Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий інститут електроенергетики
(інститут)

Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Ігнатенка Михайла Вячеславовича
(ПІБ)

академічної групи 123-21-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Моделювання та оцінка якості передачі відео по бездротових мережах Wi-Fi на основі алгоритму Drop Tail»

(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Дмитрієва І.С.			
загального розділу	доц. Дмитрієва І.С.			
спеціального розділу	доц. Дмитрієва І.С.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
Гнатушенко В.В.

"25" січня 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавр

здобувача Ігнатенка Михайла Вячеславовича
академічної групи 123-21-1
спеціальності 123 Комп'ютерна інженерія
за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)
на тему "Моделювання та оцінка якості передачі відео по бездротових мережах Wi-Fi на основі алгоритму Drop Tail"
затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 №336-с

Розділ	Зміст	Термін виконання
Загальний розділ	На основі матеріалів виробничих практик, інших науково-технічних джерел показати актуальність завдання, сформулювати мету та задачі виконання кваліфікаційної роботи	10.02.2025
Спеціальний розділ	Розглянути питання, пов'язані з передачею відеоінформації по бездротовій Wi-Fi мережі при впровадженні на маршрутизатор різних алгоритмів управління чергою пакетів.	15.03.2025-31.05.2025
	Провести моделювання передачі відео по мережі з використанням алгоритмів управління чергою, отримати і проаналізувати показники продуктивності мережі	09.06.2025

Завдання видано _____ доц. Дмитрієва І.С.
(підпис керівника) (прізвище, ініціали)
Дата видачі 25.01.2025
Дата подання до екзаменаційної комісії 10.06.2025 р.
Прийнято до виконання _____ Ігнатенко М.В.

РЕФЕРАТ

Пояснювальна записка: 66 с., 28 рисунків, 22 джерел, 1 додаток.

Об'єктом дослідження є відеотрафік Wi -Fi мережі при впровадженні різних алгоритмів управління чергою.

Мета роботи: дослідити поведінку Wi -Fi мережі з відеотрафіком при впровадженні різних алгоритмів управління чергою.

Розглянуто питання, пов'язані з передачею відеоінформації по бездротовій Wi-Fi мережі при впровадженні на маршрутизатор різних алгоритмів управління чергою пакетів. Проведено моделювання передачі відео по мережі з використанням алгоритмів управління чергою, отримано і проаналізовано показники продуктивності мережі. Виявлено, що використання алгоритму Drop Tail призводить до зростання мережевої затримки пакета. Найбільш оптимальним для розглянутої мережі визнаний алгоритм Adaptive RED, що має параметри min_{th} = 15; max_{th} =45; max_p = 0,01; α =0,065; w_q = 0.031. Отримані результати дозволяють стверджувати, що використання алгоритму Adaptive RED дає можливість підвищити якість передачі відео, при цьому зменшуючи мережеві затримки.

АНАЛІЗ ЯКОСТІ ПЕРЕДАЧІ ВІДЕО, WI-FI МЕРЕЖА, ЧЕРГА ПАКЕТІВ, ADAPTIVE RED, DROP TAIL, RIO.

ЗМІСТ

ВСТУП 5
1 КЛАСИФІКАЦІЯ І ТЕХНОЛОГІЇ БЕЗДРОТОВИХ МЕРЕЖ 9
1.1. Класифікація мереж 9
1.2 Модель взаємодії відкритих систем 13
1.3 Методи доступу до середовища передачі в бездротових мережах .. 15
1.4 Мережі бездротового доступу WiMAX 23
1.4.1 Основні принципи побудови 23
1.4.2 Базова модель мережі 24
1.4.3 Профілі ASN 28
1.4.4 Підтримка мобільності 29
1.4.5. Керування радіоресурсом 33
2 ВИМОГИ МУЛЬТИМЕДІЙНИХ ДОДАТКІВ ДО МЕРЕЖІ 36
2.1 Параметри якості обслуговування, що впливають на якість передачі мультимедійної інформації 37
2.2 Алгоритми якості обслуговування 39
2.2.1 Диференційовані та інтегровані служби 39
2.2.2 Random Early Detection 40
2.2.3 Adaptive RED 42
3 ДОСЛІДЖЕННЯ МОДЕЛІ МЕРЕЖІ ПРИ ПЕРЕДАЧІ ВІДЕО 43
3.1 Опис моделі досліджуваної мережі 43
3.2. Алгоритм Drop Tail 45
3.3 Алгоритми RED 50
3.4 . Алгоритм Adaptive RED 53
ВИСНОВКИ 59
ПЕРЕЛІК ПОСИЛАНЬ 60
ДОДАТОК А 62

ВСТУП

Системи бездротової передачі даних існують практично стільки ж, скільки й сама людська цивілізація. Незважаючи на зміну технологій, суть залишається сталою — забезпечити взаємодію між окремими елементами мережі без використання дротів, передаючи інформацію в заданий час і напрямку. Особливо стрімкий розвиток бездротових технологій відбувається протягом останніх 10–15 років [1–10].

Розмежування дротових і бездротових систем зв'язку в сучасному розумінні почалося наприкінці XIX століття, коли телекомунікації вже зосереджувалися навколо двох основних завдань — передача голосу (телефонія) та передача текстових даних (телеграф). Перевага на той час надавалася дротовому зв’язку як більш надійному та захищеному, що започаткувало епоху дротових комунікацій. Земна інфраструктура активно розросталась мережею кабелів, а попит на інформаційні сервіси неухильно зростав [2-11]. Наприкінці XX століття телекомунікації зазнали значного прориву — почалася ера цифрової обробки сигналів. Голос, зображення та інші види інформації перед передаванням почали перетворюватися у цифрову форму. Це сприяло об'єднанню раніше розділених сфер — телефонії та передавання даних — у спільне середовище. Виникло поняття «мультимедіа», що охоплює інтеграцію голосу, відео та цифрових даних у єдиній інформаційній інфраструктурі [7-13]. Локальні і регіональні мережі проникли в усі сфери людської діяльності, включаючи економіку, науку, культуру, освіту, промисловість і т.д. Технологію Ethernet (10 Мбіт/с) замінили Fast Ethernet / Gigabit Ethernet (100/1000 Мбіт/с). Зміни торкнулися також і глобальних мереж (заміна X25 на Frame Relay). Сьогодні без них неможливі такі сервіси як електронна пошта, факсимільний та телефонний зв'язок, доступ до віддалених баз даних в реальному масштабі часу, служби новин, ICQ, дистанційне навчання, відеоконференції та ін. [8-14].

Бурхливий розвиток бездротових технологій як у всьому світі так і в Україні продиктований наступними об'єктивними перевагами бездротових рішень:

- гнучкість архітектури;
- швидкість проектування і розгортання;
- високий ступінь захисту від несанкціонованого доступу;
- відмова від дорогої і не завжди можливої прокладки кабелю.

Необхідно відзначити, що сучасні телекомунікаційні технології б'ються не тільки за обсяги і дальність передачі даних, але і за якість передачі і сумісність кількох типів трафіку. Методи забезпечення якості обслуговування (QoS) є сьогодні одним з найважливіших питань мережевих технологій, тому що без їх застосування неможлива якісна робота сучасних мультимедійних додатків, таких як IP-телефонія, відео- і радіомовлення. Ці методи оперують параметрами, що характеризують швидкість передачі даних, затримку пакетів і втрату пакетів. Методи забезпечення якості обслуговування фокусують увагу на впливі черг в комунікаційних пристроях на передачу трафіку. В них використовуються різні алгоритми управління чергами, резервування і зворотного зв'язку, що дозволяє знизити негативний вплив черг до прийнятного для користувачів рівня [12-22].

Черги є невід'ємним атрибутом мереж з комутацією пакетів. Сам принцип роботи таких мереж передбачає наявність буфера біля кожних вхідного і вихідного інтерфейсів комутатора пакетів. Буферизація пакетів під час перевантажень являє собою основний механізм підтримки трафіку, що забезпечує високу продуктивність мереж цього типу. З іншого боку, черги означають невизначену затримку при передачі пакетів через мережу, а це головне джерело проблем для чутливого до затримок трафіку. Так як сьогодні оператори пакетних мереж дуже зацікавлені у передачі мультимедійного трафіку, їм необхідні засоби забезпечення компромісу

між прагненням гранично завантажити свою мережу і виконанням вимог QoS одночасно для всіх типів трафіку.

У методах забезпечення якості обслуговування використовуються різні механізми, спрямовані на зменшення негативних наслідків перебування пакетів в чергах із збереженням водночас позитивної ролі черг. Для забезпечення необхідних вимог до різних потоків даних використовуються два методи QoS: управління перевантаженнями (congestion management) і запобігання перевантаженням (congestion avoidance). Перший метод заснований на присвоєння квот і пріоритетів потокам, і в разі перевантаження потоки отримують якість, обмежену їх квотою й пріоритетом (наприклад, WFQ - Weighted Fair Queuing). Другий метод обмежує розмір черги (наприклад, RED - Random early detection).

У даній роботі будуть розглянуті алгоритми запобігання перевантаженням і їх вплив на передачу відеотрафіку.

Метою роботи є дослідження поведінки Wi-Fi мережі з відеотрафіком при впровадженні різних алгоритмів управління чергою, таких як:

• Drop Tail

• Random Early Detection In / Out Coupled (RIO -C)

• Random Early Detection In / Out De - coupled (RIO -D)

• Adaptive Random Early Detection (Adaptive RED)

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Розглянути вимоги до мережі зі сторони мультимедійного трафіку і обмеження TCP/IP мереж.

2. Провести моделювання передачі по Wi -Fi мережі відео- і web-трафіку, з використанням алгоритмів управління чергою пакетів Drop Tail, RIO - C, RIO -D, Adaptive RED, що працюють на маршрутизаторі.

3. Проаналізувати вплив цих технологій на якість передачі відео. Оцінити розмір черги, загальну затримку в мережі, PSNR отриманого відео.

4. Оцінити вплив параметрів алгоритму Adaptive RED на затримки в мережі, а також якість передачі відео, ґрунтуючись на критерії PSNR (ПОСШ).

1 КЛАСИФІКАЦІЯ І ТЕХНОЛОГІЇ БЕЗДРОТОВИХ МЕРЕЖ

1.1. Класифікація мереж

Класифікація чого б то не було – завдання невдячне, оскільки і критеріїв класифікації можна розробити досить багато, і реальні об'єкти можуть не укладатися в чіткі межі певного класу, та й в міру розвитку усталені системи класифікації можуть застарівати. Все це справедливо і для бездротових мереж передачі інформації (БМПІ). Тому зупинимося на найбільш популярних способах ранжирування різних бездротових систем.

Зазвичай БМПІ поділяють за:

• способом обробки первинної інформації

- цифрові й аналогові;

• ширині смуги передачі

- вузькосмугові, широкосмугові і надширокосмугові;

• локалізацією абонентів

- рухливі і фіксовані ;

• географічної протяжності

- персональні, локальні, регіональні (міські) та глобальні;

• увазі переданої інформації

- системи передачі мови, відеоінформації та даних.

Цілком справедливі і симптоми градації на основі використовуваної технології (супутникові мережі, атмосферні оптичні лінії і т.п.), за призначенням та ін.

Практично всі розглянуті нами технології відносяться до цифрових бездротових широкосмугових систем. Наведемо їх відмінні ознаки, охарактеризувавши і «суміжні» системи.

Термін «бездротові» пояснюється легко – відсутній сполучний дріт (оптоволоконний або мідний кабель). Також відносно просто визначити:

цифрова система чи ні. До цифрових відносять системи, у яких вхідна аналогова інформація (наприклад, голос, аналоговий телевізійний сигнал і т.п.) спочатку перетворюється в цифрову (дискретну) форму. Проте, вже тут виникає деяка нечіткість. Справді, будь-який сигнал при передачі через фізичний канал має чисто аналоговий вигляд, він в принципі не повинен бути дискретним (чим далі форма сигналу від нескінченної синусоїди, тим більше паразитних гармонік і пов'язаних з ними неприємностей), чого домагаються спеціальними методами. Тому термін «цифрова система» говорить тільки про те, що в ній вхідні аналогові дані оцифровані і обробляються переважно цифровими методами.

Ще складніше з шириною смуги. Точного визначення тут немає. Зазвичай вважають, що якщо ширина спектральної смуги, в якій працює система, набагато менше центральної частоти цієї смуги, то система вузькосмугова. В іншому випадку система широкосмугова. Критерій дуже розпливчастий. Наприклад, система широкосмугова, якщо передатна функція каналу в цій смузі істотно змінюється залежно від частоти (тобто передатна функція в робочій смузі вузькосмугової системи практично не залежить від частоти). Очевидно, що визначення ці досить розпливчасті. У нашому випадку під терміном «широкосмугова система» ми будемо розуміти такі системи, де проявляються специфічні ефекти і властивості, пов'язані з широкою робочою смугою. Тому точний критерій не суттєвий, та й неможливий.

Поділ на мобільні і рухливі системи, здавалося б, досить простий, насправді також не є тривіальним. Слід розрізняти власне можливість мобільності абонентів, що надається технологією, і поділ на мобільні і фіксовані служби зв'язку, пов'язаний з питаннями частотного розподілу та ліцензування.

Найбільш характерним прикладом такої двозначності є історія появи бездротового телефонного зв'язку стандарту IS-95 (CDMA). Устаткування цього стандарту спочатку було дозволено до використання в країні тільки

для надання послуг фіксованого зв'язку. Однак, як відомо, IS- 95 є стандартом мобільного стільникового зв'язку.

Технологічно його ніяк не можна "зафіксувати". Аналогічна невизначеність склалася зараз і у супутникового зв'язку. Якщо ж говорити з технічної точки зору, обмежувати мобільність може чутливість технології зв'язку до швидкості руху абонента, складність переходу з однієї зони обслуговування в суміжну без розриву зв'язку, сприйнятливість до короткочасних зникнень зв'язку і т. п.

Поділ за розміром зони обслуговування також досить умовний, якщо розглядати сусідні градації. До персональних мереж (WPAN - wireless personal area network) відносять системи з радіусом дії від сантиметрів до кількох метрів (до 10-15 м). Основне призначення таких мереж полягає в заміщенні кабельної системи для зв'язку обладнання (наприклад, комп'ютера і периферійних пристроїв). При цьому потужність випромінювання передавачів, як правило, 1-10 мВт. Локальні мережі (WLAN wireless local area network) передбачають взаємну віддаленість пристроїв на відстані до сотень метрів і потужності передавачів близько 100 мВт. Ці мережі призначені для об'єднання пристроїв у межах локальної зони (будівлі, підприємства і т.п.). Відзначимо, що на основі стандартів локальних бездротових мереж цілком успішно будують і мережі міського масштабу. Наприклад, в цій якості використовують такі технології, як DECT і IEEE 802.11.

До мереж міського масштабу (регіональних) можна віднести безліч різних технологій. Це й наземне теле- і радіомовлення, і стільниковий зв'язок, і транкові системи. Нещодавно з'явилося сімейство стандартів на широкосмугові бездротові мережі міського масштабу IEEE 802.16. Якщо ж говорити про глобальні бездротові системи передачі даних, то вони представлені супутниковими системами зв'язку. Однак, з урахуванням того, що, наприклад, практично всі мережі стільникового телефонії так чи інакше пов'язані одна з одною, всі вони розробляються з урахуванням

можливості взаємодії, можна говорити і про глобальні стільникові мережі. Особливою градацією є поділ в залежності від типу інформації, що передається. Наприклад, на системи передачі мови (або відеоінформації) і несинхронних даних. З одного боку, мова - це один з видів інформації. Після оцифровки потік мовних даних за виглядом не відрізняється від потоку будь-якої іншої інформації. Розвиток цифрових технологій у різних галузях телекомунікацій (наприклад, і дротяної телефонії) давно продемонстрував ефективність цифрових методів обробки, коли і мова, і дані обробляються єдиними способами. З іншого боку, потреба в інформації різного виду вже зробила реальною інтеграцію різних інформаційних мереж (телефонія, телебачення, мережі передачі цифрових даних, телеметрія) на побутовому рівні. Єдиним каналом передаються дані різної природи. Тому, можна досить впевнено припустити, що недалекий той день, коли вся мовна інформація буде оброблятися виключно цифровими методами. Тут можна було б зупинитися, але виникає важливе питання. Кожному виду інформації властиві характерні вимоги при передачі. Людина відчуває затримку передачі мови, коли вона перевищує 0,25 с. При затримках близько 0,5 с сприйняття мови для багатьох стає неприйнятним. Причому справа не тільки власне у затримці, а й у неминучому при дуплексному зв'язку луна-сигналі, який при таких затримках усунути нереально. З іншого боку, мовна інформація малочутлива до спорадичних перешкод і втрат даних. Це означає, що при пакетній передачі мови важливо, щоб затримки поширення сигналу в каналі були мінімальними, а маршрутизація і відновлення потоку даних з пакетів (навіть якщо їх послідовність порушена) відбувалися в реальному часі. При цьому допустима навіть втрата окремих пакетів. Аналогічна ситуація і з передачею відеоінформації - затримка між прийомом окремих пакетів (наприклад, MPEG- 2) не повинна перевищувати певного заданого значення, але втрата пакета, як правило, допустима. Зовсім інші вимоги пред'являються до передачі телеметричної інформації, текстових даних і

т.п. Тут, як правило, не важливий режим реального часу (у певних межах), але і недопустима втрата даних. Врахування цих особливостей може призводити до створення особливих технологій, орієнтованих на трансляцію певних видів інформації.

Наведені вище міркування показують, що будь-яке визначення, так чи інакше ранжуюче БМПІ, не варто сприймати буквально і вже тим більше не треба дивуватися застосуванню тієї чи іншої технології «не за призначенням».

1.2 Модель взаємодії відкритих систем

Еталонна модель взаємодії відкритих систем (МВОС, OSI - open system interconnection) – це найбільш вдала спроба стандартизувати протоколи обміну інформацією. Вона була розроблена і затверджена ISO в тісній взаємодії з CCITT в 1984 р. МВОС не тільки стала основою для розробки мережевих стандартів, а й стала гарною методологічною основою для вивчення і порівняння мережевих технологій. Незважаючи на те, що були розроблені й інші моделі, більшість розробників і постачальників мережевих продуктів використовують термінологію еталонної моделі МВОС.

Відповідно до МВОС всі протоколи взаємодії систем поділяються на сім рівнів: фізичний, канальний (ланки даних), мережний транспортний, сеансовий, представницький і прикладний. Розглянемо коротко основні функції перерахованих рівнів.

Нижнім рівнем ієрархії є фізичний (Physical). Він визначає електричні і механічні характеристики підключення до фізичних каналах зв'язку, а також процедури передачі потоку бітів від одного вузла до іншого. Іншими словами, функції цього рівня - передати потік бітів між двома точками за заданим каналу зв'язку. Фізичний рівень надає сервіс для канального рівня або рівня ланки даних (Data link), відповідального за

передачу даних по каналу зв'язку між двома точками (вузлами мережі). До функцій канального рівня в першу чергу відносяться упаковка інформації в кадри певної довжини, формування контрольних сум і перевірка вмісту кадрів після їх передачі, формування підтверджень про прийом кадрів, повторна передача непідтверджених кадрів тощо.

Мережевий рівень (Network) забезпечує взаємодію між вузлом і мережею. Він формує мережеві адреси пакетів, управляє потоками, адресацією, маршрутизацією, організацією та підтримкою транспортних сполучень. Одиницею інформації протоколів мережевого рівня є пакет, тому іноді цей рівень називають пакетним.

Транспортний рівень (Transport) призначений для трансляції потоків даних з одного порту в інший. Під портом мається на увазі кінець логічного каналу мережі передачі даних, де фактично завершуються операції транспортування даних і починаються обчислювальні процеси. На цьому рівні відбувається прозора трансляція даних від передавача до приймача через як завгодно складну середу передачі - через різні мережі за допомогою мережевих і фізичних технологій. На транспортному рівні встановлюються і роз'єднуються транспортні сполучення, формуються пакети, що належать переданому в сеансі зв'язку потоку. Транспортний рівень останній в ієрархії МВОС, що забезпечує транспортний сервіс; він звільняє більш високі рівні від організації передачі даних.

Основне призначення сеансового рівня (Session) - організація, підтримка і закінчення сеансів (логічного зв'язку) між прикладними процесами. Сеанси встановлюються через рівень представлення (Presentation). Мета рівня представлення - перетворення даних у форму, зручну для прикладної програми. На цьому рівні перетворюються формати даних і команд. Прикладний рівень (Application) являє собою процес обробки інформації (прикладні процеси). Він забезпечує роботу прикладної програми так, як якби обмін даними відбувався б не через мережу передачі даних, а автономно та обчислювальної машині.

Відзначимо, що, незважаючи на безсумнівну корисність МВОС, не існує жодної комунікаційної системи, структурованої у відповідності з усіма сімома рівнями цієї моделі. І якщо між фізичним і канальним рівнем ще можна провести досить чітку межу, то останній вже розпадається на два підрівні – контролю доступу до середовища передачі (MAC - Medium Access Control) та управління логічним з'єднанням (LLC - Logical Link Control). Однак, МВОС внесла певний порядок в опис процедур взаємодії телекомунікаційних систем, і хоча б у цьому вона послужила добру службу.

1.3 Методи доступу до середовища передачі в бездротових мережах

Одна з основних проблем побудови бездротових систем - це вирішення завдання доступу багатьох користувачів до обмеженого ресурсу середовища передачі. Існує кілька базових методів множинного доступу (їх ще називають методами ущільнення або мультиплексування), заснованих на поділі між станціями таких параметрів, як простір, час, частота і код. Завдання множинного доступу - виділити кожному каналу зв'язку простір, час, частоту і/або код з мінімумом взаємних перешкод і максимальним використанням характеристик передатного середовища.

Множинний доступ з просторовим поділом заснований на поділі сигналів в просторі, коли кожен бездротовий пристрій може вести передачу даних тільки в межах однієї певної території (просторової області), на якій будь-якому іншому пристрою заборонено передавати свої повідомлення. Найпростіший спосіб просторового розділення - це обмеження потужності передавачів. Ще не так давно цей метод вважався малоефективним, до тих пір, поки не отримали промисловий розвиток системи, що забезпечують досить точну локалізацію зон дії окремих передавачів. З появою апаратури (і відповідних стандартів), що забезпечує

адаптивну перебудову потужності передавачів абонентських та базових станцій, а також систем на основі антен з перебудованою діаграмою спрямованості, даний метод отримав широке поширення.

Характерний приклад - системи стільникового телефонного зв'язку, системи із цифровим формуванням діаграм спрямованості та ін.

У схемах множинного доступу з частотним розділенням (Frequency Division Multiplexing - FDM) кожен пристрій працює на певній визначеній частоті, завдяки чому декілька пристроїв можуть вести передачу даних на одній території. Це один з найбільш відомих методів, що так чи інакше використовується в найсучасніших системах бездротового зв'язку. Характерний приклад схеми FDM - робота декількох радіостанцій на одній території, але на різних частотах. При цьому їх робочі частоти повинні бути розділені захисним частотним інтервалом, що дозволяє виключити взаємні перешкоди. Ця схема хоча й дозволяє використовувати безліч пристроїв на певній території, сама по собі призводить до невиправданого марнотратства зазвичай мізерних частотних ресурсів, оскільки вимагає виділення окремої частоти для кожного бездротового пристрою.

Більш гнучким є множинний доступ з часовим поділом (Time Division Multiplexing TDM). У даній схемі канали розподіляються за часом, тобто кожен передавач транслює сигнал на одній і тій же частоті, але в різні проміжки часу (як правило, циклічно повторюються) при чіткій синхронізації процесу передачі. Подібна схема досить зручна, оскільки часові інтервали можуть динамічно перевизначатися між пристроями мережі. Пристроям з великим трафіком призначаються більш тривалі інтервали, ніж пристроям з меншим обсягом трафіку.

Однак метод часового ущільнення не може використовуватися в чисто аналогових мережах. Навіть якщо вихідні дані аналогові (наприклад, мова), він вимагає їх оцифровки і розбиття на пакети. Швидкість передачі готельного пакета, як правило, істотно перевищує швидкість передачі вихідних оцифрованих даних.

Характерний приклад застосування часового ущільнення (в провідних мережах) - це метод передачі телефонного трафіку за допомогою каналів E1. Основний недолік систем з часовим ущільненням - це миттєва втрата інформації при зриві синхронізації в каналі, наприклад, через сильні перешкод, випадкових або навмисних. Однак, успішний досвід експлуатації таких знаменитих TDM-систем як стільникові телефонні мережі стандарту GSM свідчить про достатню надійність механізму часового ущільнення. Ще один тип множинного доступу - це мультиплексування з кодовим розділенням (Code Division Multiplexing CDM). Спочатку через складність реалізації дана схема використовувалася у військових цілях, але з часом міцно зайняла свою позицію в цивільних системах. Іменем заснованого на CDM механізму поділу каналів (CDMA CDM Access) навіть названий стандарт стільникового телефонного зв'язку IS- 95a, а також ряд стандартів третього покоління стільникових систем зв'язку (CDMA2000, WCDMA та ін.) У даній схемі всі передавачі передають сигнали на одній і тій же частоті, але з різними базовими кодами.

Принцип кодового ущільнення ілюструє ситуація, коли багато людей в одній кімнаті розмовляють на різних мовах. При цьому кожна людина розуміє тільки одну певний мову. Для кожного розмова незрозумілою мовою буде сприйматися як нічого не значущий шум, позбавлений корисної інформації. А на тлі цього шуму він буде сприймати потік інформації на зрозумілій йому мові. У схемі CDM кожен передавач замінює кожен біт вихідного потоку даних на CDM-символ - кодову послідовність довжиною в 11, 16, 32, 64 і т.п. біт (їх називають чипами). Кодова послідовність унікальна для кожного передавача, причому їх підбирають так, щоб кореляція двох будь-яких CDM-кодів була мінімальна (а в ряді випадків - щоб автокореляція CDM-коду при фазовому зсуві була також мінімальна). Як правило, якщо для заміни 1 у вихідному потоці

даних використовують якийсь CDM-код, то для заміни 0 застосовують той же код, але інвертований.

Найбільш сильна сторона даного ущільнення полягає в підвищеній захищеності і прихованості передачі даних: не знаючи коду неможливо отримати сигнал, а в ряді випадків - і виявити його присутність. Крім того, кодовий простір незрівнянно більш значний в порівнянні з частотної схемою ущільнення, що дозволяє без особливих проблем привласнювати кожному передавачу свій індивідуальний код. Основною ж проблемою кодового ущільнення до недавнього часу була складність технічної реалізації приймачів і необхідність забезпечення точної синхронізації передавача і приймача для гарантованого отримання пакета.

Відзначимо, що ущільнення з кодовим поділом - метод синтетичний, тобто він базується на частотному або часовому методі ущільнення. У найбільш «чистому» вигляді метод кодового ущільнення реалізується в разі DSSS. Крім того, відомі і використовуються методи розширення спектру за допомогою частотних і часових стрибків (відповідно FHSS - Frequency Hoping Spread Spectrum і THSS Time Hoping Spread Spectrum). У разі розширення спектру за допомогою частотних стрибків (ще його називають методом псевдовипадкової перебудови робочої частоти - ППРЧ) в заданому частотному діапазоні F одночасно працює кілька передавачів, кожен у вузькій смузі, у багато разів менший F. Центральна частота кожного передавача в ході роботи дискретно змінюється за законом, що задається унікальною для нього кодовою послідовністю. Приймач знає цю кодову послідовність і перебудовується за частотою прийому синхронно з передавачем. Кодові послідовності вибирають так, щоб мінімізувати ймовірність одночасної роботи двох передавачів. Тим самим забезпечується певний захист від прослуховування і перешкод.

Даний метод в ряді випадків виявляється досить ефективним і застосовується, зокрема, в такій популярній сьогодні технології БМПІ, як Bluetooth.

Як правило, описані схеми в бездротових мережах використовуються в поєднанні один з одним. Наприклад, для мобільних мереж GSM одночасно використовуються схеми ущільнення SDM, TDM і FDM, в системах стандарту IEEE 802.16 ефективно поєднуються технології OFDM, CDM, FDM / TDM і SDM [15-22].

Розглянуті вище механізми - це способи поділу єдиного ресурсу на канали передачі. Однак, ці канали треба ще призначити конкретним пристроям. Розглянемо кілька найбільш популярних схем розподілу канальних ресурсів на базі технології TDM (аналогічні механізми можливі й при інших методах ущільнення).

Найпростіший алгоритм для схеми ущільнення TDM - це фіксований розподіл часових інтервалів між різними пристроями. Розподілом займається базова станція (центральний пристрій), яка повідомляє кожному абонентському пристрою час початку передачі. Подібна схема ідеально підходить для бездротових мереж, які мають фіксовану пропускну здатність. Однак вона не оптимальна у випадку нерегулярної передачі, оскільки під час мовчання пристрою його інтервал не може бути використаний іншою терміналом. Тому число абонентських станцій (або допустима швидкість передачі) принципово і суттєво обмежене.

Протилежністю даної схеми є механізм повністю випадкового доступу або класична схема Aloha. У ній при передачі даних мобільним пристроєм не використовується який-небудь алгоритм, що дозволяв би уникнути колізій (одночасної роботи двох передавачів в один час на одній частоті). Це означає, що будь-який пристрій може передавати дані в будь-який час і немає ніякої гарантії, що ці дані будуть успішно доставлені отримувачу. Дана схема - один з найперших механізмів доступу для систем бездротового зв'язку. Вона була розроблена в 70 -х роках в Гавайському університеті і застосовувалася в мережі ALOHANET для бездротового з'єднання кількох станцій (університетських будинків, що розташовувалися на різних островах Гавайського архіпелагу). Ця схема

добре працює в мережах зі слабким завантаженням, тобто в мережах, що мають мале число пристроїв або передаючих невелику кількість інформації в одиницю часу. При пуасонівському розподілі інтенсивності генерації пакетів пристроями максимальна пропускна здатність системи досягається вже при 18 % завантаженні.

Удосконаленням основної схеми Aloha з'явився метод множинного доступу з детектуванням несучої (Carrier Sense Multiple Access - CSMA).

Детектування несучої частоти означає лише те, що канал прослуховується пристроєм. Якщо він зайнятий, тобто інший пристрій передає дані, то передавач переходить у режим очікування до того моменту, коли канал стане вільним. Цей метод дозволяє значно поліпшити пропускну здатність системи. Як і в методі випадкового доступу, в даній схемі не потрібно наявності центрального пристрою, тобто кожен пристрій приймає рішення про передачу самостійно. Оскільки фактично доступ до середовища отримує та станція, яка першою почала передачу, даний механізм ще називають методом конкурентного доступу.

Існує кілька версій схеми CSMA. При використанні нестійкою схеми CSMA станції слухають канал і, якщо канал вільний, негайно починають передачу. Якщо канал зайнятий, станція перед повторним визначенням стану каналу вичікує випадковий проміжок часу, після чого знову слухає канал. Якщо канал вільний, то термінал передає дані. У Р-наполегливих схемах CSMA вузли теж визначають стан каналу, але дані передаються з імовірністю *P*. Пристрій може відкласти передачу до наступного часового інтервалу з імовірністю *1-P*, тобто здійснюється додатковий поділ доступу до середовища. У йнаполегливих системах CSMA всі станції, яким необхідно передавати дані, одночасно отримують доступ до середовища, як тільки воно звільняється.

Іншою варіацією даного методу є CSMA/CA (CA - Collision Avoidance, із запобіганням конфліктів), що використовується в бездротових ІТТ стандарту IEEE 802.11. Тут після визначення незайнятості

каналу час очікування вибирається випадково в деякому часовому проміжку. У специфікації HIPERLAN 1 використовується схожа схема - безпріоритетний множинний доступ з виключенням (Elimination Yield - Non- Preemptive Multiple Access, EY - NPMA).

Схема з цифровим детектуванням (DSMA - Digital Sense Multiple Access) використовує схожий з CSMA/CA принцип роботи. Цей метод також називають множинним доступом з детектуванням придушення (Inhibit Sense Multiple Access - ISMA). Різниця полягає в тому, що зайнятість каналу визначається не шляхом прослуховування, а за допомогою посилки базовою станцією пакета, в якому визначається статус каналу. У даній схемі базова станція повинна бути синхронізована з передавачами так, щоб передавачі не передавали дані під час передачі статусу каналу. Якщо канал зайнятий, то станції чекають випадкового проміжку часу для подальшої передачі. Оскільки кілька станцій можуть одночасно передати дані, центральна станція посилає пакет з підтвердженням про отримання пакету даних.

У сучасних БМПІ, як правило, використовують поєднання механізмів централізованого призначення часових інтервалів і методів конкурентного доступу. Тобто робота цих систем відбувається в два етапи.

Перший етап - резервування ресурсів (часових інтервалів) для майбутньої передачі. На цьому етапі всі станції заявляють (намагаються заявити) про свої потреби в канальних ресурсах. На другому етапі відбувається безпосередня передача даних у відведеному часовому інтервалі. У цих схемах використовується центральний термінал, за допомогою якого проводиться синхронізація передач і здійснюється резервування. Як правило, механізми резервування призводять до збільшення часу затримки отримання пакетів при слабкій завантаженні системи, але при цьому забезпечують їй більш високу пропускну здатність.

Прикладом подібного механізму є схема множинного доступу з розподілом за запитом (Demand Assigned Multiple Access DAMA), названа

також схемою Aloha з резервуванням. Вона, зокрема, застосовується в супутникових системах зв'язку. Протягом певного часового інтервалу, розбитого на міні-інтервали, всі станції намагаються зарезервувати для себе майбутні часові інтервали для передачі даних. Оскільки на стадії резервування відбуваються конфлікти, деяким станціям не вдається зарезервувати канальний ресурс. Якщо станції вдалося зарезервувати часовий інтервал, то жодна інша станція не зможе в цей час здійснювати передачу. Таким чином, базова станція збирає всі успішні запити (решта ігноруються) і посилає назад список із зазначенням прав доступу до подальшим часових інтервалах. Цьому списку підкоряються всі станції.

Схема DAMA відноситься до схем з явним резервуванням, коли кожен інтервал для передачі резервується явно. Схема TDMA з резервуванням відрізняється від попередньої схеми тим, що етап резервування відбувається не на підставі конкурентного доступу, а за звичайною фіксованою схемою TDMA. Кожному пристрою призначається часовий міні-інтервал, протягом якого він повідомляє, чи буде передавати дані. Тому на початку кожного циклу передачі базова станція передає пакет, розбитий на N інтервалів, в кожному з яких зазначено, зарезервований канал чи ні. Потім слідують N інтервалів для даних. Даний метод гарантує кожній зарезервували канал станції певну пропускну здатність. Решта станції можуть пересилати дані протягом інтервалів, які ніхто не зарезервував , але вже на принципах конкурентного доступу без гарантії доставки пакетів. Схема з резервуванням пакетів (PRMA - Packet Reservation Multiple Access) є прикладом з прихованим резервуванням, оскільки інтервали резервуються неявно. Центральний пристрій на початку кожного циклу розсилає список з розподілом часових інтервалів. Саме ж резервування відбувається за іншою схемою. Уявімо, що якому-небудь пристрою необхідно передати дані, але при цьому він не зарезервував часовий інтервал. Цей пристрій регулярно отримує список з зарезервованими інтервалами. Приміром, в отриманому списку вказано,

що третій, п'ятий і восьмий інтервали не зарезервовані, тобто вільні. Пристрій випадковим чином приймає рішення про те, в якому інтервалі можна спробувати передавати дані. Наприклад, пристрій передає повідомлення на п’ятий інтервал. Якщо передача пройшла успішно, пристрій отримує про це підтвердження . Базова станція резервує цей канал для нового пристрою і включає його в свій список. Якщо запит не дійшов до базової станції, пристрій повинен спробувати знову послати дані в один з вільних інтервалів.

1.4 Мережі бездротового доступу WiMAX

1.4.1 Основні принципи побудови

Мережа WiMAX являє собою сукупність бездротового і базового (опорного) сегментів. Перший описано в стандарті IEEE 802.16, другий визначено специфікаціями WiMAX-форуму. Базовий сегмент — зв’язок БС одна з одною, зв’язок з локальними та глобальними мережами і т.д. Він не належить до радіомережі. Базовий сегмент ґрунтується на IP-протоколах (IETF RFC) і стандартах Ethernet (IEEE 802.3-2005). Однак власне архітектура мережі, у тому числі механізми аутентифікації, криптозахисту, роумінгу, хендовери тощо (у частині, що не належить до бездротової мережі), описані в документах WiMAX Forum Network Architecture. Специфікації мережі WiMAX засновані на технології пакетної комутації, протоколах IP і Ethernet і доповнюють їх у міру необхідності. Архітектура WiMAX-мережі повинна забезпечувати незалежність архітектури мережі доступу, враховуючи радіомережу, від функцій і структури транспортної IP-мережі. Мережа WiMAX повинна легко масштабуватися і гнучко змінюватися, ґрунтуватися на принципах декомпозиції (тобто будуватися на основі стандартних логічних модулів, об’єднаних через стандартні інтерфейси). Масштабованість і гнучкість можлива за таких експлуатаційних параметрів, як щільність абонентів,

географічна протяжність зони покриття (районна, міська або приміська мережа), частотні діапазони, топологія мережі (ієрархічна, плоска, mesh і т.д.), мобільність абонентів.

1.4.2 Базова модель мережі

Базова модель (БМ) мережі WiMAX — це логічне уявлення мережевої архітектури WiMAX. Термін «логічне» у даному випадку означає, що модель розглядає набір стандартних логічних функціональних модулів і стандартних інтерфейсів (точок поєднання цих модулів). Під час практичної реалізації один пристрій може мати декілька функціональних елементів або, навпаки, функція може бути розподілена між різними пристроями.

БМ включає три основні елементи – безліч абонентських (мобільних) станцій (МС), сукупність мереж доступу (сервісна мережа доступу, ASN) і сукупність мереж підключення (CSN). Крім того, у БМ входять так звані базові точки (R1-R8) (рис. 1.1). Мережі ASN належать провайдеру мережі доступу (NAP) — організації, яка надає доступ до радіомережі для одного або декількох сервіс-провайдерів WiMAX (NSP). У свою чергу, сервіс-провайдер WiMAX – організація, що надає IP-з'єднання та послуги WiMAX кінцевим абонентам. У межах даної моделі вже сервіс-провайдери WiMAX укладають угоди з Інтернет-провайдерами, операторами інших мереж доступу, угоди про роумінг і т.д. Сервіс-провайдери щодо абонента можуть бути домашніми і гостьовими, кожен — зі своєю мережею CSN. Мережа доступу ASN являє собою велику кількість базових станцій (БС) бездротового доступу за стандартом IEEE 802.16 і шлюзів для зв'язку з транспортною IP-мережею (тобто локальною або глобальною мережею передачі інформації) (рис. 1.2). Фактично ця мережа пов'язує радіомережу IEEE 802.16 і IP-мережу. ASN включає як мінімум одну БС і як мінімум один ASN-шлюз. Але і БС, і шлюзів в одній ASN може бути декілька, причому одна БС може бути логічно пов'язана з декількома шлюзами.

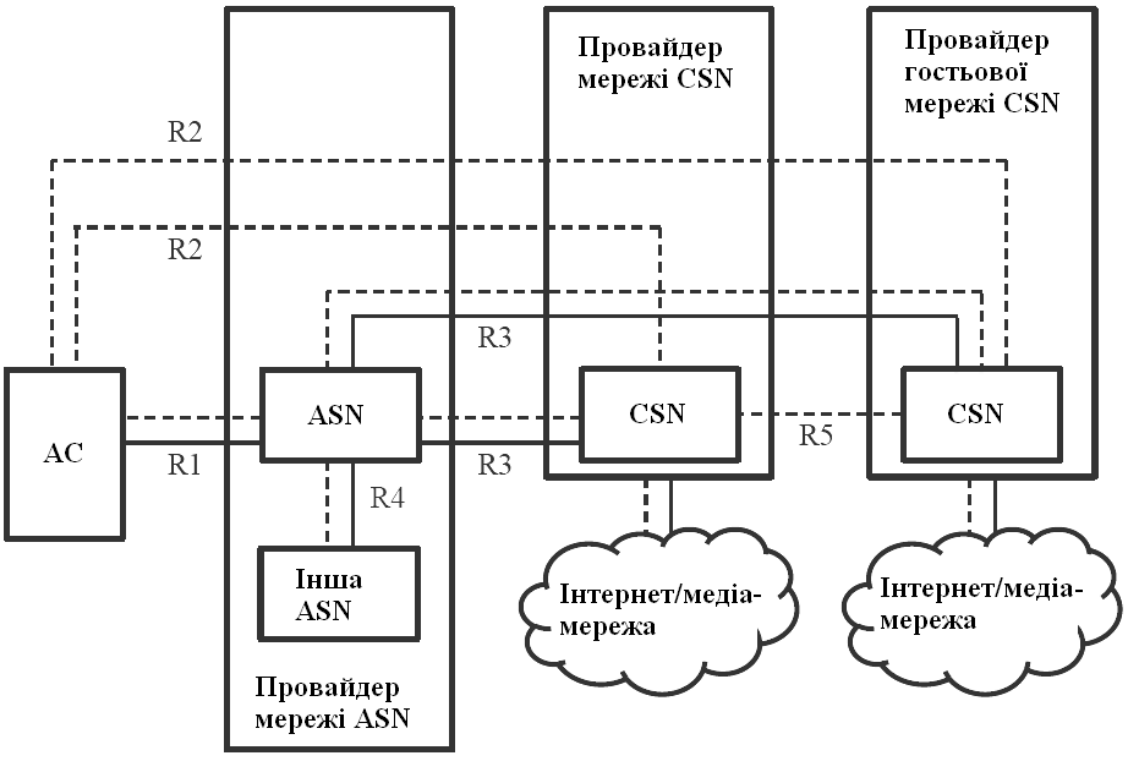

Рисунок 1.1 – Базова модель мережі WiMAX:

- - - - - потоки даних; —— потоки керування

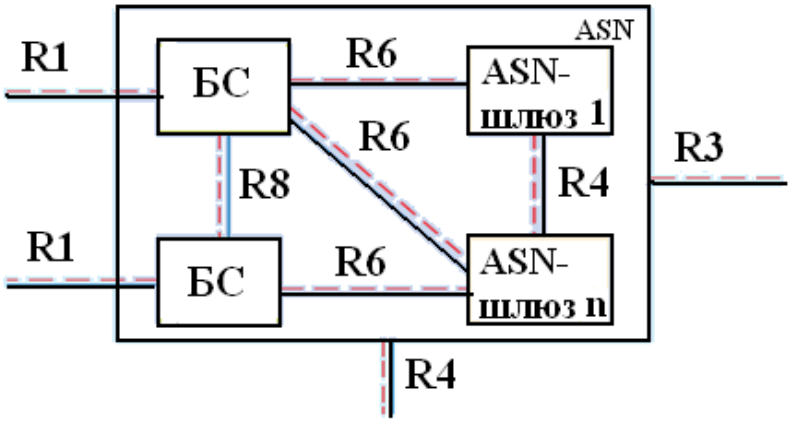

Рисунок 1.2 – Логічна модель мережі доступу ASN

БС у межах даної моделі – це логічний пристрій, що підтримує набір протоколів IEEE 802.16 і функції зовнішнього сполучення. Логічна БС односекторна, з одним частотним номіналом. Очевидно, що реальна БС являє собою набір декількох логічних БС. Шлюз ASN — це також логічний пристрій, що зв’язує БС одного ASN з іншими мережами доступу

і мережею підключення CSN. Шлюз ASN забезпечує зв'язність як на рівні каналів передачі даних, так і на рівні керування. Для кожної МС базова станція логічно пов'язана з одним шлюзом. Але реально функції ASN-шлюзу для кожної МС можуть бути розподілені між кількома шлюзами, що належать одній або декільком мережам доступу. Шлюз ASN опціонально може бути представлений як сукупність двох груп функціональних елементів – блока рішення (DP – Decision Point) і блока виконання (EP-Enforcement Point). EP реалізує функції, пов'язані з передачею потоку даних, у той час як у DP зосереджені функції, безпосередньо не пов'язані з передачею даних (наприклад, функції контролера керування радіоресурсу мережі). Ці два функціональні модулі з'єднані через базову точку R7. Ніде докладно вона не розкрита, але без згадки про можливість такої декомпозиції функцій ASN-шлюзу неможливо пояснити наявність R7. Загалом розподіл функцій між реальними шлюзами і БС визначений так званими профілями ASN. На сьогодні їх затверджено три (A, B і C).

Мережа підключення CSN – це власне мережа оператора WiMAX, саме в ній реалізуються функції керування авторизацією, аутентифікацією і доступом (AAA), підключення абонентів WiMAX до глобальних IP-мереж, надання таких послуг, як IP-телефонія, доступ до телефонних мереж загального користування, доступ до Інтернету і приватних мереж тощо. Важливо відзначити, що БМ мережі WiMAX припускає, що однією мережею доступу ASN можуть користуватися кілька сервіс-провайдерів WiMAX. І навпаки, одна CSN може підключатися до мереж різних провайдерів доступу. У CSN реалізовані такі функції, як надання мобільним абонентам IP-адрес і інших мережевих параметрів на період мережевої сесії, сервер політик/контролю доступу та зберігання профілів абонентів, передача (тунелювання) даних між мережами доступу та підключення, білінг абонентів WiMAX і міжоператорські розрахунки, тунелювання даних між різними CSN у разі роумінгу, забезпечення

мобільності під час виходу МС за межі однієї ASN. Підтримуються такі WiMAX-послуги, як з'єднання «точка-точка», авторизація та/або підключення до мультимедійних IP-сервісів, функції легального перехоплення трафіка і т.д. CSN може включати такі елементи, як маршрутизатори, сервери (прокси-сервери) для функцій аутентифікації та доступу, бази даних користувачів, шлюзи і т.д. У зв'язку з підтримкою мобільності в базовій моделі мережі WiMAX введено поняття домашніх і гостьових сервіс-провайдерів – H-CSP і V-CSP відповідно.

Домашній NSP — це оператор, який уклав договір про обслуговування з абонентом WiMAX. Саме він реалізує функції авторизації, аутентифікації і контролю доступу (у тому числі білінг і стягнення абонентської плати). Для підтримки роумінгу домашній сервіс-провайдер WiMAX укладає роумінгові угоди з іншими NSP.

Гостьовий NSP (V-NSP) — це оператор, який надає WiMAX-абоненту послуги роумінгу. Перш за все V-NSP забезпечує для такого абонента функції AAA, а також повний або частковий доступ до всіх послуг WiMAX-мережі. При цьому можливі різні варіанти маршрутизації трафіка – через домашню мережу підключення або безпосередньо через гостьову CSN-мережу.

Базові точки в рамках БМ мережі WiMAX — це канали зв'язку між базовими модулями. Вони являють собою стандартні інтерфейси, причому не обов'язково фізичні, особливо якщо з'єднані базовою точкою модулі конструктивно знаходяться в одному пристрої.

Базова точка R1 являє собою канал зв'язку між МС і мережею доступу ASN. Це — бездротовий інтерфейс, відповідний стандарту IEEE 802.16, однак припустимі й додаткові протоколи керування.

Базова точка R2 — канал між МС і CSN. Вона включає протоколи і процедури, пов'язані з аутентифікацією МС, авторизацією і IP-конфігуруванням. Це суто логічний інтерфейс, йому не відповідає жоден конкретний фізичний інтерфейс між МС і CSN.

Базова точка R3 містить набір протоколів керування між ASN і CSN для реалізації процедур AAA, виконання різних політик і керування мобільністю. Вона також підтримує функції передачі даних (у тому числі тунелювання) між ASN і CSN.

Базова точка R4 — це канал зв'язку між ASN-шлюзами різних ASN-мереж або між ASN-шлюзами в межах однієї ASN.

Базова точка R5 — канал зв'язку між мережею домашнього і гостьового сервіс-провайдерів.

Базова точка R6 служить інтерфейсом між БС і ASN-шлюзом.

Базова точка R7 — віртуальний канал всередині ASN-шлюзу для зв'язку двох груп функцій (пов'язаних і не пов'язаних з каналом передачі інформації). Конкретизації протоколів R7 слід очікувати в майбутньому.

Базова точка R8 – це канал зв'язку безпосередньо між базовими станціями. Він повинен підтримувати передачу керувальних повідомлень і опціонально — безпосередню трансляцію даних (для швидкого й безшовного хендовера).

1.4.3 Профілі ASN

Профілями ASN називають розподіл логічних функцій ASN-мереж між фізичними пристроями. У стандарті описано три типи ASN-профілів. Профілю B відповідає як концентрація всіх функцій в одному пристрої, так і їх довільний розподіл. Профілі A і C більш конкретні. На рівні опису вони надзвичайно схожі. Різниця полягає в тому, що функції контролера радіоресурсу (RRC) та керування хендовером у профілі A належать до ASN-шлюзу, а в профілі C – до БС. Однак незначні формальні відмінності на практиці призвели до того, що профіль A був офіційно закритий влітку 2007р. на сесії WiMAX-форуму в Мадриді, а загальновизнаним стандартом став профіль C. Дійсно, профіль A, концентруючи функції керування в ASN-шлюзі, ускладнює сумісність обладнання різних постачальників. У профілі B інтелект БС зростає, вони відіграють важливу роль в керуванні

трафіком і мобільністю. Профіль С – найбільш відкрита і тому перспективна система. У ньому на відміну від профілю А БС відповідають за керування радіоресурсом і забезпечення хендовера. В ідеальному випадку всі елементи такої системи взаємозамінні на продукти інших постачальників, сертифікованих WiMAX Forum.

1.4.4 Підтримка мобільності

Уся робота з опису і стандартизації мереж WiMAX має одну мету — забезпечити глобальну мобільність абонентів WiMAX, їх свободу переміщатися між різними мережами в усьому світі, не втрачаючи зв'язку. Для цього необхідний механізм глобального розподілу загальних мережевих ресурсів між різними операторами-провайдерами. Можливі кілька різних варіантів розподілу мережевих ресурсів: однією ASN-мережею користуються декілька CSN-провайдерів, кілька ASN-мереж (одного або кількох операторів) взаємодіють з різними CSN, одному оператору належить ASN і CSN тощо.

У мобільних IP-мережах питання забезпечення мобільності пристроїв вирішують на основі двох основних механізмів — призначення глобальної додаткової IP-адреси або використання зовнішнього агента (рис.1.3).

Протокол мобільного IP: у кожного пристрою є дві IP-адреси — основна (HoA), присвоєна йому в домашній мережі, і додаткова (CoA). Якщо пристрій з'являється в новій мережі (зовнішній), йому може бути присвоєна глобальна додаткова IP-адреса (наприклад, на основі протоколу динамічного призначення адрес DHCP). Цю адресу пристрій повідомляє своєму домашньому агенту (HA – home agent) – маршрутизатору, який перехоплює всі повідомлення за основною IP-адресою даного пристрою і направляє їх з додаткового IP (як правило, у режимі тунелювання та інкапсуляції IP-в-IP).

Другий механізм забезпечення мобільності полягає в тому, що в зовнішній мережі використовується так званий зовнішній агент (FA, foregion agent). Це маршрутизатор, у якому пристрій реєструється в разі підключення до зовнішньої мережі. FA як додаткову IP-адресу присвоює пристрою адресу зі свого пулу IP-адрес. Додаткова адреса CoA служить тільки для мережевої взаємодії. Усі користувацькі додатки, наявні на мобільному пристрої і в інших вузлах мережі, застосовують основну IP-адресу (рис.1.4).

WiMAX-мережа орієнтована на підтримку стека протоколів MIP. Проте в мережах WiMAX не всі абонентські пристрої зобов'язані підтримувати мобільний IP. Причому DHCP-сервер може знаходитися як у домашній, так і в гостьовій мережі. Можливе його розміщення і в мережі ASN. У такому випадку інформація про IP-адресу абонентської станції передається в домашню мережу під час її підключення та аутентифікації.

У WiMAX-мережах виділяють два види мобільності — мікро- й макромобільность. Також їх називають ASN- і CSN-мобільність. Таким чином, для ASN-мобільності не потрібна підтримка протоколів рівня MIP. На рівні ASN-мобільності реалізується хендовер у межах однієї ASN-мережі. При цьому до процесу залучаються тільки інтерфейси R6 (між БС шлюзами) і R8 (між базовими станціями).

Відзначимо особливий випадок ASN-мобільності, коли МС виходить за межі однієї ASN і потрапляє в іншу (рис. 1.5). При цьому МС підключається до нового зовнішнього агента, але дані від цього FA передаються до колишнього зовнішнього агента по каналу R4. Очевидно, що в даному випадку з боку мережі CSN (тобто домашнього агента) жодних змін не відбулося.

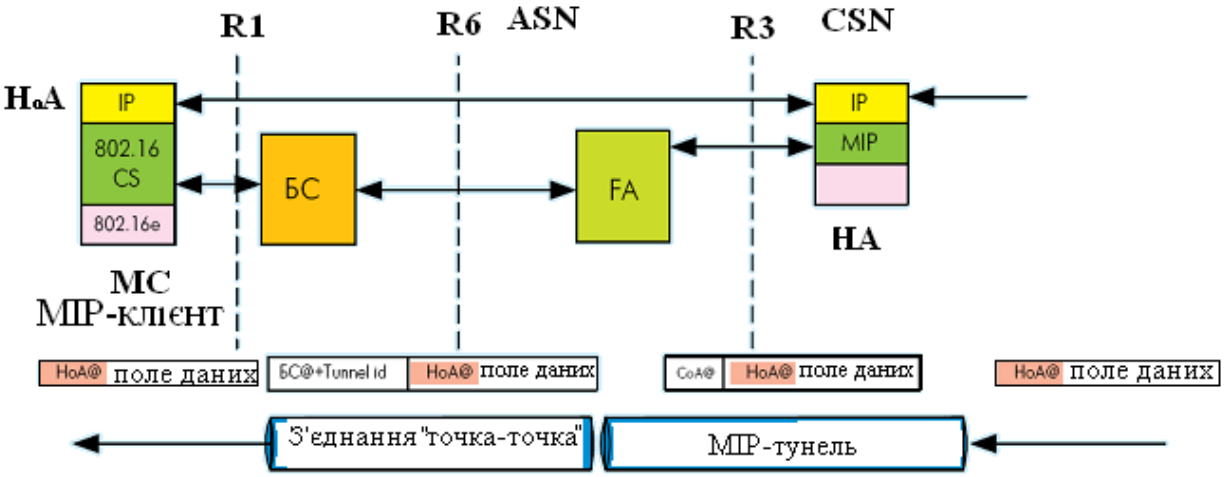

Рисунок 1.3 – Передача пакетів у WiMAX-мережі з підтримкою MIP

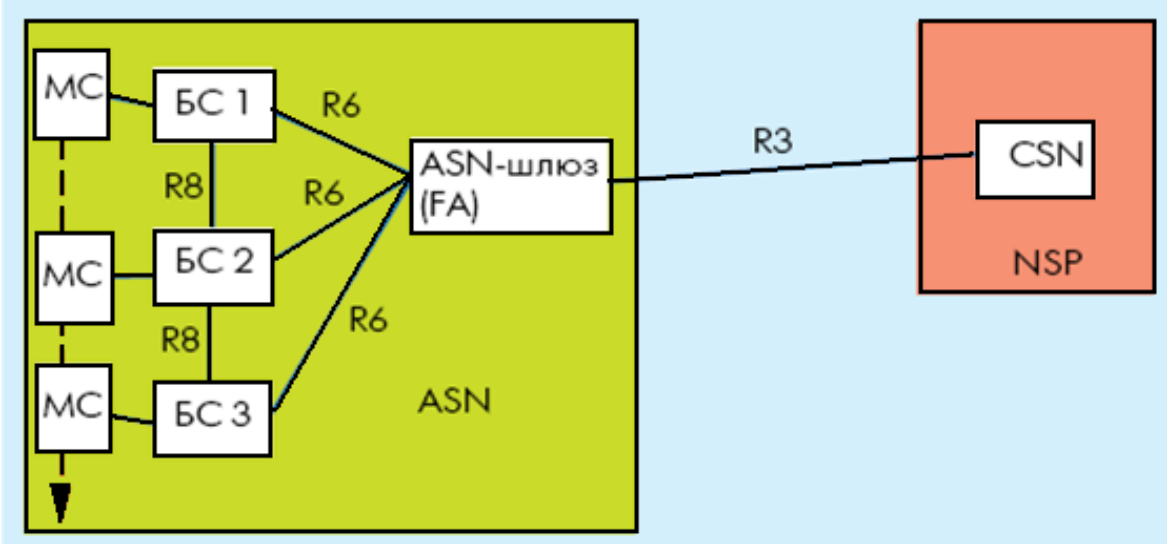

Рисунок 1.4 – ASN-мобільність за хендовера в межах однієї ASN-мережі

Макромобільність — зміна зовнішнього агента, пов'язаного з HA по каналу R3. Зміна зовнішнього агента однозначно обумовлює зміну CoA-адреси MC. У цьому випадку зміни стосуються мережевого рівня, тобто рівня інтерфейсу R3. Тому даний вид мобільності ще називають R3-мобільністю. Оскільки MC можуть не підтримувати функції мобільного IP, стандарт WiMAX-мереж передбачає два сценарії CSN-мобільності — з підтримкою MIP-клієнтів (CMIP) і прокси-мобільний IP (PMIP). У першому випадку MIP-клієнт реалізований у кожній мобільній станції, у другому як мобільний вузол розглядають усю ASN-мережу, а зовнішній

агент є MIP-клієнтом і виконує функції прокси-сервера MIP. Важливо зазначити, що різні механізми мобільності можуть співіснувати в межах однієї інтегрованої мережі. Більше того, можлива оптимізація підключення.

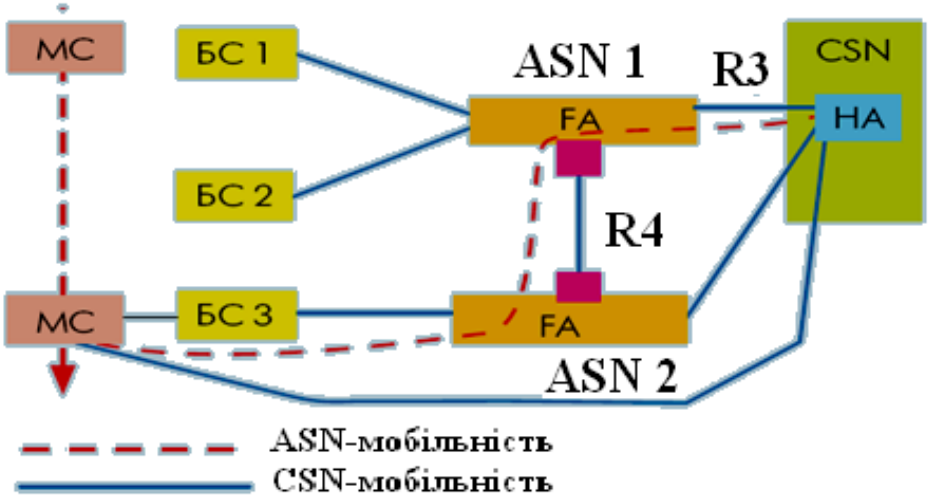

Рисунок 1.5 – Перехід від моделі ASN-мобільності до CSN-мобільності

Усі розглянуті вище функції належать до основної на сьогодні версії TCP/IP-протоколів — IPv4. Однак на зміну їм прийшла нова версія IPv6. Основна причина її появи — брак адресного простору, обумовлений 32-розрядною IP-адресою, а також відсутність вбудованої підтримки QoS (Quality of Service). У новій версії передбачені 128-розрядні адреси, крім того, що важливо для мобільних мереж, — так звана альтернативна адреса. Вона може бути присвоєна групі пристроїв, розподілених у мережі, але пакет надходить тільки до найближчого вузла з такою адресою. Запланована також маршрутизація, яка виключить обов’язкову передачу пакетів через домашнього агента. Немає необхідності і в зовнішньому агенті, так само як і в інкапсуляції вихідних IP-пакетів під час їх трансляції мобільному вузлу. Замість зовнішнього агента застосовують маршрутизатор доступу (AR — access router).

1.4.5. Керування радіоресурсом

Функція ефективного керування радіоресурсами — одна з найважливіших у будь-якій безпровідній мережі. Оскільки стандарт IEEE 802.16 розглядає тільки взаємодію однієї БС з оточуючими її абонентськими станціями, питання спільної роботи декількох базових станцій належать до компетенції стандартів WiMAX-мереж. Ці функції зосереджені в ASN-сегменті або в БС (профіль С), або в ASN-шлюзі (профіль А).

Функції керування радіоресурасами реалізують два логічні пристрої — контролери радіоресурсу:

− Radio Resource Controller (RRC);

− агент радіозасобів (Radio Resource Agent — RRA).

У кожній БС (і тільки в БС) повинен бути свій RRA. Навпаки, контролер RRC може розташовуватися як у БС, так і в ASN-шлюзах або на окремих серверах у межах ASN-мережі. Але, оскільки фактично стандартним став ASN-профіль С, будемо розглядати тільки розміщення функцій RRC у БС. У цьому випадку виникає потреба в додатковому логічному пристрої — RRC-ретрансляторі, розташованому в ASN-шлюзах і призначеному для обміну керувальною інформацією між RRC-контролерами (рис. 1.6). При цьому обмін відбувається через інтерфейси R6 і R4. Однак, якщо БС безпосередньо пов’язані одна з одною каналом R8, можливий обмін повідомленнями між RRC-контролерами даних БС і через цей інтерфейс.

Основні функції, які реалізує RRA, — збір інформації про радіостановище навколо БС і керування нею. Види вимірів і методика їх проведення вказані в стандарті IEEE 802.16. Крім того, RRA збирають і інформацію про вимірювання параметрів протоколів верхніх рівнів, наприклад, інтенсивність помилок передачі пакетів MAC-рівня. До завдання цього пристрою входить і трансляція керувальної інформації від RRC до МС радіопослуг. Характерний приклад такої інформації — перелік

сусідніх БС та їх параметрів. У свою чергу, основна функція контролера RRC — збір і зберігання інформації від пов'язаних із ним RRA та взаємодія з іншими контролерами RRC.

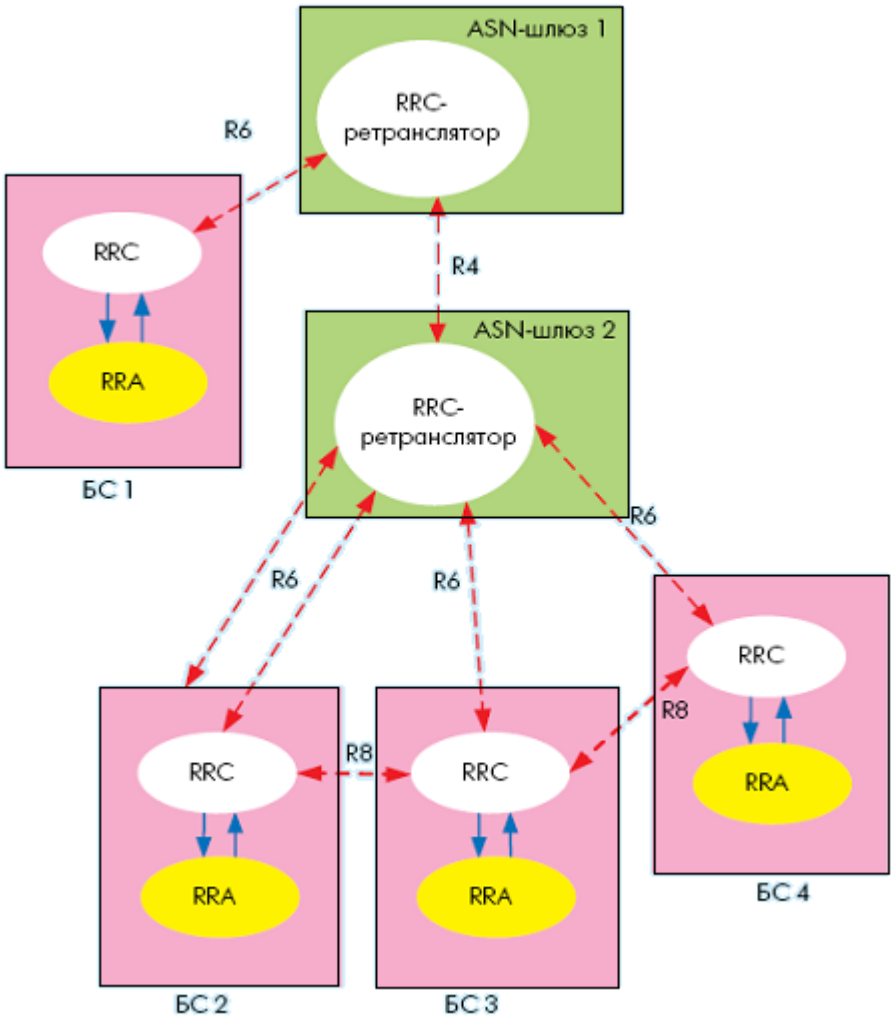

Рисунок 1.6 – Базова модель системи для ASN-профілю С

Таким чином, основне завдання керування радіоресурсом — це ініціювання процедур вимірювання параметрів радіомережі, збір цих відомостей від усіх БС та їх збереження в загальнодоступній базі даних мережі. Цю інформацію застосовують для керування хендовером, забезпечення якості обслуговування QoS і т.д. Крім того, стандартом передбачені: можливість вимірювання таких параметрів, як рівень потужності сигналів БС і рівень інтерференції; передача таких керувальних повідомлень, як реконфігурація субканалів у заданому секторі

БС, зміна максимальної потужності сигналу БС, зміна таблиць розподілу ресурсів БС, у тому числі — співвідношення між висхідним і спадним субкадрами в режимі часового дуплексування (TDD), трансляція дескрипторів висхідного/спадного каналів (UCD/DCD) між сусідніми БС, зміна широкомовної інформації та ін.

2 ВИМОГИ МУЛЬТИМЕДІЙНИХ ДОДАТКІВ ДО МЕРЕЖІ

Доставка мультимедійного трафіку пред'являє жорсткі вимоги до продуктивності мереж, відмінні від тих, які накладаються для передачі тексту і зображень.

• Затримки.

Користувачі інтернету відчувають затримку при завантаженні тексту і зображень. Ці затримки не впливають на якість змісту після його повного отримання. Для мультимедійних додатків ситуація інша. Після початку відтворення аудіо- або відеопотоку наступні кадри повинні надходити вчасно. В іншому випадку додаток повинен компенсувати відсутність даних. Наприклад, додаток може зробити паузу. Через це виникає переривчасте зображення або звук.

• Втрати.

Багато мультимедійних додатків можуть примиритися з невеликими втратами даних. Наприклад, відеоплеєр може відновити відсутню частину кадрів на основі найближчих кадрів. Однак, оскільки втрати і затримки знижують якість інформації, багато додатків мають обмежену підтримку для відновлення загублених пакетів.

• Висока пропускна здатність.

Передача потоків аудіо та відео вимагає досить високої пропускної здатності. Наприклад, нестиснене голосове повідомлення потребує швидкості 64 Кбіт/с. Ефективна техніка стиснення дозволяє зменшити цю вимогу до 9-10 Кбіт/с. Вимога до пропускної спроможності для відео потоків сильно варіюється залежно від якості, частоти кадрів, розміру зображення.

Спочатку мережі TCP/IP розроблялися і використовувалися для передачі текстів з невеликою кількістю зображень. Ці мережі забезпечують оптимальний і надійний транспорт, який добре підходить для більшості

додатків Інтернету (WEB, FTP, електронна пошта), однак вони мають деякі обмеження, критичні для мультимедійних додатків:

• Якість сервісу. IP надає оптимальний сервіс без встановлення з'єднання, який допускає не тільки втрату пакетів, а й доставку їх не в правильному порядку.

• Повторна передача даних. Передача інформації використання протоколу TCP передбачає повторну передачу втрачених сегментів повідомлень, тобто повідомлення доставляються надійним способом. Надійна доставка не є головною метою мультимедійних додатків, оскільки повторна передача загубленого сегмента може викликати занадто велику затримку при відтворенні.

2.1 Параметри якості обслуговування, що впливають на якість передачі мультимедійної інформації

Щоб правильно спроектувати мережу передачі трафіку реального часу, необхідно враховувати недоліки основних засобів міжмережевої взаємодії, які впливають на якість передачі мультимедійної інформації.

Затримки.

Затримка - це період часу, за який пакет проробляє шлях від джерела до одержувача. Прийнято виділяти причини затримок: затримки на поширення, затримки на серіализацію, затримки на обробку і затримки черги.

Затримка на поширення викликана довжиною шляху, який повинен пройти сигнал. Для оптоволоконної мережі, що охоплює 20 000 км, одностороння затримка становить 70 мілісекунд. Появу затримки на обробку обумовлюють пристрої, які передають кадри по мережі. Затримки на серіалізацію – це період часу, протягом якого біт переміщується в інтерфейс. Ці затримки впливають на загальну затримку незначно.

Затримки черги відбуваються в результаті утримування пакетів в черзі через перевантаження вихідного інтерфейсу.

Це відбувається, коли прийнято більше пакетів, ніж інтерфейс може обробити за даний інтервал.

Рекомендація сектора стандартизації при міжнародному телекомунікаційному союзі (ITU-T) говорить, що для хорошої якості передачі мультимедійної інформації значення однобічної наскрізної затримки не повинно перевищувати 150 мс.

Джиттер

Інший спосіб затримки черги - це джиттер. Джиттер – це нерівномірність затримок на доставку пакетів. Відправник очікує, що пакети доставлятимуться з однаковими інтервалами. Але ці пакети можуть затриматися в мережі і не досягти адресата за цей період. Різниця часу між тим, коли очікувалося отримання пакету і часом фактичного отриманням, називається джиттер. Час відправлення та отримання пакетів A і B. Однак пакет C зіткнувся з затримкою, тому отриманий пізніше очікуваного моменту. Ось чому буфер компенсації джиттера, який згладжує нерівномірність затримок пакетів, просто необхідний. Він затримує вхідні пакети, щоб передавати їх додатком із заданим інтервалом. Крім того, він також фіксує помилки, контролюючи номер послідовності в полях повідомлень протоколу RTP.

Чим більше нерівномірність затримок, тим більшим повинен бути буфер компенсації джиттера. Використання статичного буфера - не найкращий варіант. Він може виявитися або занадто великим або занадто маленьким. Це може призводити до погіршення якості інформації через втрати пакетів при маленькому буфері або через надмірні затримки при занадто великому буфері. Іноді краще просто видаляти деякі пакети, маючи буфер обмеженого обсягу, ніж створювати додаткові затримки в буфері компенсації джиттера. Адаптація встановлення розмірів буфера може ефективно компенсувати затримки. Динамічний буфер компенсації

джиттера збільшується або зменшується залежно від варіації затримок останніх пакетів. Для визначення рівня джитера використовуються часові мітки в заголовку протоколу RTP. Для вирішення цих проблем необхідно використовувати QoS.

2.2 Алгоритми якості обслуговування

2.2.1 Диференційовані та інтегровані служби

Прийнято розділяти якість обслуговування на інтегровані і диференційовані служби. Диференційовані служби зазвичай використовуються у великих мережах. В основі їх роботи – встановлення відповідного рівня QoS для певної частини трафіку. Це здійснюється за рахунок встановлення поля «тип обслуговування» в заголовку IP пакета. Інтегральні служби використовуються, коли ще до відправлення необхідно упевнитися в тому, що певний тип трафіку буде поставлений з відповідним рівнем QoS. Для цього використовується резервування ресурсів. У інтегральних служб є недолік. Їм потрібна попередня домовленість між пристроями мережі при установці каналу для кожного потоку. Це організувати складно у великий мережі і за наявності великого числа потоків. У той же час, диференціальні служби можна організувати локально на кожному пристрої, без попереднього налаштування всіх вузлів уздовж маршруту.

Хоча ці два механізми істотно відрізняються, основна їх мета - забезпечення необхідної пропускної спроможності і затримки для певного додатки. У даній роботі розглядаються диференціальні служби.

До основних завдань якості обслуговування можна віднести:

- Маркування пакетів. Функція маркування пакетів використовується вузлами мережі для призначення пріоритету обслуговування трафіку шляхом установки відповідного значення в поле QoS в заголовку IP-пакета.

- Розподіл ресурсів. Розподіл ресурсів припускає здатність диференціювати і визначати вимоги до обробки різних пакетів. Відповідно до цих вимог алгоритм обслуговування повинен планувати порядок передачі пакетів , поставлених в чергу. Тут можна виділити наступні технології : FIFO (First - in - First- out), WFQ (Weighted Fair Queuing).
- Запобігання перевантаження і відкидання пакетів. Це передбачає використання активного алгоритму керування розмірами черзі, що дозволяє передбачити перевантаження черзі ще до її переповнення.

2.2.2 Random Early Detection

Алгоритм довільного раннього виявлення (Random Early Detection - RED) являє собою алгоритм запобігання перевантаження, запропонований Саллі Флойдом (Sally Floyd) і Ваном Якобсоном (Van Jacobson) [16-18]. Випадкове раннє виявлення (RED) представляє собою випереджаюче відкидання пакетів. При цьому підході з метою підвищення продуктивності мережі вузол відкидає кілька вхідних пакетів перш, ніж черга повністю переповниться. Основна мета цього алгоритму - попередження перевантаження. RED призначений не для реагування на виникнення перевантаження, а для його запобігання.

Основними параметрами алгоритму є: межі зміни середньої довжини черги (min_{th}, max_{th}), максимальна ймовірність відкидання (max_p), ваговий коефіцієнт середньої черги (w_q). Як уже згадувалося раніше, механізм RED використовує превентивний підхід до запобігання перевантаження мережі. Замість очікування фактичного переповнення черги, RED починає відкидати пакети з ненульовою ймовірністю, коли середній розмір черги перевищить певне мінімальне граничне значення. Ця ймовірність визначається за формулою (2.1) [20-22]:

$$P = P_{max} \frac{avg - min_{th}}{max_{th} - min_{th}} \quad (2.1)$$

Таким чином, ймовірність відкидання пакетів буде лінійно зростати від 0 при min_{th} до певного значення P_{max} при max_{th} , як це показано на рис. 2.1.

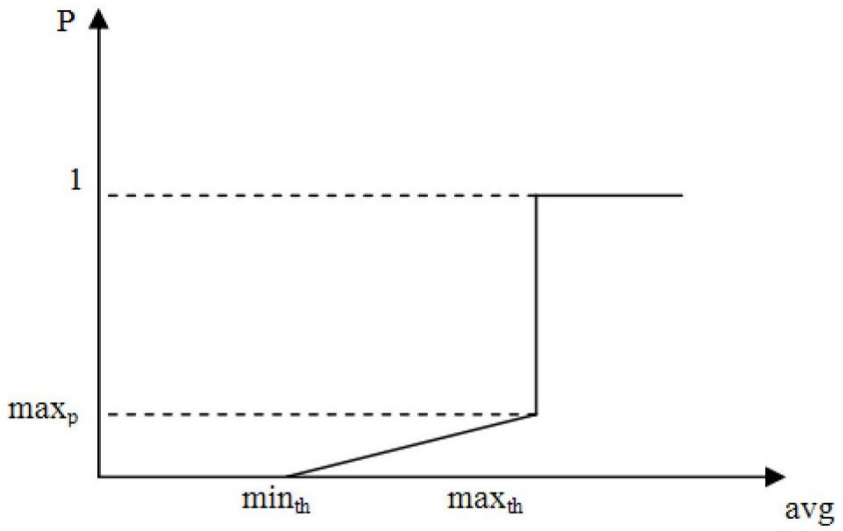

Рисунок 2.1 – Залежність ймовірності відкидання пакету від середнього розміру черги

Отже, середній розмір черги строго обмежений максимальним граничним значенням, оскільки в цьому випадку ймовірність відкидання пакетів досягає свого найбільшого значення. Іншими словами, головна мета механізму довільного раннього виявлення (RED) полягає в мінімізації середнього розміру черги. При визначенні ймовірності відкидання пакетів механізм RED обчислює не поточний, а експоненціально зважений середній розмір черги. Поточний середній розмір черги визначається на підставі попереднього середнього та поточного дійсного розміру. Використання механізмом RED середнього розміру черги обумовлено прагненням реагувати тільки на тривалу перевантаження мережі і "не помічати" моментальних сплесків трафіку. Середній розмір черги обчислюється за формулою (2.2).

$$avg = (1 - w_q)\, avg + w_q \cdot q \qquad (2.2)$$

де q - поточний розмір черги.

Sally Floyd і Van Jacobson [27] запропонували використовувати співвідношення (2.3) для визначення W_Q

$$W_Q = 1 - e^{1/c} \quad (2.3)$$

де C – пропускна здатність каналу [пакет / сек]

Як буде показано в результаті моделювання, алгоритм RED відкидає набагато менше число пакетів, ніж алгоритм Drop Tail, проте він не забезпечує виграш у затримці. Для вирішення цієї проблеми можна розглянути наступний алгоритм, який називається Adaptive RED (ARED).

2.2.3 Adaptive RED

Wu-chang Feng показав, що одним з головних недоліків RED те, що середній розмір черги знаходиться в залежності від встановлених параметрів. Алгоритм може виявитися або агресивним, або консервативним. Для вирішення цієї проблеми він запропонував алгоритм ARED. Головна його відмінність від алгоритму RED - зміна максимальної ймовірності відкидання залежно від зміни середньої довжини черги.

Додатковим параметром, використовуваним в цьому алгоритмі є параметр α (α < 1). За допомогою цього параметра можна контролювати максимальну ймовірність відкидання. Це дозволить більш жорстко контролювати розмір черги.

Залишається проблема вибору налаштувань параметрів для цих алгоритмів. Багато дослідників згодні з тим, що вплив алгоритму на якість передачі потоків сильно залежить від правильного завдання його параметрів, але до цих пір немає зрозумілої інструкції, як на практиці вибирати значення цих параметрів. У даній роботі за допомогою моделювання в NS-2 оцінюється вплив параметрів цих алгоритмів на якість передачі.

3 ДОСЛІДЖЕННЯ МОДЕЛІ МЕРЕЖІ ПРИ ПЕРЕДАЧІ ВІДЕО

3.1 Опис моделі досліджуваної мережі

У проведеному дослідженні імітується робота мережі на 50 комп'ютерів з топологією, представленою на рис. 3.1.

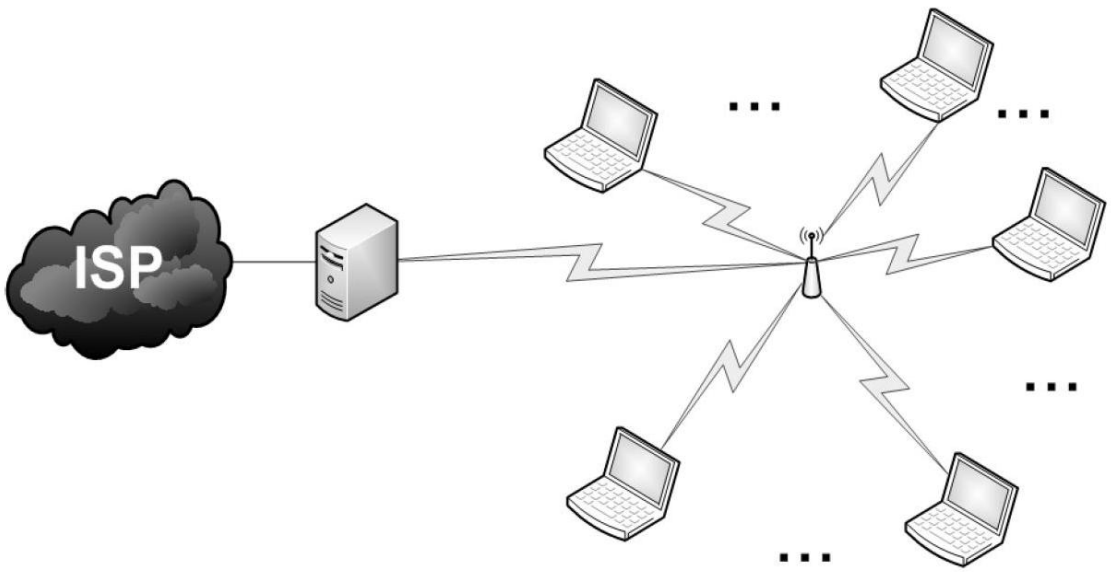

Рисунок 3.1 – Топологія досліджуваної мережі

Наведена топологія є моделлю мережі інтернет-кафе, в якій 50 відвідувачів користуються послугами Інтернету і IP-телебачення. Постачальником послуг є ISP, він надає вихід в Інтернет і підключення до відео-сервісів. ISP з'єднаний з бездротовим Wi-Fi-маршрутизатором каналом в 100 Мбіт/с. Кожен користувач підключається до маршрутизатора по бездротовому каналу з пропускною здатністю 54 Мбіт/с. На маршрутизаторі можливе функціонування різних алгоритмів управління чергою фреймів.

У ході дослідження до кожного користувача передається один з трьох видів трафіку. Час моделювання становить 10 секунд. Параметри потоків представлені в таблиці 3.1.

Таблиця 3.1 – Параметри відео-потоків, що передаються

Назва потоку	Пряма швидкість потоку	Зворотна швидкість потоку	Розмір пакета
Відео-трафік	2/5 Мбіт/с	-	1028 байт
Web-трафік	768 кбіт/с	48 кбіт/с	1024 байт
FTP-трафік	1 Мбіт/с	1 Мбіт/с	1024 байт

Передане відео стиснено з використанням XVID відеокодека.

Відео фрагмент єдиний для всіх частин дослідження, це стандартне відео «Foreman», обране через наявність великої динамічної частини зображення. Даний вибір зроблено не випадково, тому що втрати відео пакетів позначаються більшою мірою саме на такому типі відео. Розмір видеокадра 352x288 пікселів, частота - 30 кадрів/с. У ході роботи розглядається залежність якості переданого відео, від різних алгоритмів управління чергою фреймів на маршрутизаторі. У даній роботі для оцінки якості отриманого відео використовується одна з найбільш популярних метрик для оцінки якості переданого відео PSNR (Peak Signal to Noise Ratio – Пікове співвідношення сигнал/шум), що визначається за формулою (3.1).

PSNR вимірюється за допомогою логарифмічною шкали і обчислюється за середньоквадратичне помилку MSE (mean squared error) між вихідним відеокадром і отриманим відеокадром щодо числа $(2^k - 1)^2$ (квадрата найбільш можливого значення пікселя, де k - бітова глибина кольору):

$$PSNR = 20 \log_{10} \frac{2^k - 1}{MSE} (dB) \qquad (3.1)$$

Високе значення PSNR (на практиці більше 30 дБ) означає певну схожість отриманого і вихідного кадру. Великим мінусом використання PSNR в системах цифрової обробки зображень є те, що дана величина не має абсолютного значення. Безглуздо говорити про те, що якщо критерій

PSNR дорівнює, наприклад 25 дБ, то це добре. Величина PSNR використовується зазвичай тільки для порівняння різних алгоритмів обробки або для вивчення впливу параметрів на ефективність того чи іншого алгоритму. Слід мати на увазі, що критерій PSNR характеризує «середню» якість зображення в цілому, а на різних його фрагментах помилки, в принципі, можуть відрізнятися.

Величину PSNR можна легко і швидко обчислити, тому воно так популярно при оцінюванні якості відео. Для спостереження за роботою мережі відстежується її завантаження і час затримки пакетів. Для оцінки ефективності роботу алгоритму управління чергою розглядається залежність кількості пакетів в черзі від часу.

У роботі розглядаються наступні алгоритми управління чергою:

- Drop Tail
- RED
- RIO-C
- RIO-D
- Adaptive RED

3.2. Алгоритм Drop Tail

На рисунках 3.2 і 3.3 представлені графіки PSNR для відеокадрів і розміру черги залежно від часу. Для цього випадку максимальний розмір черги був встановлений 30 пакетів. Коли черга заповнюється до заданого максимального розміру, все знову надходять пакети відкидаються, поки черга не матиме місце, достатнє для надходження вхідного трафіку. Ми можемо спостерігати, що найбільше число таких переповнень зосереджено на інтервалі 5-10 сек. Це пояснюється тим, що динамічність картинки в дані моменти більше.

Графік PSNR дає нам уявлення про якість прийнятого відео. Найбільша частина кадрів знаходиться на рівні нижче 30 Дб, провали на графіку чітко

співвідносяться із часом переповнення черги. Середнє значення склало 30,41 Дб. Однак, навіть за відсутності переповнення якість відео низька. Це можна пояснити втратою пакетів, і, як наслідок, відставанням зміни динамічної частини зображення від оригіналу.

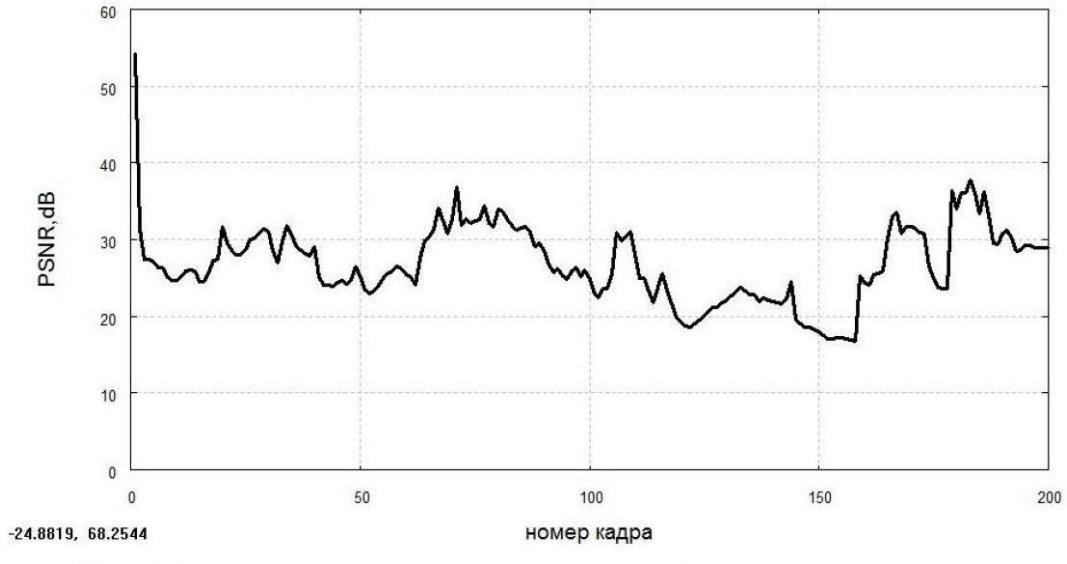

Рисунок 3.2 – Залежності пікового відношення сигнал/шум від номера кадру для тестового відеофрагменту при використанні алгоритму Drop Tail

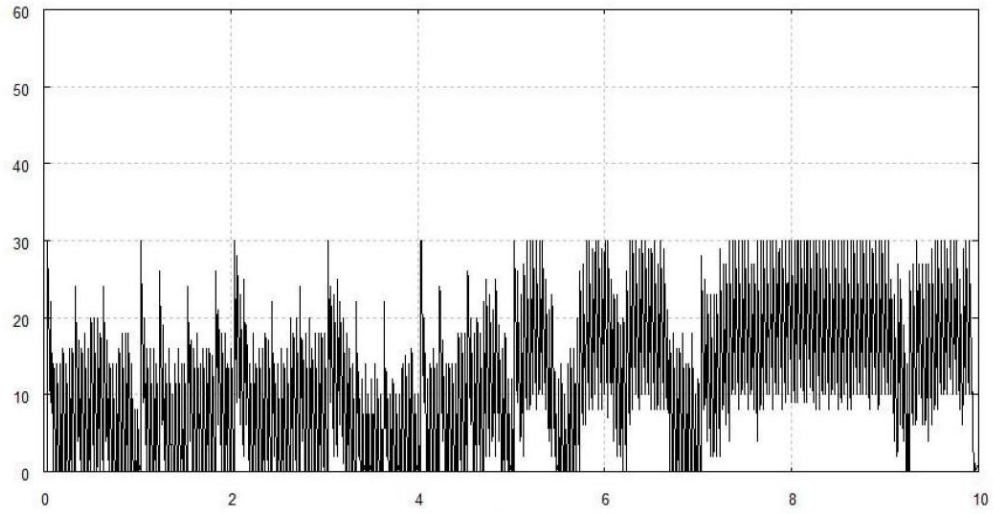

Рисунок 3.3 – Залежність розміру черги на маршрутизаторі від часу при використанні алгоритму Drop Tail

Для поліпшення ситуації підемо по шляху збільшення максимального розміру черги.

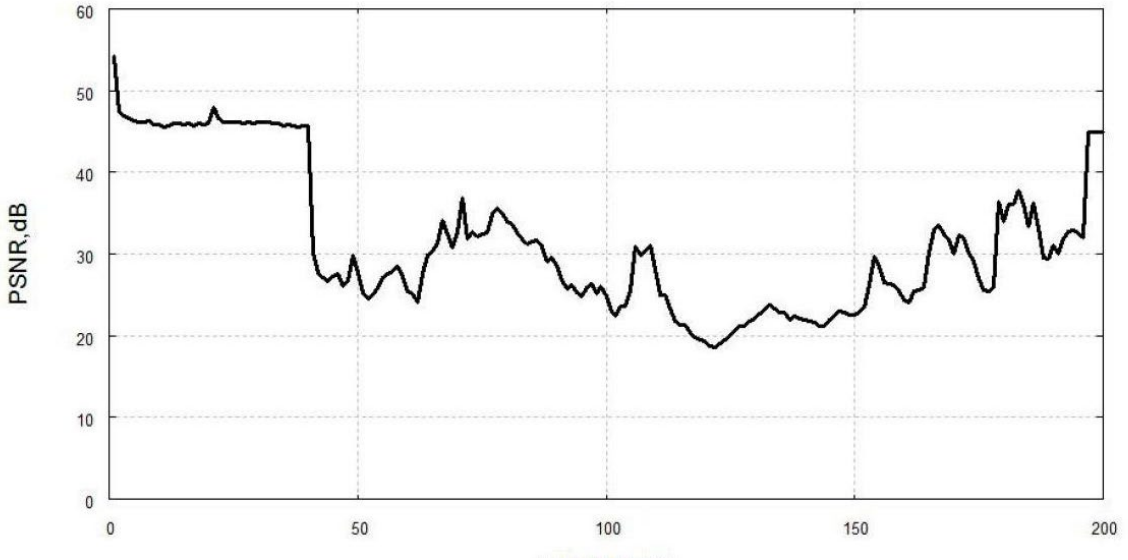

Рисунок 3.4 – Залежності пікового відношення сигнал/шум від номера кадру для тестового відеофрагменту при використанні алгоритму Drop Tail

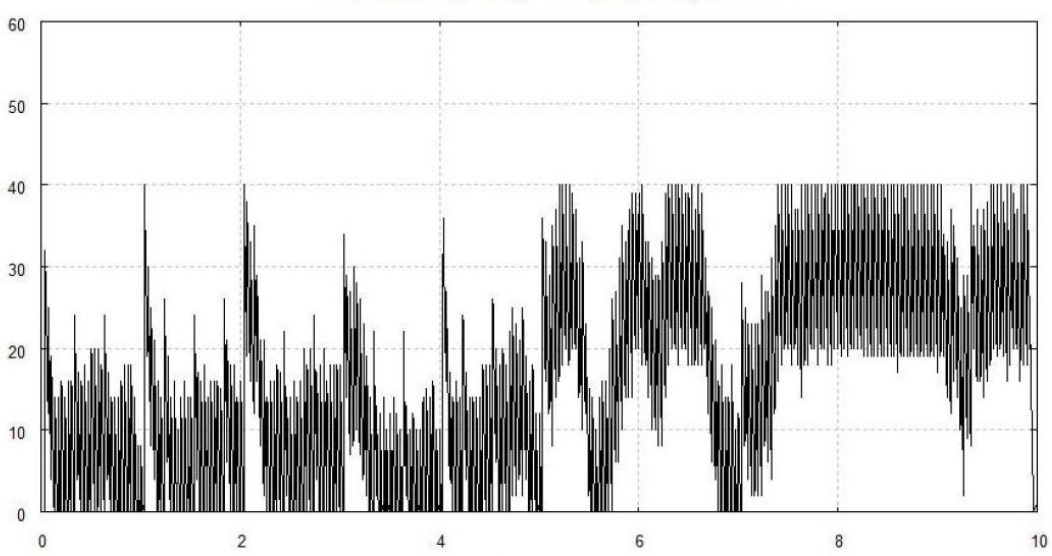

Рисунок 3.5 – Залежність розміру черги на маршрутизаторі від часу, при використанні алгоритму Drop Tail

Наступні графіки наведені для черги максимум 40 пакетів. Даного обмеження як і раніше недостатньо. Велика частина відео прийнята в низькій якості, в той же час знизилося число наближень розміру черги до максимального. Зниження якості відео в ті моменти, коли черга не переповнена, викликано особливістю кодування. Велика частина

відправленої інформації не містить безпосередньо кодовану картинку, а несе в собі лише вектори зміщення. При втраті цих даних спотворення будуть відображатися на динамічній частини зображення. Втрата ж пакетів, що несуть інформацію про все зображення, більш критична. Цим і викликаний різкий провал на графіку PSNR .

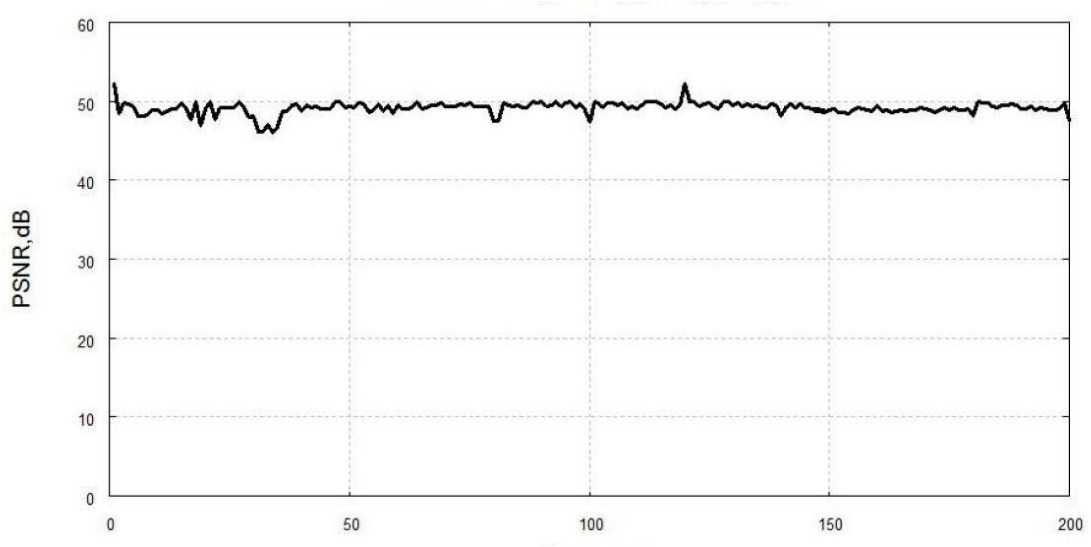

Рисунок 3.6 – Залежності пікового відносини сигнал/шум від номера кадру для тестового відеофрагменту при використанні алгоритму Drop Tail

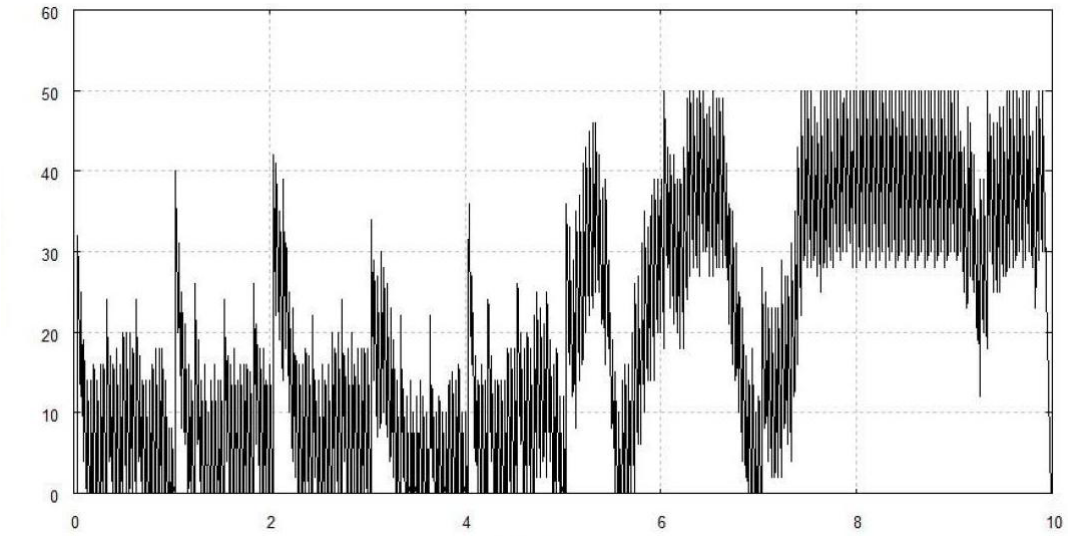

Рисунок 3.7 – Залежність розміру черги на маршрутизаторі від часу , при використанні алгоритму Drop Tail

Подані графіки візуалізують роботу мережі і якість передачі відео для випадку установки максимального розміру черги рівним 50 пакетам.

Середнє значення PSNR склало 49,56 дБ. На графіку розміру черги як і раніше є інтервали, на яких черга максимальна. Через те, що алгоритм сигналізує тільки про переповнення черг, вони можуть виявитися заповненими протягом досить тривалого часу.

За великого розміру черг збільшується час доставки мережевого пакета від однієї робочої станції до іншої. Графік затримки пакету в черзі представлений на рис. 3.8. Ми можемо помітити що одночасно з переповненням черзі відбувається збільшення затримки, і вона продовжує зростати, тому що маршрутизатор не виходить з режиму переповнення буфера черги. У результаті виходить, що Drop Tail нераціонально використовує простір пам'яті маршрутизатора. Як буде показано далі, вирішити сформовану проблему можливо впровадженням алгоритмів RED на маршрутизаторі.

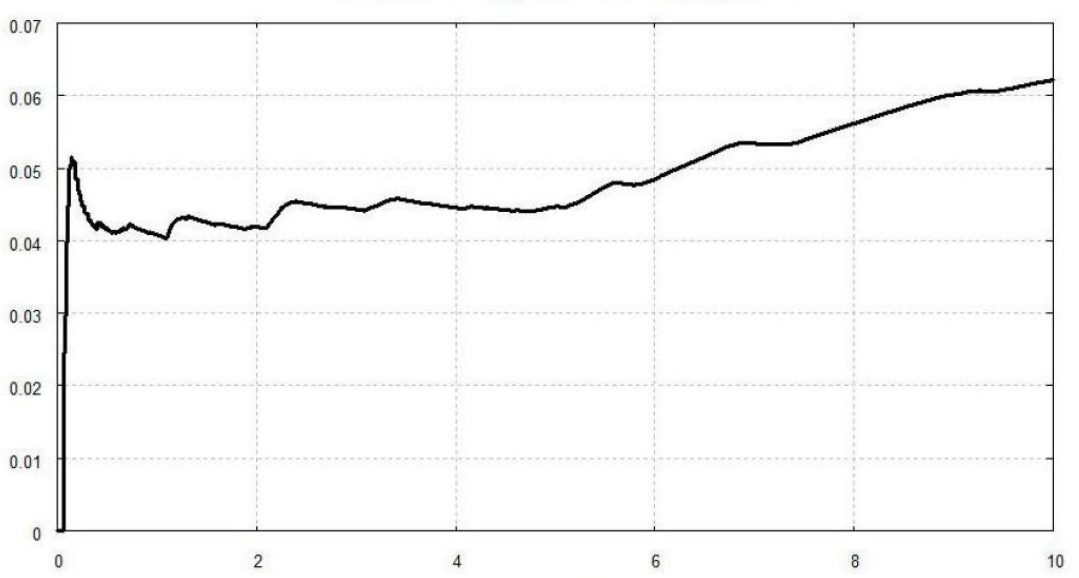

Рисунок 3.8 – Залежність затримки пакету в мережі від часу, при використанні алгоритму DropTail

3.3 Алгоритми RED

Другим досліджуваним алгоритмом управління чергою є Random Early Detection (RED). Даний алгоритм має кілька модифікацій, розглянемо першу із них - RED In / Out Coupled (RIO -C), графіки представлені на рис. 3.9 – 3.10. Ґрунтуючись на проведеному раніше вивченні алгоритму Drop Tail, для черги були обрані наступні параметри: кількість віртуальних черг - 2, мінімальний розмір – 10 пакетів, максимальний - 30 пакетів , $max_{\text{р}}$ = 0.10 .

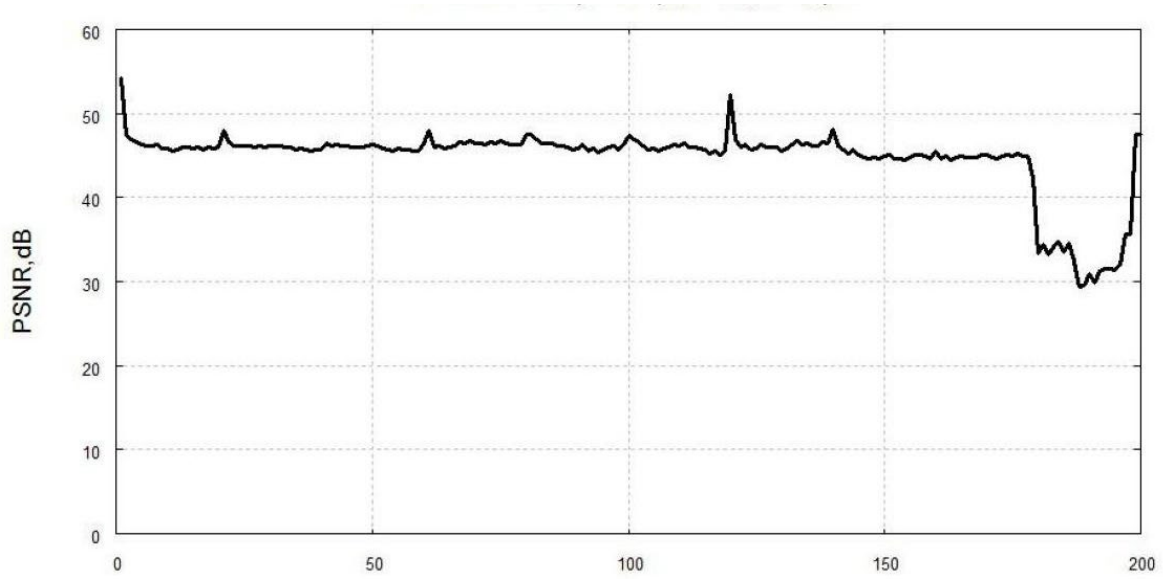

Рисунок 3.9 – Залежності пікового відносини сигнал / шум від номера кадру для тестового відеофрагменту при використанні алгоритму RIO – C

На графіку розміру буфера черзі можна помітити, як алгоритм розвантажує пам'ять маршрутизатора. Алгоритм приймає рішення відкинути пакет чи ні, ґрунтуючись на статистиці. Існує ймовірність відкинути пакет, максимальне значення якої задає користувач і воно має перебувати в інтервалі [0.10; 0.50]. Постійно відслідковується розмір черзі, при його збільшенні зростає ймовірність втрати пакетів, причому це поширюється як на пакети, що тільки прибули, так і на ті, що перебувають в черзі. У порівнянні з Drop Tail ми вже не спостерігаємо таких тривалих перевантажень маршрутизатора. Відкидання пакетів не може не

позначитися на якості відео, в кінцевому підсумку якість відео погіршується до 30 Дб, проте середнє значення PSNR склало 45,27 Дб.

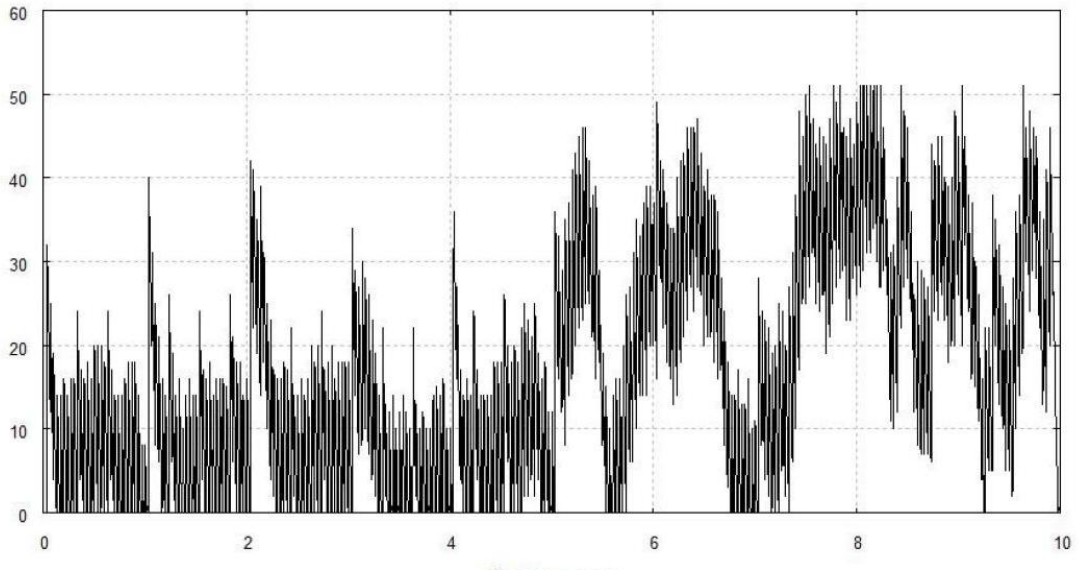

Рисунок 3.10 – Залежність розміру черги на маршрутизаторі від часу, при використанні алгоритму RIO – C

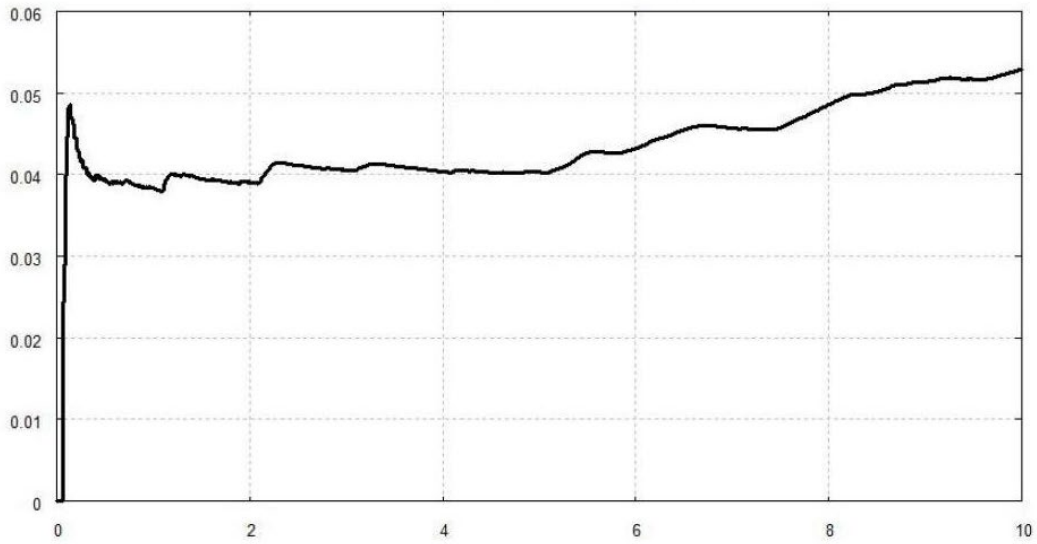

Рисунок 3.11 – Залежність затримки пакету в мережі від часу , при використанні алгоритму RIO – C

Звернемося до графіка затримки пакета в черзі. Так само, як і в попередніх випадках , при наближенні поточного значення розміру буфера черзі до максимального відбувається збільшення часу затримки пакета.

В даному випадку максимальна затримка склала 0.0527 сек. Це нижче, ніж при роботі алгоритму Drop Tail, але збільшення затримки позначається на прийнятому відео та роботі алгоритмів джіттер-буфера, що не можна вважати позитивним.

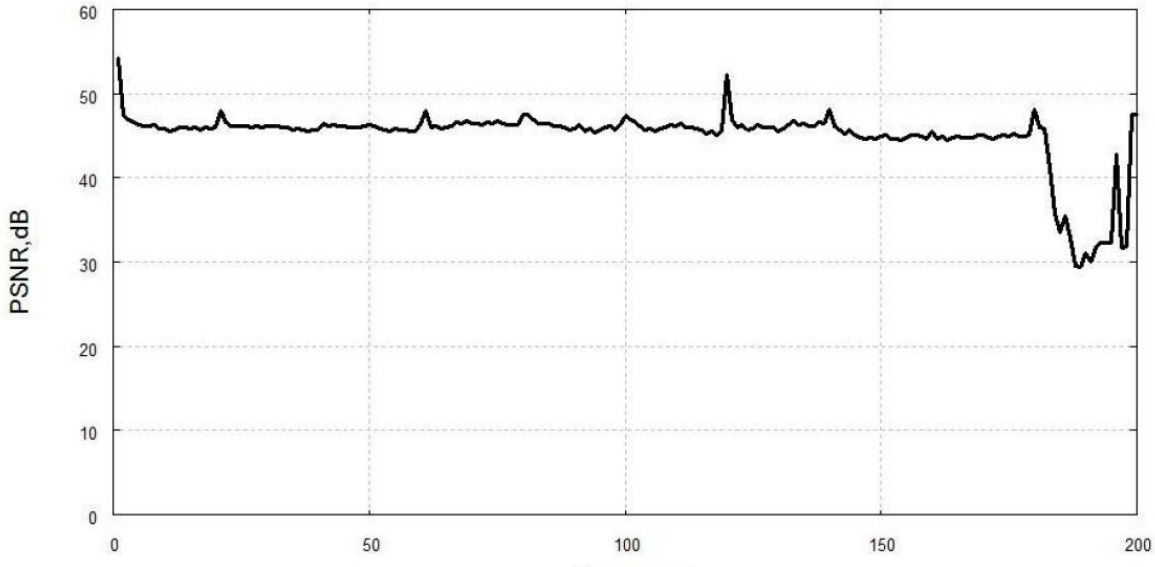

Рисунок 3.12 – Залежності пікового відносини сигнал / шум від номера кадру для тестового відеофрагменту при використанні алгоритму RIO –D

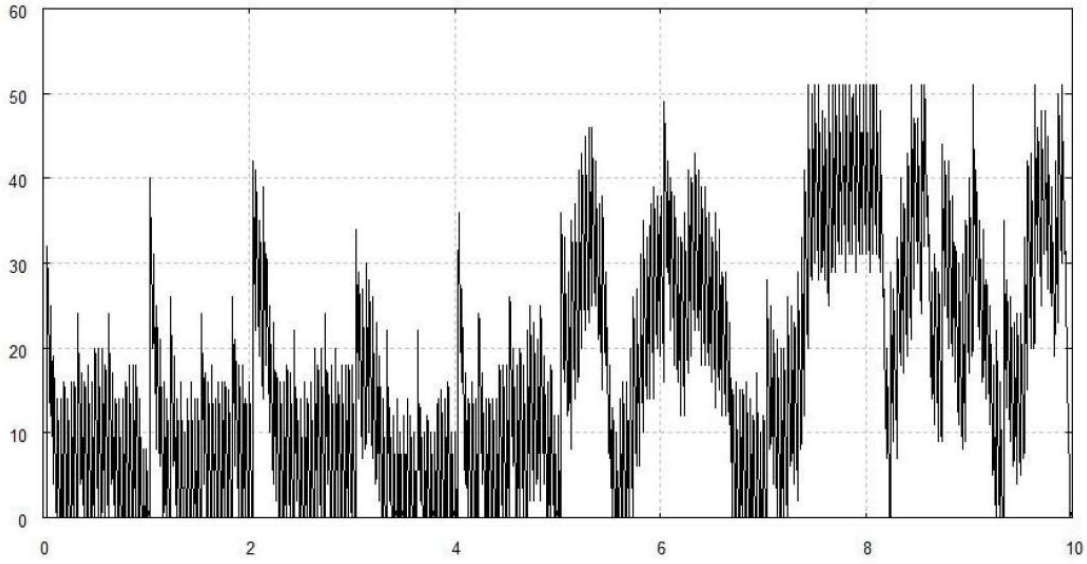

Рисунок 3.13 – Залежність розміру черги на маршрутизаторі від часу, при використанні алгоритму RIO –D

Для версії алгоритму RED In/Out Decoupled (RIO-D) графіки представлені на рис. 3.12 – 3.13. Відмінність від попередньої версії полягає в тому, що ймовірність відкидання існує тільки для нових прибуваючих пакетів, а ті пакети, що вже знаходяться в черзі, не будуть відкинуті. Це підтверджується і на отриманих графіках. Якщо провести порівняння графіків розміру черги, то можна помітити, що у разі RIO –D на періоді (8; 10) секунд розмір черги пакетів має більше мінімальне значення і не спостерігається таких різких провалів, як у випадку використання RIO-C.

Графіки затримки пакетів ідентичні для обох випадків і представлені на малюнку вище. Алгоритми не можуть зовсім усунути збільшення затримки, але в порівнянні з Drop Tail, максимальний час менше.

3.4 . Алгоритм Adaptive RED

На рис. 3.14 показана залежність довжини черги від часу для алгоритму ARED з параметрами min_{th} = 15; max_{th} = 45; max_p = 0,01; α = 0,065. У даному випадку використано стандартне значення величини w_q = 0,002. При порівнянні цієї залежності з залежностями вище можна помітити, що середня довжина черги при використанні ARED менше, ніж при використанні Drop Tail і RED. Графік більш згладжений, алгоритм плавно змінює розмір черги, різкі викиди пояснюються передачею I–кадрів кодованої відеопослідовності.

Якість відео, яке можна оцінити на графіку PSNR (рис.3.15) так само перевершує якість відео для випадків використання алгоритмів RED, але поступається якості передачі відео при використанні алгоритму Drop Tail з максимальним розміром черги. Для частини відео з малою динамікою значення PSNR збігаються з алгоритмами Drop Tail і RED. Для динамічної ж частині спостерігається спочатку різкий провал, викликаний тим, що алгоритм ще не встигає розвантажити пам'ять маршрутизатора, і подальше

збільшення значення PSNR, в той час як при використанні алгоритмів RED такого процесу не спостерігається.

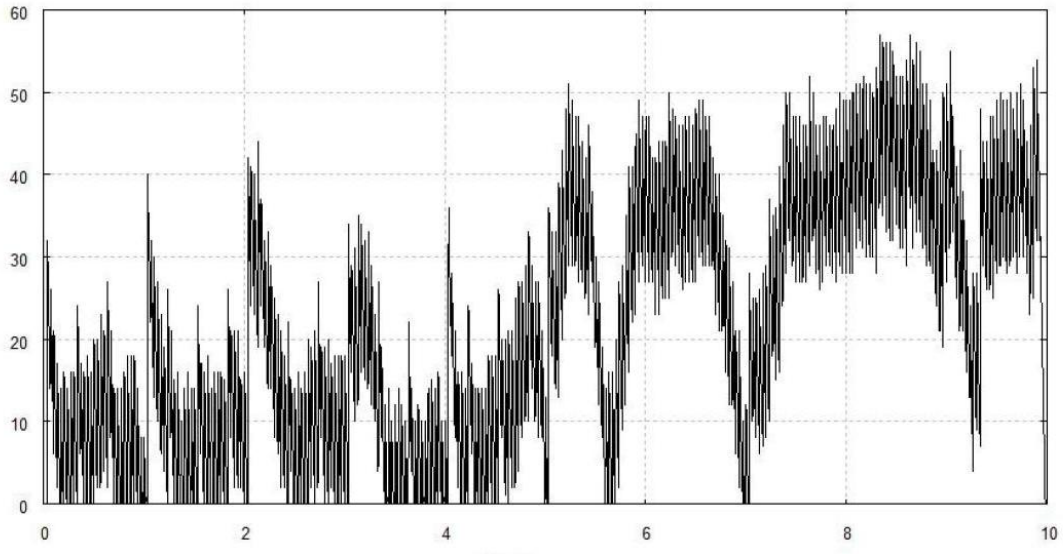

Рисунок 3.14 -– Залежності пікового відносини сигнал / шум від номера кадру для тестового відеофрагменту при використанні алгоритму Adaptive RED

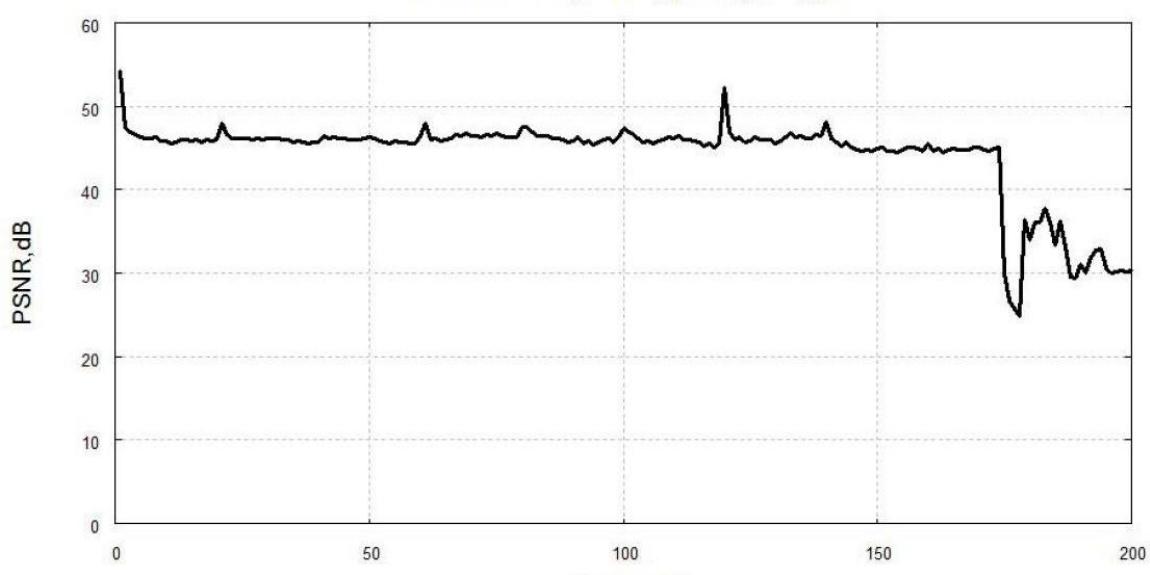

Рисунок 3.15 – Залежність розміру черги на маршрутизаторі від часу , при використанні алгоритму Adaptive RED

Для того щоб отримати максимальну якість відео підемо шляхом налаштування параметрів алгоритму під конкретно розглянутий випадок. Для цього зробимо розрахунок значення w_q під конкретну пропускну здатність каналу. Графіки залежності розміру черги від часу і PSNR від

номера кадру представлені на рис. 3.16 – 3.17. ARED має наступні параметри: min_{th} = 15; max_{th} = 45; max_p = 0,5; α = 0,065; w_q = 0.031.

У порівнянні з попереднім випадком ми маємо поліпшення якості відео, кадри передаються по мережі неспотвореними. Розмір черги зменшився, більшу частину часу він не перевищує 20 пакетів. Різкі збільшення черги пов'язані з передачею I-кадрів , оскільки увесь інший час передаються лише вектори руху, ці викиди є одиничними, і алгоритм не може відреагувати на них.

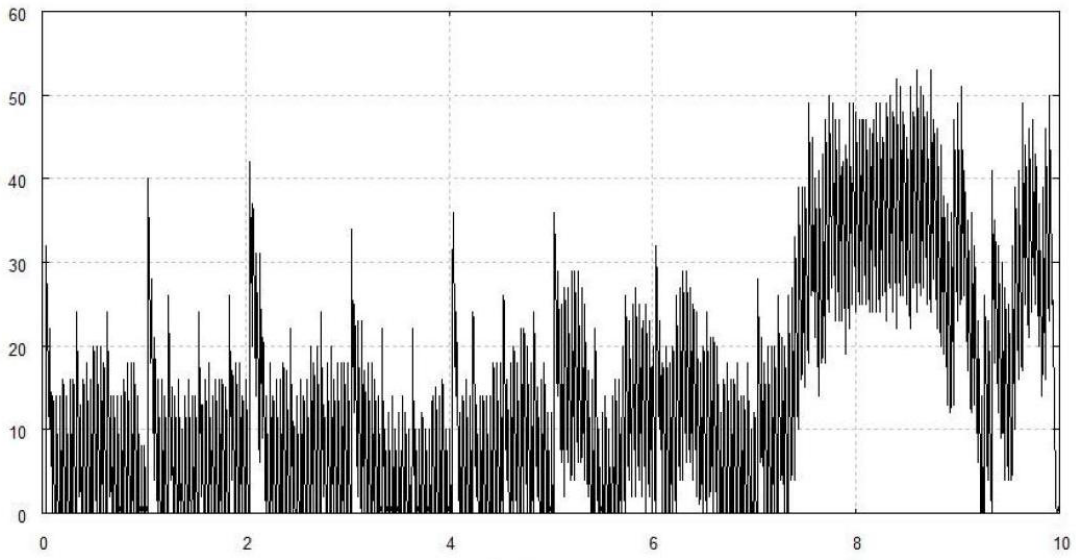

Рисунок 3.16 – Залежності пікового відносини сигнал / шум від номера кадру для тестового відеофрагменту при використанні алгоритму Adaptive RED

Порівнюючи залежності затримок в мережі від часу для трьох алгоритмів, можна помітити, що завдяки малому розміру черги затримки на доставку пакетів при використанні ARED менше (рис. 3.18).

На рис. 3.19 показана залежність довжини черги від часу для алгоритму ARED з параметрами min_{th} = 15; max_{th} = 45; max_p = 0,01; α = 0,065; w_q = 0.031. Як можна помітити, збільшення черги до високого рівня спостерігається лише на проміжку 8–9 сек. Це пов'язано з підвищеною динамікою переданого відео в даний момент часу. При зменшенні кількості переданої інформації алгоритм знижує розмір черги.

Відео передається у високій якості, середнє значення PSNR – 46.3 Дб, це пояснюється тим, що більшу частину часу розмір черги далекий від максимального.

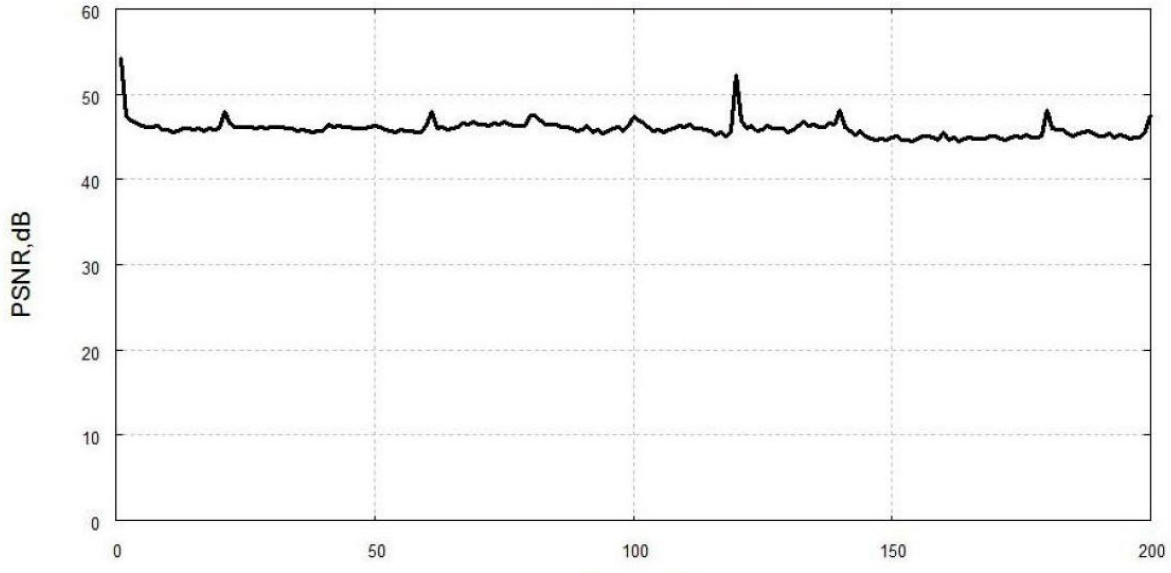

Рисунок 3.17 – Залежність розміру черги на маршрутизаторі від часу , при використанні алгоритму Adaptive RED

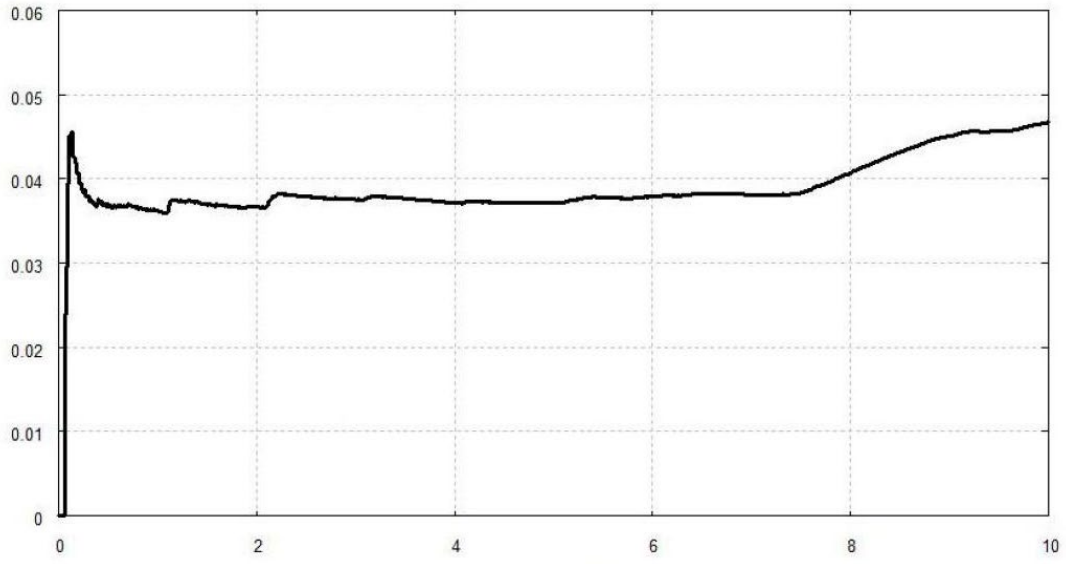

Рисунок 3.18 – Залежність затримки пакету в мережі від часу при використанні алгоритму Adaptive RED

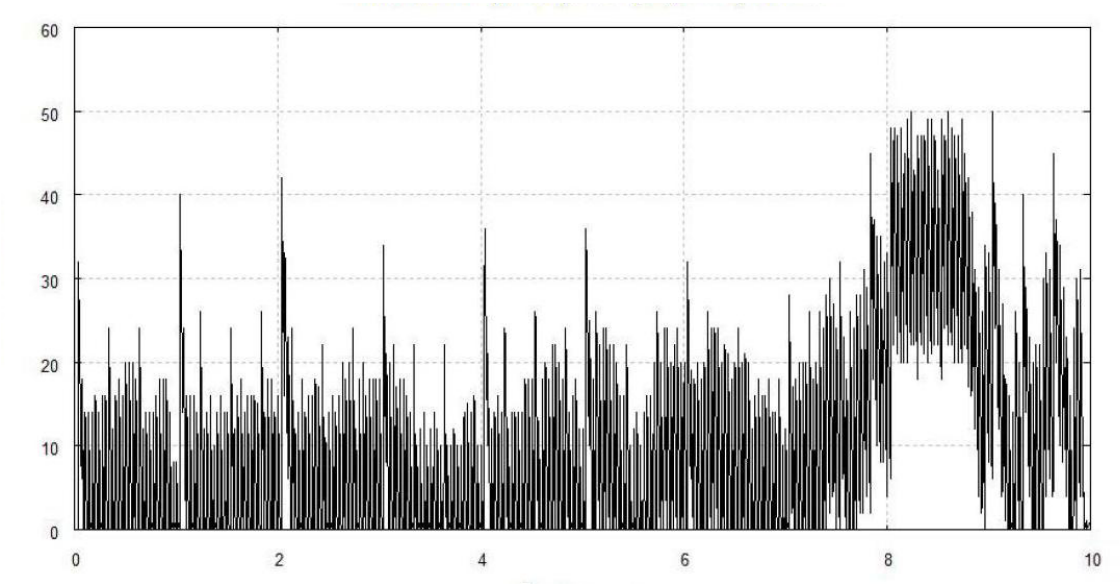

Рисунок 3.19 – Залежності пікового відносини сигнал / шум від номера кадру для тестового відеофрагменту при використанні алгоритму Adaptive RED

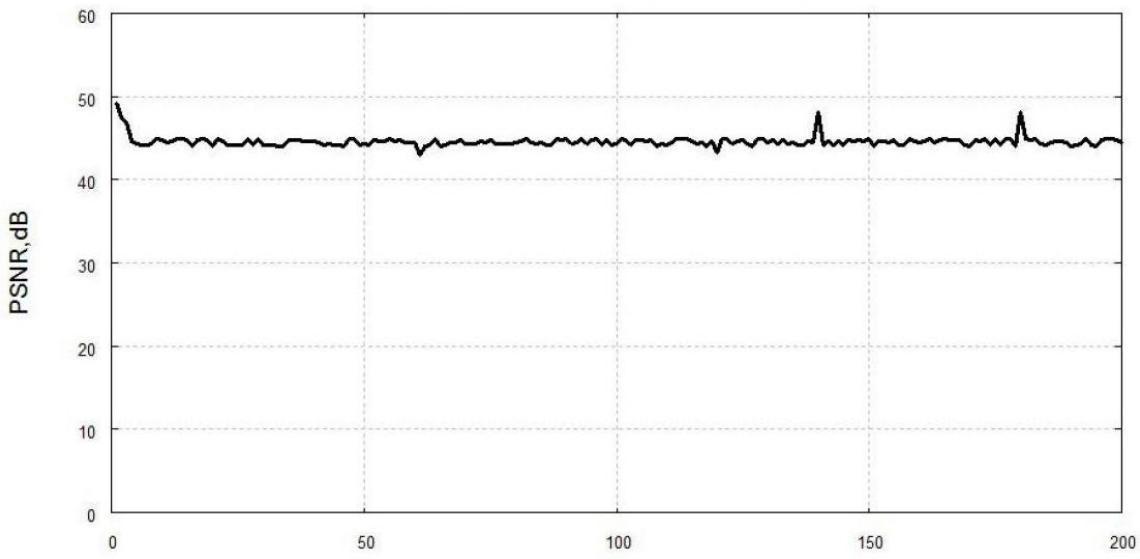

Рисунок 3.20 – Залежність розміру черги на маршрутизаторі від часу при використанні алгоритму Adaptive RED

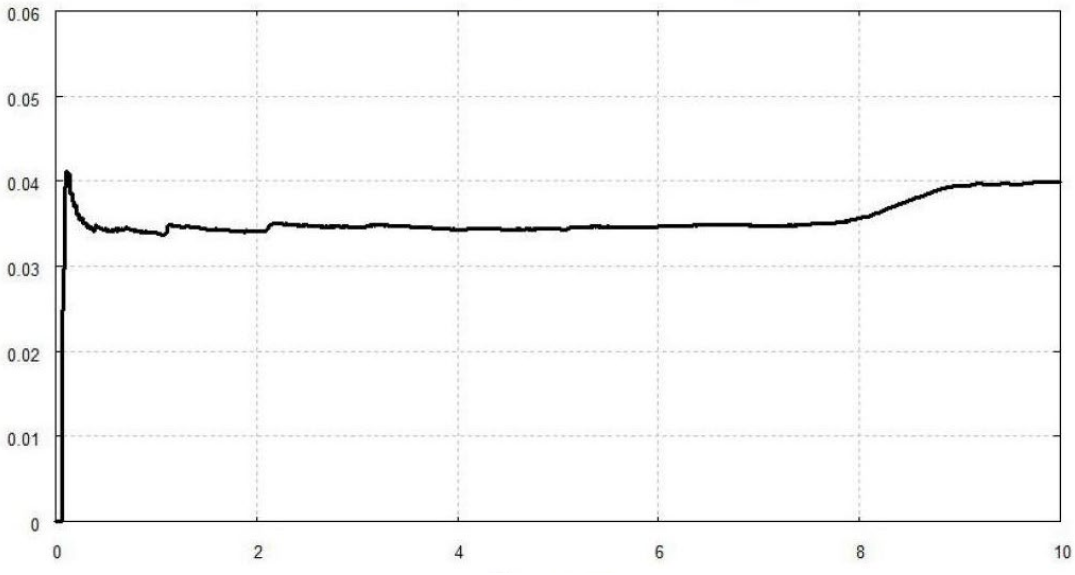

Рисунок 3.21 – Залежність затримки пакету в мережі від часу при використанні алгоритму Adaptive RED

У зв'язку з тим, що маршрутизатор не навантажений, затримка пакетів в мережі знаходиться на постійному рівні, і лише при збільшенні динаміки відео зростає черга і мережева затримка. Наростання не значне з рівня 0.034 сек до 0.04 сек. Даний випадок роботи алгоритму Adaptive RED показує нам найкраще співвідношення якість відео/затримка в мережі.

ВИСНОВКИ

У ході роботи були розглянуті питання, пов'язані з передачею відеоінформації по бездротовій Wi-Fi мережі, при впровадженні на маршрутизатор різних алгоритмів управління чергою пакетів. Також, визначені фактори, що впливають на якість передачі відео. За результатами дослідження були виявлені недоліки у найбільш примітивному алгоритмі – Drop Tail.

Розглянуті алгоритми групи RED, вивчений вплив їх параметрів на роботу мережі. Виявлено тонкощі, пов'язані з налаштуванням параметрів алгоритмів. Було проведено моделювання передачі відео по мережі з використанням даних алгоритмів управління чергою, отримані і проаналізовані показники продуктивності мережі – розмір черги і час доставки пакета, оцінена якість передачі відео на основі найбільш поширеного критерію PSNR.

Аналізуючи отримані результати можливо зробити наступні висновки:

• Найбільший вплив на продуктивність мережі і якості отриманого відео надає довжина черги.

• Алгоритм Drop Tail здатний підтримувати якісну передачу відео тільки при великих обсягах черги.

• Через особливості своєї роботи, алгоритм Drop Tail нераціонально використовує пам'ять маршрутизатора.

• Алгоритми RED і Adaptive RED при правильному налаштуванні здатні поліпшити якість передачі відео, при цьому надаючи меншу навантаження на пам'ять маршрутизатора.

• Найбільш оптимальним для розглянутої конфігурації мережі, з точки зору затримки на доставку пакетів і якості передачі відео, виявився алгоритм Adaptive RED, що має параметри: min_{th} = 15; max_{th} = 45; max_p = 0,01; α = 0,065; w_q = 0.031.

ПЕРЕЛІК ПОСИЛАНЬ

1. Athuraliya S., Li V., S. H. Low S.,YinQ., RED: Active Queue Management, //IEEE Network, May 2001, P.202 – 207
2. Christiansen M., Jeffay K., Ott D., Smith F. Tuning RED for Web traffic // Proceedings of ACM SIGCOMM 2000, August-September 2000, P. 139-150.
3. IEEE Standart Association, available at http://www.ieee.org
4. Floyd S., Gummadi R., Shenker S.Adaptive RED: an algorithm for increasing the robustness of RED's Active Queue Management, http://www.icir.org/floyd/papers/adaptiveRed.pdf, August 2001.
5. Floyd.S., and Fall K. Promoting the use of end-to-end congestion control in the Internet // IEEE/ACM Transactions on Networking, August 1999, P.402–422.
6. Floyd S., Jacobson V. Random early detection gateways for congestion avoidance //IEEE/ACM Transactions on Networking, August 1999, P. 397–413.
7. Elloumi O., Afifi H. RED algorithm in ATM networks // IEEE ATM Workshop 1997. Proceedings, May 2003, P. 312 – 319.
8. Eddy W., Allman M. A comparison of RED's byte and packet modes // Computer Networks, June 2003, P. 103-125.
9. Le L., Aikat J., K. Jeffay. The effects of Active Queue Management and explicit congestion notification on Web performance // IEEE/ACM Transactions on Networking, August 2005, P. 134-147.
10. Feng W. A self-configuring RED gateway //Infocom, Mar 1999, P. 221 – 234.
11. Feng W., Kandlur D., Saha D. Techniques for eliminating packet loss in congested TCP/IP networsk // U. Michigan CSE-TR-349-97, November 1999.
12. Fall K., Varadhan K. The ns nanual. http://www.isi.edu/nsnam/ns/ns-documentation.html

13. Aweya J., Ouellette M., Montuno D.,Chapman A. Enhancing TCP performance with a load-adaptive RED mechanism //International Journal of Network Management, V. 11, N. 1, 2005, P. 304 – 325.
14. Braden R., Clark D., Crowcroft J., Davie D., Deering A.,Estrin D., Floyd S.,Jacobson V., Minshall G., Partridge C., Ramakrishnan K., Zhang L.Recommendations on queue management and congestion avoidance in the Internet. RFC 2309, April 2005.
15. Chiu D., Jain R. Analysis of the increase/decrease algorithms for congestion avoidance in computer networks // Journal of Computer Networks and ISDN, 17(1), June 2003.
16. Lin D., Morris R. Dynamics of Random Early Detection // Proceedings of SIGCOMM 97, September 2001, P.127 – 138.
17. Mahajan, R., Floyd, S. Controlling high-bandwidth flows at the congested Router // ICSI Tech Report TR-01-001, April 2001, P. 235 – 247.
18. Ott T., Lakshman T., Wong L. SRED: Stabilized RED //Proceedings IEEE INFOCOM '99, New York, March 2003, P.123 – 129.
19. Rosolen V., Leduc G. A RED discard strategy for ATM networks and its performance evaluation with TCP/IP traffic // IEE/ACM Computer Communication Review, July 2006, P. 345 – 353.
20. Shenker S., Zhang L., Clark D.Some observations on the dynamics of a congestion control algorithm // ACM Computer Communication Review, October 2008, P.30 – 39.
21. Altman E., Jimenez T. NS simulator for beginners // Lecture notes, 2003-2004 Univ. De Los Andes, Merida, Venezuela and ESSI, Sophia-Antipolis,France, 2003.
22. Kunniyur S., Srikant R. Analysis and design of an adaptive virtual queue (AVQ) algorithm for Active Queue Management // CSL Technical Report, University of Illinois, January 2007 P. 153 – 159.

ДОДАТОК А
ФРАГМЕНТ ЛІСТИНГУ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

```
import ns.core
import ns.network
import ns.applications
import ns.wifi
import ns.mobility
import ns.internet

# This is a simple example in order to show how to configure an IEEE 802.11n Wi-Fi network.

def main(argv):
    cmd = ns.core.CommandLine ()
    cmd.udp = "True"
    cmd.simulationTime = 10 #seconds
    cmd.distance = 1.0 #meters
    cmd.frequency = 5.0 #whether 2.4 or 5.0 GHz

    cmd.AddValue ("frequency", "Whether working in the 2.4 or 5.0 GHz band (other values gets rejected)")
    cmd.AddValue ("distance", "Distance in meters between the station and the access point")
    cmd.AddValue ("simulationTime", "Simulation time in seconds")
    cmd.AddValue ("udp", "UDP if set to True, TCP otherwise")
    cmd.Parse (sys.argv)

    udp = cmd.udp
    simulationTime = float(cmd.simulationTime)
    distance = float(cmd.distance)
    frequency = float(cmd.frequency)

    print "MCS value" , "\t\t", "Channel width", "\t\t", "short GI","\t\t","Throughput" ,'\n'
    for i in range(0,8): #MCS
        j = 20
        while j <= 40: #channel width
            for k in range(0,2): #GI: 0 and 1
                if udp:
                    payloadSize = 1472  #bytes
                else:
                    payloadSize = 1448  #bytes
```

```
                ns.core.Config.SetDefault ("ns3::TcpSocket::SegmentSize",
ns.core.UintegerValue (payloadSize))

            wifiStaNode = ns.network.NodeContainer ()
            wifiStaNode.Create (1)
            wifiApNode = ns.network.NodeContainer ()
            wifiApNode.Create (1)

            channel = ns.wifi.YansWifiChannelHelper.Default ()
            phy = ns.wifi.YansWifiPhyHelper.Default ()
            phy.SetChannel (channel.Create ())

            # Set guard interval
            phy.Set ("ShortGuardEnabled", ns.core.BooleanValue (k))
            wifi = ns.wifi.WifiHelper.Default ()
            if frequency == 5.0:
                wifi.SetStandard (ns.wifi.WIFI_PHY_STANDARD_80211n_5GHZ)

            elif frequency == 2.4:
                wifi.SetStandard (ns.wifi.WIFI_PHY_STANDARD_80211n_2_4GHZ)
                ns.core.Config.SetDefault
("ns3::LogDistancePropagationLossModel::ReferenceLoss", ns.core.DoubleValue (40.046))

            else:
                print "Wrong frequency value!\n"
                return 0

            mac = ns.wifi.HtWifiMacHelper.Default ()
            DataRate = ns.wifi.HtWifiMacHelper.DataRateForMcs (i)
            wifi.SetRemoteStationManager ("ns3::ConstantRateWifiManager","DataMode",
DataRate,
                                          "ControlMode", DataRate)

            ssid = ns.wifi.Ssid ("ns3-80211n")

            mac.SetType ("ns3::StaWifiMac",
                    "Ssid", ns.wifi.SsidValue (ssid),
                    "ActiveProbing", ns.core.BooleanValue (False))

            staDevice = wifi.Install (phy, mac, wifiStaNode)
            mac.SetType ("ns3::ApWifiMac",
                    "Ssid", ns.wifi.SsidValue (ssid))
```

```
                apDevice = wifi.Install (phy, mac, wifiApNode)

                # Set channel width
                ns.core.Config.Set
("/NodeList/*/DeviceList/*/$ns3::WifiNetDevice/Phy/ChannelWidth", ns.core.UintegerValue (j))

                # mobility
                mobility = ns.mobility.MobilityHelper ()
                positionAlloc = ns.mobility.ListPositionAllocator ()

                positionAlloc.Add (ns.core.Vector3D (0.0, 0.0, 0.0))
                positionAlloc.Add (ns.core.Vector3D (distance, 0.0, 0.0))
                mobility.SetPositionAllocator (positionAlloc)

                mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel")

                mobility.Install (wifiApNode)
                mobility.Install (wifiStaNode)

                # Internet stack
                stack = ns.internet.InternetStackHelper ()
                stack.Install (wifiApNode)
                stack.Install (wifiStaNode)

                address = ns.internet.Ipv4AddressHelper ()

                address.SetBase (ns.network.Ipv4Address ("192.168.1.0"), ns.network.Ipv4Mask
("255.255.255.0"))
                staNodeInterface = address.Assign (staDevice)
                apNodeInterface = address.Assign (apDevice)

                # Setting applications
                serverApp = ns.network.ApplicationContainer ()
                sinkApp = ns.network.ApplicationContainer ()
                if udp == "True":
                   # UDP flow
                   myServer=ns.applications.UdpServerHelper (9)
                   serverApp = myServer.Install (ns.network.NodeContainer (wifiStaNode.Get (0)))
                   serverApp.Start (ns.core.Seconds (0.0))
                   serverApp.Stop (ns.core.Seconds (simulationTime + 1))
```

```
                myClient = ns.applications.UdpClientHelper (staNodeInterface.GetAddress (0), 9)
                myClient.SetAttribute ("MaxPackets", ns.core.UintegerValue (4294967295))
                myClient.SetAttribute ("Interval", ns.core.TimeValue (ns.core.Time ("0.00001"))) #
packets/s
                myClient.SetAttribute ("PacketSize", ns.core.UintegerValue (payloadSize))

                clientApp = myClient.Install (ns.network.NodeContainer (wifiApNode.Get (0)))
                clientApp.Start (ns.core.Seconds (1.0))
                clientApp.Stop (ns.core.Seconds (simulationTime + 1))
            else:
                port = 50000
                apLocalAddress = ns.network.Address (ns.network.InetSocketAddress
(ns.network.Ipv4Address.GetAny (), port))
                packetSinkHelper = ns.applications.PacketSinkHelper ("ns3::TcpSocketFactory",
apLocalAddress)
                sinkApp = packetSinkHelper.Install (wifiStaNode.Get (0))

                sinkApp.Start (ns.core.Seconds (0.0))
                sinkApp.Stop (ns.core.Seconds (simulationTime + 1))

                onoff = ns.applications.OnOffHelper ("ns3::TcpSocketFactory",
ns.network.Ipv4Address.GetAny ())
                onoff.SetAttribute ("OnTime", ns.core.StringValue
("ns3::ConstantRandomVariable[Constant=1]"))
                onoff.SetAttribute ("OffTime", ns.core.StringValue
("ns3::ConstantRandomVariable[Constant=0]"))
                onoff.SetAttribute ("PacketSize", ns.core.UintegerValue (payloadSize))
                onoff.SetAttribute ("DataRate", ns.network.DataRateValue (ns.network.DataRate
(1000000000))) # bit/s
                apps = ns.network.ApplicationContainer ()

                remoteAddress = ns.network.AddressValue (ns.network.InetSocketAddress
(staNodeInterface.GetAddress (0), port))
                onoff.SetAttribute ("Remote", remoteAddress)
                apps.Add (onoff.Install (wifiApNode.Get (0)))
                apps.Start (ns.core.Seconds (1.0))
                apps.Stop (ns.core.Seconds (simulationTime + 1))

            ns.internet.Ipv4GlobalRoutingHelper.PopulateRoutingTables ()

            ns.core.Simulator.Stop (ns.core.Seconds (simulationTime + 1))
            ns.core.Simulator.Run ()
```

```
                ns.core.Simulator.Destroy ()

                throughput = 0
                if udp == "True":
                    # UDP
                    totalPacketsThrough = serverApp.Get (0).GetReceived ()
                    throughput = totalPacketsThrough * payloadSize * 8 / (simulationTime *
1000000.0) # Mbit/s

                else:
                    # TCP
                    totalPacketsThrough = sinkApp.Get (0).GetTotalRx ()
                    throughput = totalPacketsThrough * 8 / (simulationTime * 1000000.0)     # Mbit/s

                print i, "\t\t\t", j , " MHz\t\t\t", k , "\t\t\t" , throughput , " Mbit/s"
            j *= 2
        return 0

    if __name__ == '__main__':
        import sys
        sys.exit (main (sys.argv))
```