежі, а також обмеження матеріальних збитків від неї.

Основний напрямок діяльності пожежної охорони полягає у профілактиці пожеж і в обмеженні їх розмірів. Пожежі або вибухи на підприємствах завдають великих матеріальних збитків і майже завжди супроводжуються нещасними випадками з людьми (опіки, поранення) тощо.

Контроль за дотриманням затверджених відповідно до діючого законодавства норм і правил пожежної безпеки на об’єктах народного господарства здійснюють органи Державного пожежного нагляду (ДНП) управління пожежної охорони Міністерства надзвичайних ситуацій України.

Відповідальність за прийняття протипожежних заходів в організаціях покладається персонально на їх керівників без права передовіряти цю

відповідальність іншим, підлеглим їм особам, вони здійснюють загальне керівництво роботою в галузі пожежної безпеки підприємств і організацій.

На підприємстві встановлюються первинні засоби пожежогасіння відповідно до вимог Правил пожежної безпеки України. У приміщеннях з комп'ютерами рекомендується використовувати системи автоматичної пожежної сигналізації для виявлення пожежі та оповіщення працівників. Для приміщення, по якому проводиться розрахунок, потрібно влаштування місць утримання засобів пожежогасіння вогнегасників порошкових типу ОПУ–5 з вільним доступом у випадку необхідності їх використання.

Приміщення, згідно НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою» відноситься до категорії «Д», а клас можливої пожежі, згідно ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва», визначається, як «Е» (у зв'язку з тим що у приміщенні багато комп'ютерів).

Для даного класу пожежі підходять декілька типів вогнегасників, такі як: порошкові, хладонові та вуглекислі вогнегасники. Використовуючи ці дані згідно з НАПБ Б.03.001-2004 «Типові норми належності вогнегасників» та так як площа приміщення складає 15 м^2 достатньо одного порошкового вогнегасника об'ємом 5 літрів, ВВ5.

4.5 Заходи безпеки у надзвичайних ситуаціях

Для захисту життя та здоров'я в НС слід застосовувати наступні основні заходи цивільної оборони:

– укриття людей в пристосованих під потреби захисту населення приміщеннях виробничих, громадських і житлових будівель, а також у спеціальних захисних спорудах;

– евакуацію населення із зон НС;

– використання засобів індивідуального захисту органів дихання та шкірних покровів;

– проведення заходів медичного захисту;

– проведення аварійно-рятувальних та інших невідкладних робіт у зонах НС.

Укриття населення в пристосованих приміщеннях і в спеціальних захисних спорудах слід проводити за місцем постійного тимчасового перебування людей безпосередньо під час дії вражаючих чинників джерел НС, а також при загрозі їх виникнення.

Евакуація населення із зон НС. Евакуацію слід проводити у разі загрози виникнення або появи реальної небезпеки формування в цих зонах під впливом руйнівних і шкідливих сил природи, техногенних факторів та застосування сучасної зброї, критичних умов для безпечного перебування людей, а також при неможливості задовольнити стосовно жителів постраждалих територій мінімально необхідні вимоги і нормативи життєзабезпечення.

Евакуацію слід здійснювати шляхом організованого виведення та вивезення населення в довколишні безпечні місця, заздалегідь підготовлені за планами економічного і соціального розвитку відповідних регіонів, міст і населених пунктів та обладнані відповідно до вимог і нормативів тимчасового розміщення, забезпечення життя і побуту людей.

Використання засобів індивідуального захисту органів дихання та шкірних покривів. Засоби індивідуального захисту органів дихання і шкіри (ЗІЗ) в системі захисних заходів у зонах НС повинні запобігати наднормативні впливу на людей небезпечних і шкідливих аерозолів, газів і парів, що попали в навколишнє середовище при руйнуванні обладнання і комунікацій відповідних об'єктів, а також знижувати небажані ефекти дії на людину світлового, теплового та іонізуючого випромінювання.

В якості засобів індивідуального захисту органів дихання слід використовувати загальновійськові, цивільні і промислові протигази, що випускаються промисловістю, респіратори, простіші та підручні засоби.

В якості засобів індивідуального захисту шкіри слід використовувати загальновійськові захисні комплекти, різні захисні костюми промислового виробництва і простіші засоби захисту шкіри.

ЗІЗ, що випускаються промисловістю повинні бути направлено переважно для забезпечення особового складу формувань, що готуються для проведення рятувальних та інших невідкладних робіт в осередках ураження. Інше населення повинно використовувати простіші та підручні засоби.

Проведення заходів медичного захисту. Заходи медичного захисту населення при НС слід проводити з метою запобігання або зниження тяжкості уражень, шкоди для життя і здоров'я людей під впливом небезпечних і шкідливих факторів стихійного лиха, аварій і катастроф, а також для забезпечення епідемічного благополуччя в районах НС та у місцях дислокації евакуйованих. Дані цілі повинні досягатися застосуванням профілактичних медичних препаратів, антидотів, протекторів, стимуляторів резистентності, своєчасним наданням кваліфікованої медичної допомоги ураженим і їх спеціалізованим стаціонарним лікуванням до визначеного результату, імунопрофілактикою серед категорій осіб підвищеного ризику інфікування та проведенням інших протиепідемічних заходів.

Заходи медичного захисту в природних і техногенних НС слід планувати і здійснювати з використанням наявних сил і засобів міністерств і відомств, безпосередньо вирішують завдання захисту життя і здоров'я людей, а також спеціалізованих функціональних підсистем: екстреної медичної допомоги, санітарно-епідеміологічного нагляду, захисту та життєзабезпечення населення в НС, екологічної безпеки та інших, з їх нарощуванням шляхом створення і розгортання необхідної кількості медичних формувань і установ.

Першу медичну допомогу потерпілим до їх евакуації в лікувальні установи надають безпосередньо в осередках ураження в ході рятувальних та інших невідкладних робіт. Надання цієї допомоги слід здійснювати за участю заздалегідь сформованих для такої мети з самого населення санітарних постів

і санітарних дружин, до складу яких слід включати осіб, спеціально навчених загальним прийомам надання само- і взаємодопомоги і здатних організувати практичне виконання населенням цих прийомів в екстремальних умовах.

В рамках підготовки до виконання заходів медичного захисту населення в НС необхідно заздалегідь створювати також спеціальні медичні формування і установи; вести підготовку медичного персоналу; накопичувати медичні засоби захисту, медичного та спеціального майна і техніки для оснащення медичних формувань і установ; проводити профілактичні заходи і щеплення населенню, готувати до розгортання додаткову кінцеву мережу, розробляти режими поведінки і дії населення в НС.

Проведення аварійно-рятувальних та інших невідкладних робіт у зонах НС. Аварійно-рятувальні та інші невідкладні роботи в зонах НС слід проводити з метою термінового надання допомоги населенню, яке піддалося безпосереднього або опосередкованого впливу руйнівних і шкідливих сил природи, техногенних аварій та катастроф, а також для обмеження масштабів, локалізації або ліквідації виниклих при цьому НС.

Комплексом аварійно-рятувальних робіт необхідно забезпечити пошук і видалення людей за межі зон дії небезпечних і шкідливих для їх життя та здоров'я факторів, надання невідкладної медичної допомоги постраждалим і їх евакуацію в лікувальні установи, створення для врятованих необхідних умов фізіологічно нормального існування людського організму.

Невідкладні роботи повинні забезпечити блокування, локалізацію або нейтралізацію джерел небезпеки, зниження інтенсивності, обмеження розповсюдження та усунення дій полів вражаючих факторів в зоні лиха, аварії або катастрофи до рівнів, що дозволяють ефективно застосувати інші заходи захисту.

Аварійно-рятувальні та інші невідкладні роботи слід планувати і здійснювати з використанням сил і засобів міністерств і відомств, державних

міжгалузевих консорціумів, корпорацій, концернів і асоціацій, а також територіальних, функціональних і відомчих підсистем за належністю підконтрольних їм територій та об'єктів, які мають необхідними фахівцями (охорони здоров'я, охорони правопорядку, матеріально-технічного постачання, соціального забезпечення та інші) і технічними засобами, які придатні для використання в осередках ураження в цілях перевезень людей, у тому числі з травмами і пошкодженнями, виробництва демонтажних, монтажних, дорожніх, вантажно-розвантажувальних і земляних робіт; проведення дегазації, дезактивації, дезінфекції та інших спеціальних робіт.

У зонах ураження необхідно організувати життєзабезпечення населення і особового складу формувань, які залучаються до участі у рятувальних та інших невідкладних роботах.

Завчасна підготовка і введення в дію планів захисту населення в НС, зумовлених природними стихійними лихами, техногенними аваріями, катастрофами, а також застосуванням сучасної зброї, повинні передбачати проведення узгоджених за часом, цілям і засобам робіт з планування і здійснення комплексу організаційних, інженерно-технічних і спеціальних заходів цивільної оборони, а також формування необхідних для цього сил і засобів.

Планування, організація виконання і безпосереднє керівництво проведенням заходів щодо захисту населення в НС перебувають у компетенції органів виконавчої влади на місцях, постійно діючих територіальних, функціональних і відомчих ланок, спеціалізованих органів управління, сил і формувань ТЕ, диспетчерських (чергових) служб підприємств та інших об'єктів.

ВИСНОВКИ

В магістерській роботі досліджувались алгоритми роботи протоколів множинного доступу.

Основною метою роботи було визначення показників ефективності протоколів конкурентного доступу для моделі системи передачі інформації з пакетною передачею даних.

Дослідження проводились за допомогою програмного забезпечення MATLAB.

З проведеного моделювання протоколу ALOHA можна зробити наступні висновки:

а) якщо ефект захоплення не розглядається, то пропускна здатність близька до теоретичного значення навіть для заданої кількості терміналів – 100 користувачів;

б) якщо використовується ефект захоплення, то пропускна здатність каналу зв’язку стає більшою, також зменшується середній час затримки передачі.

Але, з результатів моделювання можемо побачити, що пропускна здатність протоколу S–ALOHA краща, за пропускну здатність протоколу ALOHA. Аналогічний висновок можна зробити і про суттєве зменшення значення середнього часу затримки для S–ALOHA.

Протокол множинного доступу з детектуванням несучої CSMA розглядається як вдосконалення основної схеми ALOHA. У цьому протоколі канал прослуховується відповідним пристроєм. Це означає, що якщо він зайнятий, тобто інший пристрій передає дані, то передавач переходить до режиму очікування до того моменту, доки канал не звільниться. Цей метод дозволяє суттєво покращити пропускну здатність системи.

Аналіз моделювання протоколу CSMA також свідчить, що максимум пропускної здатності виявився залежним від нормалізованого часу затримки.

Також можна зробити висновок, що максимальна пропускна здатність для схеми CSMA більша за пропускну здатність чистої схеми ALOHA і S–ALOHA.

Різниця між протоколами CSMA і ISMA полягає у тому, що зайнятість каналу визначається не шляхом прослуховування, а через надсилання базовою станцією пакета, в якому визначається статус каналу.

Як видно з моделювання, максимальна пропускна здатність протоколу ISMA залежить від нормалізованого часу затримки розповсюдження; також збільшується пропускна здатність при використанні ефекту захоплення, оскільки частину пакетів можна розглядати як успішно прийняті у точці доступу через суттєво різні потужності від різних користувачів у точці доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кабак В.С., Уваров Р.В. Функціональні пристрої телефонів мобільного зв'язку: Навчальний посібник. [Текст] / В.С. Кабак, Уваров Р.В. – Запоріжжя, 2007. – 375 с.

2. Вишневский В.М. Широкополосные беспроводные сети передачи информации. [Текст] / В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.В. Шахнович.– М.: Техносфера, 2005. – 592с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение [Текст] / Б. Скляр; Пер. с англ. ; – М.: Издательский дом "Вильямс" , 2003. – 1104с.

4. Harada H. Simulation and software radio for mobile telecommunications [Текст] / H. Harada, R. Prasad; – Artech House, 2003. – 465 p.

5. Столингс В. Беспроводные линии связи и сети. [Текст] / В.Столлингс ; Пер. с англ. ; – М. : Издательский дом "Вильямс" , 2003. – 604с.

6. Вишневский В.М., Портной С.Л, Шахнович И.В. Энциклопедия WiMAX. Путь к 4 G. –М. : Техносфера , 2009. – 472с..

7. Григорьев В. А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. [Текст] / – М. : ЭКО-ТРЕНДЗ , 2005. – 384с..

8. Феер К. Беспроводная цифровая связь. [Текст] / К. Феер; Пер. с англ. ; -М.: Радио и связь, 2000. – 519с.

9. Афанасьев В.В. Бизнес модели развития сетей мобильной связи / В.В. Афанасьев // Мобильные системы. – 2003. - №10. – С.35-42

Додаток А

Повний лістинг програм для моделювання протоколів

```
%main.m
%
%Packet communication system
%
%MATLAB version
%Programmed by M.Okita
%Checked be H.Harada
%
clear;

%definition of the global variable
global STANDBY TRANSMIT COLLISION PERMIT
global Srate Plen Ttime Dtime
global Mnum Mplen Mstime Mstate
global Tint Rint
global Spnum Splen Tplen Wtime
STANDBY =  0;                                   %definition of
the fixed number
TRANSMIT = 1;
COLLISION =  2;
PERMIT = 3;
                                                %definition of the
protocol
protocol = {'paloha'          %pure ALOHA         :  pno = 1
           'saloha'           %Slotted ALOHA      :  pno = 2
           'npcsma'           %np CSMA            :  pno = 3
           'snpisma'          %Slotted np CSMA    :  pno = 4
         };
                                                %definition of
communication channel
brate = 512e3;                                  %bit rate
Srate = 256e3;                                  %symbol rate
Plen = 128;                                     %length of a packet
Dtime = 0.01;                                   %normalized
propagation delay
alfa = 3;                                       %decline fixed number
of propagation loss
sigma = 6;                                      %standard deviation of
shadowing [dB]
r = 100;                                        %service area radius
[m]
bxy = [0, 0, 5];                                %proposition of the
access point(x,y,z) [m]
tcn = 10;                                       %capture ratio [dB]
                                                %definition of the
access terminals
```

```
Mnum = 100;                                    %number of the access
terminal
mcn = 30;                                      %C/N at the access
point when
                                               %transmitted from area
edge
                                               %simulation condition
pno = 4;                                       %protocol number
capture = 1;                                   %capture effect
0:nothing
                                               %
1:consider
spend = 10000;                                 %number of packets
that simulation is finished
outfile = 'test.dat';                            %name of file to
store the result
Ttime = Plen /Srate;                          %transmission time of
one packet
mpow = 10^(mcn/10)*sqrt(r^2+bxy(3)^2)^alfa; %true value of C/N
fid = fopen(outfile, 'w');
fprintf(fid,'Protocol                          = %d\n',pno);
fprintf(fid,'Capture                           = %d\n',capture);
fprintf(fid,'Normalize_delay_time              = %f\n',Dtime);
fprintf(fid,'Bit_rate(bps)                     = %d\n',brate);
fprintf(fid,'Symbol_rate(sps)                  = %d\n',Srate);
fprintf(fid,'Length_of_Packet(sbl)             = %d\n',Plen);
fprintf(fid,'Number_of_mobile_station          = %d\n',Mnum);
fprintf(fid,'Transmission_power(C/N)           = %f\n',mcn);
fprintf(fid,'Capture_ratio(dB)                 = %f\n',tcn);
fprintf(fid,'Number_of_Packet                  = %d\n',spend);
fprintf('\n*********Simulation Start*********\n\n');
if capture ==0
                fprintf('%s without capture effect\n\n',char
(protocol(pno)));
else
                fprintf('%s with capture effect\n\n',char
(protocol(pno)));
end
mxy = position (r, Mnum, 0);                          %positioning of
the access terminals
randn('state', sum(100*clock));                         %resetting of
the random table
mrnd = randn(1,Mnum);                                 %decision of
the shadowing
for G=[0.1:0.05:1,1.2:1:14]                           %offered
traffic
 if G>=Mnum
  break
end
Tint = -Ttime /log(1-G/Mnum);                         %expectation
value of the packet generation interval
Rint = Tint;                                          %expectation
value of the packet resending interval
```

```
Spnum = 0;
Splen = 0;
Tplen = 0;
Wtime = 0;
now_time = feval (char(protocol(pno)),-1);
                                                    %initialize of
the access terminals
while 1
     next_time = feval(char(protocol(pno)),now_time);

     if Spnum >= spend
         %disp(Spnum);
           break
     end
     idx = find(Mstate==TRANSMIT | Mstate==COLLISION);
     if capture ==0                                 %without
capture effect
             if length (idx) >1
               Mstate (idx) = COLLISION;          %collision
occurs
             end
    else                                                %with
capture effect
       if length (idx) >1
                dxy = distance (bxy, mxy(idx,:),1); %calculation
of the distance
                pow = mpow*dxy.^-alfa.*10.^(sigma/10*mrnd(idx));
%calculation of received power
       [maxp no] = max(pow);
            if Mstate(idx(no)) == TRANSMIT
              if length(idx) == 1
                  cn = 10*log10(maxp);
              else
                  cn = 10*log10(maxp/(sum(pow)-maxp+1));
              end
              Mstate(idx) = COLLISION;
              if cn >= tcn            %received power larger
than capture ratio
                 Mstate (idx(no)) = TRANSMIT;  %transmitting
success
              end
           else
              Mstate(idx) = COLLISION;
            end
       end
     end
 now_time = next_time;                          %time is
advanced until the next state change time
end
          traffic = Tplen / Srate / now_time;   %calculation of
the traffic
        ts = theorys(pno, traffic, Dtime);      %calculation of
the theory value of the throughput
```

```
fprintf(fid,'%f\t%f\t%f\t%f\t%f\t%f\t%f\n',G,now_time,Splen/Srat
e, Tplen/Srate, Wtime, Tint, Rint);
fprintf('G=%f\tS=%f\tTS=%f\n',traffic,Splen/Srate/now_time,ts);
end
fprintf('\n********* Simulation End *********\n\n');
fclose(fid);
graph(outfile);
%%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%%

%position.m
%
%Positioning of the access terminals in the area of the radius
r.
%
%Input arguments
% r : The radius r that an access point is an origin.
% n : The number of access terminals.
% h : h=0 - z=0 h=1 -> z=1-4
%
% Output argument
% posxy : (x,y,z)
%
%Programmed by M. Okita
%Checked by H. Harada
%
function [posxy] = position(r,n,h)
ms = 4*r;            %calculation of the number of maximum
position
ms = ms+4*sum(fix(sqrt(r^2-[1:r-1].^2)));
if n > ms
error('n exceeds the number of position.');
end
posxy = zeros(n,3); %initialize
   for ii=1:n
     while 1
         xx = round(r*rand)*sign(sin(2*pi*rand));  %x and y are
decided at random
         yy = round(r*rand)*sign(cos(2*pi*rand));
         if xx^2+yy^2 <= r^2 && (xx==0||yy==0)       % (xx,yy) is
not (0,0) in the area
           if isempty(find(posxy(:,1)==xx & posxy(:,2)==yy)) ==
0   % (xx,yy) are vacant
              break
           end
        end
     end
   posxy (ii, [1 2]) = [xx yy];
   if h==1
      while 1
          posxy (ii, 3) = round (50*rand) / 10;
          if 1 <=posxy (ii,3) && posxy (ii, 3) <=4
             break
          end
```

```
      end
   end
end
%%%%%%%%%% end of file %%%%%%%%%%

%distance.m
%
%The calculation of distance between access point and access
terminal
%
%Input arguments
%bstn     : coordinate of access point (x,y,z)
%mstn     : coordinate of access terminals (x,y,z) (mstn vector
or matrix)
%scl      : scale (if scl is omitted, scl=1.)
%
%Output argument
%d        : distance
%
%Programmed by M. Okita
%Checked by H. Harada
%
function [d] = distance (bstn, mstn, scl)
if nargin <3              %scl is omitted
   scl = 1;
end
[v,h] = size (mstn);
d = sqrt(sum(rot90(((repmat(bstn,v,1)-mstn)*scl).^2)));
%%%%%%%%%% end of file %%%%%%%%%%

%theorys.m
%
%The calculation of the theory value of the throughput
%
%Input arguments
%no:protocol number                          1 : Pure ALOHA
%                                            2 : Slotted ALOHA
%                                            3 : np-CSMA
%                                            4 : Slotted np-ISMA
% g:offered traffic (scalar or vector)
% a:normalized propagation delay
%
%Output argument
%ts:the theory value of the throughput (scalar or vector)
%
%Programmed by M. Okita
%Checked by H. Harada
%
function[ts] = theorys(no,g,a)
switch no
case 1                                  % Pure ALOHA
     ts = g.*exp(-2*g);
case 2                                  % Slotted ALOHA
```

```
     ts = g.*exp(-g);
case 3                                  % Non-Persistent Carrier
Sense Multiple Access
     ts = g.*exp(-a*g)./(g*(1+2*a)+exp(-a*g));
case 4                                  % Slotted Non-Persistent
ISMA
     ts = a *g.*exp(-a*g)./(1+a-exp(-a*g));
end
%%%%%%%%%% end of file %%%%%%%%%%

%graph.m
%
%The function of drawing the graph of simulation result
%Input argument
%filename : name of the file in which simulation result was
stored
%
%Output argument
%nothing
%
%Programmed by M. Okita
%Checked by H. Harada
%
function graph (filename)
filename='test.dat';
mtitle1 = {'Throughput of Pure ALOHA system'          %
definition of the title
           'Throughput of Slotted ALOHA system'
           'Throughput of np CSMA system'
           'Throughput of  Slotted np ISMA system'
     };
mtitle2 = {'Average Delay time of Pure ALOHA system' %
definition of the title
           'Average Delay time of Slotted ALOHA system'
           'Average Delay time of np CSMA system'
           'Average Delay time of Slotted ISMA system'
     };
fid      = fopen (filename,'r');
nul      = fscanf (fid, '%s', 2);
protocol = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
capture  = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
dtime    = fscanf (fid, '%f', 1);
nul      = fscanf (fid, '%s', 2);
brate    = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
srate    = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
plen     = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
mnum     = fscanf (fid, '%d', 1);
nul      = fscanf (fid, '%s', 2);
```

```
mcn      = fscanf (fid, '%f', 1);
nul      = fscanf (fid, '%s', 2);
tcn      = fscanf (fid, '%f', 1);
nul      = fscanf (fid, '%s', 2);
spend    = fscanf (fid, '%d', 1);
idx = 0;
while 1
   data0 = fscanf (fid, '%f', 1);
   data1 = fscanf (fid, '%f', 1);
   data2 = fscanf (fid, '%f', 1);
   data3 = fscanf (fid, '%f', 1);
   data4 = fscanf (fid, '%f', 1);
   data5 = fscanf (fid, '%f', 1);
   data6 = fscanf (fid, '%f', 1);
   if feof(fid) == 1                          %eof
     break
   end
   idx = idx+1;
   tg(idx) = data0;                           %offered traffic
   g(idx)  = data3 / data1;                   %actual offered
traffic
   s(idx)  = data2 / data1;                   %actual throughput
   w(idx)  = data4 / spend*srate/plen;        %average delay
end
fclose(fid);
ts = theorys(protocol, g, dtime);          %calculation of the
throughput
if protocol <3                             % Pure ALOHA &
Slotted ALOHA
   plot(g,s,'bo:',g,ts,'r-');              %normal graph
   legend('result', 'theory',0);           %legend
else                                       %np-CSMA & Slotted
np-ISMA
   semilogx(g,s,'bo:',g,ts,'r-');          %semilog graph
   if protocol == 3                        % legend
     legend (strcat('result(a=',num2str(dtime),')'),'theory',0);
   else
     legend (strcat('result(d=',num2str(dtime),')'),'theory',0);
   end
end
title(char(mtitle1(protocol)), 'FontSize', 16);            %title
xlabel('Traffic (Simulation result)', 'FontSize', 14);     %x
axis label
ylabel ('Throughput', 'FontSize', 14);                     %y
axis label
figure (2);                                %preparation of the
new graph windows (line-feed)
if protocol < 3                            %Pure ALOHA & Slotted
ALOHA
   plot (g,w,'bo:');                       %normal graph
   legend ('result');                      %legend
else                                       %np-CSMA & Slotted
np-ISMA
```

```
    semilogx (g,w,'bo:');                    %semilog graph
    if protocol == 3                         %legend
      legend (strcat ('result (a=',num2str(dtime),')'),0);
    else
      legend (strcat ('result (d=', num2str (dtime),')'),0);
    end
end
title(char(mtitle2(protocol)),'FontSize', 16);
%title
xlabel('Traffic(Simulation result)','FontSize', 14);        %x
axis label
ylabel('Average Delay time (packet)','FontSize', 14);       %y
axis label
%%%%%%%%%% end of file %%%%%%%%%%
```

Додаток Б

Лістинг програм для моделювання протоколу ALOHA

```
%paloha.m
%
%pure ALOHA System
%
%Input argument
%now_time  : now time but, now_time <0 initializes
%the access terminals
%
%Output argument
%next_time : next state change time
%
%Programmed by M. Okita
%Checked by H.Harada
%
function [next_time]=paloha(now_time)
global STANDBY TRANSMIT COLLISION          %definition of the
global variable
global Srate Plen
global Mnum Mplen Mstate
global Tint Rint
global Spnum Splen Tplen Wtime
persistent mgtime mtime                    %definition of the
static variable
if now_time < 0                             %initialize access
terminals
   rand('state', sum(100*clock));             %resetting of the
random table
   mgtime =-Tint*log(1-rand(1,Mnum));          %packet
generation time
   mtime =mgtime;                             %packet
transmitting time
   Mstate   =zeros(1,Mnum);
   Mplen(1:Mnum)=Plen;                        %packet length
   next_time=min(mtime);
   return
end
idx=find(mtime==now_time & Mstate==TRANSMIT); %findind of the
terminal which transmission succeeded
if length(idx)>0
   Spnum    =Spnum+1;
   Splen    =Splen+Mplen(idx);
   Wtime    =Wtime+now_time-mgtime(idx);
   Mstate(idx)=STANDBY;
   mgtime(idx)=now_time-Tint*log(1-rand);        %next packet
generation time
```

```
   mtime(idx) =mgtime(idx);                          %next packet
transmitting time
end
idx=find(mtime==now_time & Mstate==COLLISION);%finding of the
terminal which transmission failed
if length(idx)>0
   Mstate(idx)=STANDBY;
   mtime(idx)=now_time-Rint*log(1-rand(1,length(idx)));
%resending time
end
idx=find(mtime==now_time);                       %finding of the
terminal which transmission start
if length (idx)>0
   Mstate(idx) =TRANSMIT;
   mtime(idx)  =now_time+Mplen(idx)/Srate;          %end time of
transmitting
   Tplen       =Tplen+sum(Mplen(idx));
end
next_time=min(mtime);                            %next state change
time
%%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%%
```

Додаток В

Лістинг програм для моделювання протоколу S–ALOHA

```
%saloha.m
%
%Slotted ALOHA System
%
%Input argument
%now_time: now_time but, now_time<0 initializes the access
terminals
%
%Output argument
%next_time: next state change time
%
function[next_time]=saloha(now_time)
global STANDBY TRANSMIT COLLISION          %definition of the
global variable
global Srate Plen
global Mnum Mplen Mstate
global Tint Rint
global Spnum Splen Tplen Wtime

persistent mgtime mtime slot               %definition of the
static variable
if now_time < 0                            %initialize access
terminal
   rand('state', sum(100*clock));          %resetting of the
random table
   slot=Plen/Srate;                       %slot length
   mgtime=-Tint*log(1-rand(1,Mnum));
   mtime=(fix(mgtime/slot)+1)*slot;        %packet transmitting
time
   Mstate=zeros(1,Mnum);
   Mplen(1:Mnum)=Plen;                     %packet length
   next_time=min(mtime);
   return
end

idx=find(mtime==now_time & Mstate==TRANSMIT);   %finding of the
terminal which transmission succeeded
if length(idx) > 0
   Spnum=Spnum+1;
   Splen=Splen+Mplen(idx);
   Wtime=Wtime+now_time-mgtime(idx);
   Mstate(idx)=STANDBY;
   mgtime(idx)=now_time-Tint*log(1-rand);       %next packet
generation time
   mtime(idx)=(fix(mgtime(idx)/slot)+1)*slot;   %next packet
transmitting time
end
```

```
idx=find(mtime==now_time & Mstate==COLLISION);  %finding of the
terminal which transmission failed
if length(idx) > 0
   Mstate(idx)=STANDBY;
   mtime(idx)=now_time-Rint*log(1-rand(1,length(idx)));
%waiting time
   mtime(idx)=(fix(mtime(idx)/slot)+1)*slot;    %resending time
end
idx=find(mtime==now_time);                      %finding of the
terminal which transmission start
if length(idx) > 0
   Mstate(idx)=TRANSMIT;
   mtime(idx)=now_time+Mplen(idx)/Srate;        %end time of
transmitting
   mtime(idx)=round(mtime(idx)/slot)*slot;
   Tplen=Tplen+sum(Mplen(idx));
end
next_time=min(mtime);                           %next state
change time
%%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%%
```

Додаток Г

Лістинг програм для моделювання протоколу CSMA

```
%npcsma.m
%
%non-persistent CSMA System
%Input argument
%now_time: now time but, now_time<0 initializes the access
terminals
%
%Output argument
%next_time: next state change time
%
function[next_time]=npcsma(now_time)
global STANDBY TRANSMIT COLLISION          %definition of the
global variable
global Srate Plen
global Mnum Mplen Mstime Mstate
global Tint Rint
global Spnum Splen Tplen Wtime
persistent mgtime mtime                %definition of the static
variable
if now_time<0                              %initialize access
terminals
rand('state', sum(100*clock));             %resetting of the
random table
   mgtime=-Tint*log(1-rand(1,Mnum));          %packet generation
time
   Mstime=zeros(1,Mnum)-inf;                  %packet
transmitting time
   mtime=mgtime;                              %state change time
   Mstate=zeros(1,Mnum);
   Mplen(1:Mnum)=Plen;
   next_time=min(mtime);
   return
end
idx=find(mtime==now_time & Mstate==TRANSMIT);  %finding of the
terminal which transmission succeeded
if length(idx)>0
   Spnum=Spnum+1;
   Splen=Splen+Mplen(idx);
   Wtime=Wtime+now_time-mgtime(idx);
   Mstate(idx)=STANDBY;
   mgtime(idx)=now_time-Tint*log(1-rand);      %next packet
generation time
   mtime(idx)=mgtime(idx); %next packet transmitting time
end
idx=find(mtime==now_time & Mstate==COLLISION); %finding of the
terminal which transmission failed
if length(idx) > 0
```

```
   Mstate(idx)=STANDBY;
   mtime(idx)=now_time-Rint*log(1-rand(1,length(idx)));
%resending time
end
idx=find(mtime==now_time & Mstate==STANDBY);   %finding of the
terminal which carrier sensing
if length(idx) > 0
   Tplen=Tplen+sum(Mplen(idx));
   for ii=1:length(idx)
     jj=idx(ii);
     if carriersense (jj, now_time)==0         %channel is idle
       Mstate(jj)=TRANSMIT;                    %packet
transmitting
       Mstime(jj)=now_time;                    %start time of
transmitting
       mtime(jj)=now_time+Mplen(jj)/Srate;     %end of time of
transmitting
     else                                      % channel is busy
       mtime(jj)=now_time-Rint*log(1-rand);    %waiting time
     end
  end
end
next_time=min(mtime);                          %next state
change time
%%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%%

%carriersense.m
%
%The function of the carrier sense
%
%Input arguments
%no: terminal which carrier sensing
%now_time: now time
%
%Output argument
%result    : 0:idle  1:busy
%
function [result]=carriersense(no,now_time)
global Mnum Mstime Ttime Dtime         %definition of the global
variable
delay=Dtime*Ttime;                     %calculation of the delay
time
idx=find(((Mstime+delay)<= now_time) & (now_time <=
(Mstime+delay+Ttime)));  %carrier sense
if length(idx)>0                      %carrier is detected
   result=1;                           %channel is busy
else                                   %carrier can't be
detected
   result=0;                           %channel is idle
end
%%%%%%%%%% end of file %%%%%%%%%%
```

Додаток Д

Лістинг програм для моделювання протоколу ISMA

```
%snpisma.m
%
%Slotted non-persistent Isma System
%
%Input argument
%now_time: now time but, now_time<0 initializes the access
terminals
%
%Output argument
%next_time: next state change time
%
function[next_time]=snpisma(now_time)
global STANDBY TRANSMIT COLLISION PERMIT     %definition of the
global variable
global Srate Plen Dtime
global Mnum Mplen Mstime Mstate
global Tint Rint
global Spnum Splen Tplen Wtime
persistent mgtime mtime slot                 %definition of the
static variable
if now_time<0  %initialize access terminals
   rand('state',sum(100*clock));             %resetting of the
random table
   mgtime=-Tint*log(1-rand(1,Mnum));
   Mstime=zeros(1,Mnum)-inf;                 %packet
transmitting time
   mtime=mgtime;                             %inhibit sensing
time
   Mstate=zeros(1,Mnum);
   Mplen(1:Mnum)=Plen;                       %packet length
   next_time=min(mtime);                     %state change time
   slot=Plen/Srate*Dtime;                    %idle slot length
   return
end
idx=find(mtime==now_time & Mstate==TRANSMIT);%finding of the
terminal which transmission succeeded
if length(idx) > 0
   Spnum=Spnum+1;
   Splen=Splen+Mplen(idx);
   Wtime=Wtime+now_time-mgtime(idx);
   Mstate(idx)=STANDBY;
   mgtime(idx)=now_time-Tint*log(1-rand);     %next packet
generation time
   mtime(idx)=mgtime(idx);
end
```

```
idx=find(mtime==now_time & Mstate==COLLISION); %finding of the
terminal which transmission failed
if length(idx) > 0
   Mstate(idx)=STANDBY;
   mtime(idx)=now_time-Rint*log(1-rand(1,length(idx)));
%resending time
end
idx=find(mtime==now_time & Mstate==STANDBY);   %finding of the
terminal which inhibit sensing
if length(idx) > 0
   Tplen=Tplen+sum(Mplen(idx));
   for ii=1:length(idx)
     jj=idx(ii);
     if inhibitsense(jj,now_time)==0           %channel is idle
       Mstate(jj)=PERMIT;
       [temp1 kk]=max(Mstime);                 %calculation of
the transmitting start time slot
       if temp1 < 0
         mtime(jj)=ceil(now_time/slot)*slot;
       else
         temp1=temp1+Mplen(kk)/Srate;
         temp2=now_time-temp1;
         if temp2 < 0
           mtime(jj)=temp1+slot;
         else
           mtime(jj)=temp1+ceil(temp2/slot)*slot;
         end
       end
     else                                      %channel is busy
       mtime(jj)=now_time-Rint*log(1-rand);    %waiting time
     end
   end
end
idx=find(mtime==now_time & Mstate==PERMIT);    %finding the
terminal which transmission start
if length(idx) > 0
   Mstate(idx)=TRANSMIT;
   Mstime(idx)=now_time;
   mtime(idx)=now_time+Mplen(idx)/Srate;       %end time of
transmitting
end
next_time=min(mtime);                          %next state
change time
%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%

%inhibitsense.m
%
%The function of the inhibit sense
%
%Input arguments
%no: terminal which inhibit sensing
%now_time: now time
%
```

```
%Output argument
%inhibit  : 0:  idle    1: busy
function[inhibit]=inhibitsense(no,now_time)
global Mnum Mstime Ttime Dtime          %definition of the global
variable
delay=Dtime*Ttime;                      %calculation of delay
time
inhibit=0;
idx=find((Mstime+delay)<= now_time &
now_time<=(Mstime+delay+Ttime));  %inhibit sensing
if length(idx)>0
   idx=find(idx~=no);                    %escept itself
   if length(idx)>0                     %inhibit is detected
     inhibit=1;                          %channel is busy
   end
end
%%%%%%%%%%%%%% end of file %%%%%%%%%%%%%%
```