Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки, факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра Радіотехніки та телекомунікацій
(повне найменування кафедри)

Пояснювальна записка

до магістерської роботи
(ступінь вищої освіти)

на тему „Дослідження завадостійкості технології Wi-Fi в умовах аеропорту"

Виконав: студент(ка) VI курсу, групи РТ-918м

Спеціальності 172 «Телекомунікації та радіотехніка»
(код і найменування спеціальності)

Освітньої програми Інформаційні мережі зв'язку

Бубенець І. І.
(прізвище та ініціали)

Керівник Костенко В. О.
(прізвище та ініціали)

Рецензент Фурманова Н. І.
(прізвище та ініціали)

2019

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут інформатики та радіоелектроніки, факультет радіоелектроніки та телекомунікацій
Кафедра Радіотехніки та телекомунікацій
Ступінь вищої освіти другій (магістерський)
Спеціальність 172 «Телекомунікації та радіотехніка»
(код і найменування)
Освітня програма Інформаційні мережі зв'язку
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри РТТ
к.т.н., доц. Морщавка С.В.
«____» _____ 20___ року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА (КИ)

Бубенець Ілля Іванович
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження завадостійкості технології Wi-Fi в умовах аеропорту

керівник роботи доц. Костенко Валер'ян Остапович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «08» листопада 2019 року № 365
2. Строк подання студентом роботи 20 грудня 2019 року
3. Вихідні дані до роботи Умови роботи Wi-Fi мережі у Запорізькому аеропорті на 2-ох поверхах і динамічними приміщень.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Моделювання роботи мережі Wi-Fi в умовах аеропорту з урахуванням завад, формулювання рекомендацій для практичного застосування

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

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4 розділ	Костенко В.О доц		
Н.контроль	Мороз І.В		
Економічна	Лівошко Т.В доц		
Охорона праці	Якімцов Ю.В.		

7. Дата видачі завдання « 02 » Вересня 2019 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Знайомство з літературними джерелами по темі дипломну	20 вересня 2019	викон.
2.	Збір інформації з аеропортів, що до досвіду роботи Wi-Fi	04 жовтня 19	викон
3.	Моделювання мережі в мережевому симуляторі OPNET	31 жовтня 19	викон.
4	Формування результатів моделювання та обробки експеремектальних даних	14 листопада	викон.
5.	Підготовка економічного блоку та блоку захисту праці.	29 листопада	викон.
6.	Написання дипломної роботи	10 грудня 19	викон.
7.	Підготовка презентації	15 грудня 19	викон.
8.	Захист дипломної роботи	17 грудня 19	викон.

Студент(ка) _____ Бубенець І.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Костенко В.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 122 сторінки, 41 рисунок, 23 таблиці, 14 джерел

Об'єкт дослідження – завадостійкості мережі Wi-Fi в умовах постійних шумів та завад, які відбуваються середовищі аеропорту.

Мета роботи – визначення причин виникнення основних завад та шумів в умовах аеропорту, проведення аналізу завадостійкості Wi-Fi в цих умовах та знайдення рішень з їх усунення.

Метод дослідження – експериментальний.

В першому розділі розглянуто теоретичні основи бездротового доступу Wi-Fi, основні стандарти бездротового доступу та фактори впливу на поширення Wi-Fi сигналу. У другому розділі приведені послуги Wi-Fi в аеропортах та проблема перешкод, які наявні в цих умовах. У третьому розділі проводиться аналіз мережевих симуляторів, їх опис та на основі цих даних обирається найкращий симулятор. У четвертому розділі проводиться аналіз моделі, проводиться збір отриманих даних, та на їх основі розробляються методи протидії завадам. У п’ятому розділі розраховані економічні аспекти проекту, виходячи з яких, він є економічно ефективним. У шостому розділі розглядається охорона праці та безпека життєдіяльності.

ЗАВАДОСТІЙКІСТЬ, МЕРЕЖІ WI-FI, ПОРІВНЯЛЬНИЙ АНАЛІЗ, АЕРОПОРТ, ШУМИ ТА ЗАВАДИ, МЕРЕЖЕВИЙ СИМУЛЯТОР, OPNET

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AP – (Access Point) точка доступу

DFD – (Data Flow Diagrams) діаграми потоку даних

WI-FI – (Wireless Fidelity) технологія бездротової локальної мережі

GMSK – (Gaussian Minimum Shift Keying) гаусовська маніпуляція з мінімальним фазовим зрушенням

CSMA/CD – (Carrier Sense Multiple Access with Collision Detection) множинний доступ з прослуховуванням несучої і виявленням колізій

DSR – (Dynamic Source Routing) динамічна маршрутизація від джерела

PSK – (Phase-Shift Keying) фазова маніпуляція

MAC – (Media Access Control) управління доступом до середовища

QAM – (Quadrature Amplitude Modulation) квадратурна амплітудна модуляція

ІС – інформаційна система

БД – база даних

ВСТУП

В останнє десятиліття XX століття бездротові цифрові комунікації вступили в фазу бурхливого розвитку, яка триває і в даний час. Поштовхом до цього стало, з одного боку, інтенсивний розвиток глобальної мережі Інтернет, з іншого – впровадження нових, прогресивних методів кодування, модуляції і передачі інформації. В даний час очевидно, що бездротові широкосмугові мережі знаходяться поза конкуренцією по оперативності розгортання, мобільності, ціною і широтою можливих пропозицій, у багатьох випадках будучи єдиним економічно виправданим рішенням.

Технологія WI-FI застосовується і розвивається давно, вона дозволяє створити безпечний і високошвидкісний канал передачі даних для кожного абонента. Але можуть виникнути великі проблеми з завадостійкістю на території з великою кількістю завад та шумів. Аеропорт і є одним з таких місць.

Бездротові послуги в аеропортах розширилися від інструменту голосового зв’язку між контролем повітряного руху та пілотами, між службами громадської безпеки аеропорту, як поліція, пожежні та технічними службами в аеропорті, до повсюдної та складної інформаційної системи, які зазвичай підтримуються через спільну мережеву інфраструктуру.

В цій роботі буде проведено аналіз проблем зв'язаних з інтерференцією, завадами та шумами для WI-FI на території аеропорту. Тому ця робота є актуальною на цей час.

1 ТЕОРЕТИЧНІ ОСНОВИ ТЕХНОЛОГІЇ БЕЗДРОТОВОГО ДОСТУПУ WI-FI

1.1 Основні поняття і теоретичні положення

Бурхливий розвиток інтернету і глобальна комп'ютеризація суспільства дала величезний стрибок розвитку бездротових технологій. Бездротовий зв'язок дозволяє підключити віддалені об'єкти, замінюючи кілометри проводів і заощаджуючи чимало грошей, а також, рухатися в зоні покриття мережі залишаючись на зв'язку.

Існує три типи бездротових мереж (рисунок 1.1):

– бездротові персональні мережі або WPAN (Wireless Personal Area Network);

– бездротові локальні мережі або WLAN (Wireless Local Area Network);

– бездротова глобальна мережа або BWA (Broadband Wireless Access

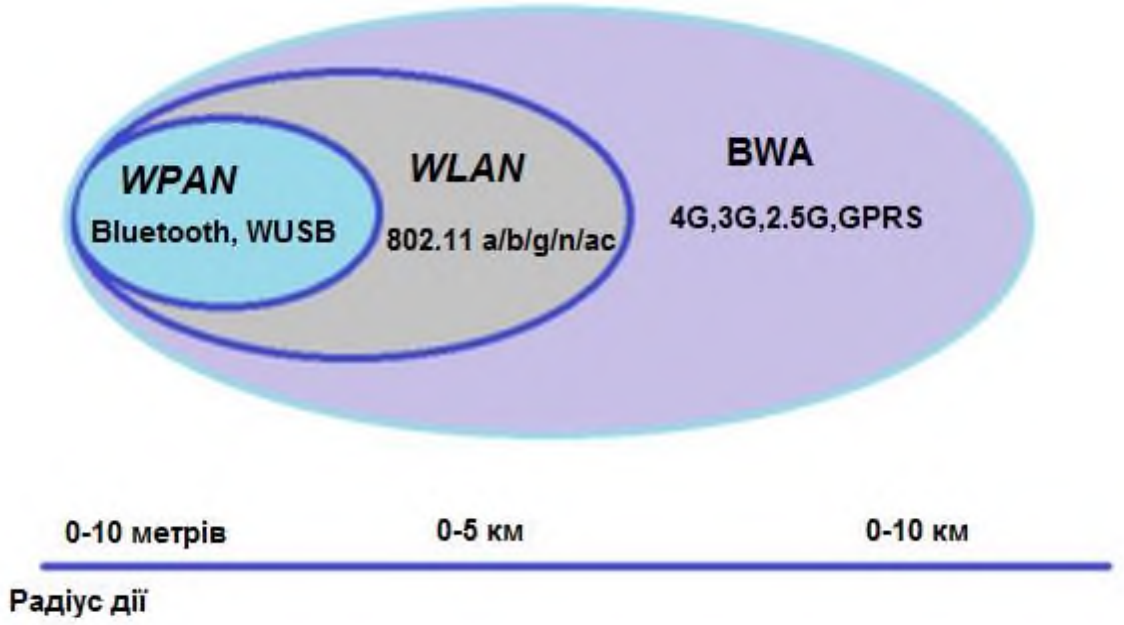


Рисунок 1.1 – Дальність дії бездротових мереж

При побудові мереж WLAN і WPAN, а також систем широкосмугового бездротового доступу BWA (Broadband Wireless Access) використовуються схожі технології, та їх діапазон робочих частот (рисунок 1.2). Мережі WLAN і WPAN працюють в неліцензійних діапазонах частот 2,4 і 5 ГГц, при їх розгортанні не потрібне частотне планування і координація з іншими радіомережами, що працюють в тому ж діапазоні.

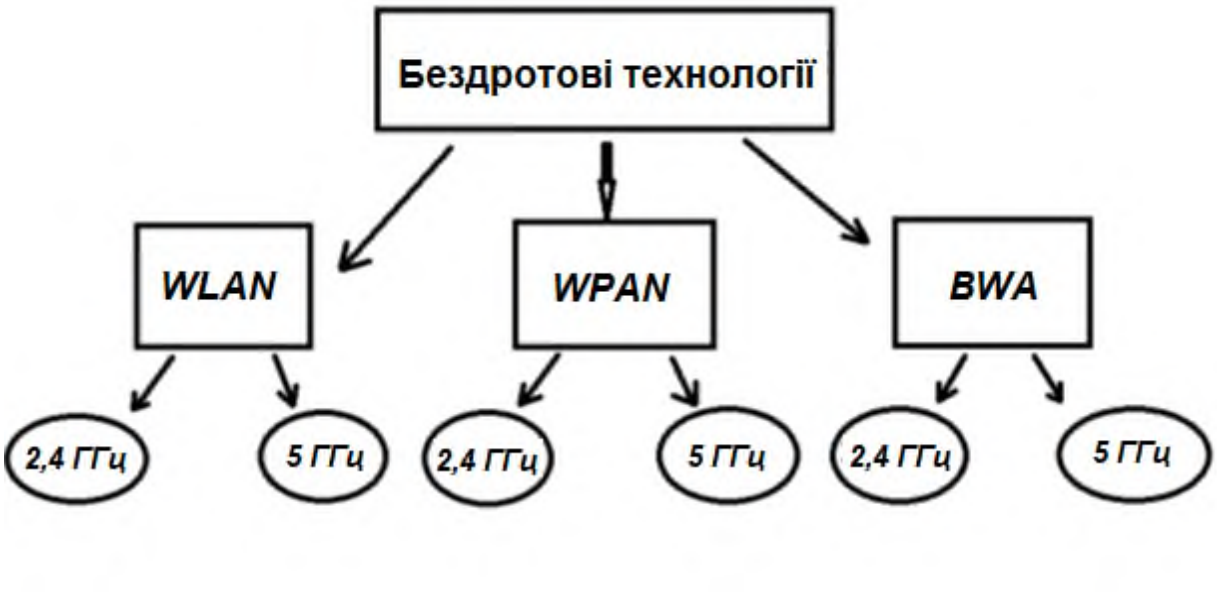


Рисунок 1.2 – Класифікація діапазонів робочих частот бездротових технологій

Бездротові локальні мережі WLAN

Основні призначення бездротових локальних мереж (WLAN) – організація доступу до інформаційних ресурсів всередині будівлі. Друга за значимістю сфера застосування – це організація громадських комерційних точок доступу (hot spots) в людних місцях – готелях, аеропортах, кафе, а також організація тимчасових мереж на період проведення заходів (виставок, семінарів).

Бездротові локальні мережі створюються на основі сімейства стандартів IEEE 802.11. Ці мережі відомі також як WI-FI (Wireless Fidelity). Хоча сам термін в стандартах явно не прописаний, бренд WI-FI отримав в світі найширше розповсюдження.

1.2 Основні стандарти бездротового доступу

У 1990 році Комітет IEEE 802 (Institute of Electrical and Electronic Engineers) сформував групу для створення стандартів бездротових мереж. Це група зайнялася розробкою мереж, що працюють на частоті 2.4 ГГц зі швидкостями 1 і 2 Мбіт/с. У 1997 році був створений перший стандарт IEEE 802.11.

Стандарт IEEE 802.11 став першим продуктом WLAN від незалежної міжнародної компанії, але до моменту старту стандарту закладеної швидкості виявилося недостатньо. Це послужило причиною подальших доробок, після яких з'явилось багато стандартів протоколу IEEE 802.11.

Стандарт IEEE 802.11b.

Стандарт IEEE 802.11b був прийнятий в 1999 році. Підтримує швидкість передачі даних до 11 Мбіт/с і має діапазон 2,4 ГГц, цей стандарт користувався популярністю у виробників бездротового обладнання. Устаткування працювало на максимальній швидкості, мало невеличкий радіус дії і при погіршенні сигналу знижувало швидкість передачі даних для збільшення радіусу дії. Для передачі сигналу використовується метод прямої послідовності (Direct Sequence Spread Spectrum), який використовує 5 діапазонів, що перекривають один одного для передачі даних. Значення кожного біта кодуються послідовністю додаткових кодів (Complementary Code Keying).

Стандарт IEEE 802.11a.

Стандарт IEEE 802.11a ратифікований в 1999 р. і підтримує швидкість передачі даних до 54 Мбіт/с. Робочий діапазон 2.4 ГГц і 5 ГГц. В якості методу модуляції сигналу використовує ортогональне частотне мультиплексування (OFDM). OFDM передбачає паралельну передачу сигналу по декільком частотам діапазону, в той час як технології розширення спектру виробляють передачу сигналу послідовно. За рахунок цієї технології збільшується пропускна здатність каналу і якість сигналу. До недоліків стандарту IEEE 802.11a відносяться більш висока споживана потужність радіопередавачів для частот 5 ГГц, а так же менший

радіус дії (обладнання для 2,4 ГГц може працювати на відстані до 300м, а для 5 ГГц - близько 100 м).

Стандарт IEEE 802.11g.

Стандарт IEEE 802.11g підтримує швидкість передачі даних до 54 Мбіт/с і працює в діапазоні частот 2.4 Гц, що дозволяє забезпечити сумісність зі стандартом IEEE 802.11b, який використовує той же діапазон. За рахунок менших несучих частот в порівнянні зі стандартом 802.11a на одну і ту ж площу потрібно менше точок доступу. Стандарт 802.11g використовує схему модуляції сигналу OFDM. Це ортогональне мультиплексування частот, яке менше схильне до погіршення якості від працюючих поруч каналів (інтерференція). Таким чином, стандарт IEEE 802.11g може «обслуговувати» бездротових клієнтів з меншими затримками, ніж IEEE 802.11b.

Стандарт IEEE 802.11n.

Цей стандарт був затверджений 11 вересня 2009 році. Стандарт 802.11n підвищує швидкість передачі даних майже вчетверо в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 600 Мбіт/с (стандарт IEEE 802.11ac до 1.3 Гбіт/с), застосовуючи передачу даних відразу на чотирьох антенах. На кожній антені швидкість досягає до 150 Мбіт/с. Пристрої 802.11n працюють в діапазонах 2,4-2,5 ГГц або 5,0 ГГц.

Крім того, пристрої 802.11n можуть працювати в трьох режимах:

– успадкованому (Legacy), в якому забезпечується підтримка пристроїв 802.11b/g і 802.11a;

– змішаному (Mixed), в якому підтримуються пристрої 802.11b/g, 802.11a і 802.11n;

– «чистому» режимі – 802.11n (саме в цьому режимі і можна скористатися перевагами підвищеної швидкості і збільшеною дальністю передачі даних, що забезпечуються стандартом 802.11n).

Стандарт IEEE 802.11ac.

Черговим етапом розвитку технології було позначено створенням стандарту, здатного забезпечити максимальну пропускну здатність понад 1 Гбіт/с при збереженні колишньої дальності і стабільності з'єднання. Задача була вирішена в 2011 році з виходом чорнових варіантів - draft- нового стандарту WI-FI, який отримав назву 802.11/ac. Однак остаточна сертифікація та затвердження стандарту відбулося лише в кінці 2013 року і перші пристрої з підтримкою 802.11/ac почали з'являтися у продажу з 2014 року.

Відмінностей нового стандарту 802.11/ac від попереднього 802. 11/n багато і вони істотні. WI-FI 802.11/ac використовує для передачі даних частоту 5 ГГц. Це пов'язано з великою кількістю і шириною каналів, які можуть використовуватися на цій частоті, а також менша зашумленість даного діапазону. Але, незважаючи на використання діапазону 5 ГГц, обладнання з підтримкою 802.11/ac повністю сумісна з попередніми версіями WI-FI. Істотно в 802.11/ac збільшилася швидкість передачі даних, яка стала 866 Мбіт/с на один канал. Досягнуто такі цифри за рахунок збільшення максимальної ширини каналу до 160 МГц і використання модуляції 256 QAM. Правда, слід зазначити, що в доступних на даний момент пристроях канали обмежені шириною 80 МГц, але в подальшому очікується вихід пристроїв з підтримкою каналів 160 МГц. Впроваджено технологію MU-MIMO, яка відрізняється від MIMO підтримкою OFDM мультиплексування, а також можливістю синхронного використання до 8 просторових потоків даних, що в перспективі дозволяє досягати швидкості майже в 7 Гбіт/с. Треба сказати, що в підтримці OFDM немає чогось принципово нового, технологія вже використовувалася в WI-FI і раніше. Але різниця полягає в тому, що в 802.11/n всі потоки використовувалися для передачі даних одному абоненту. Мінусом такої схеми було вкрай нераціональне використання ресурсів каналу, наприклад, при передачі потоку даних на швидкості 15 Мбіт/с абонент повністю займав канал пропускною спроможністю каналу 150 Мбіт/с. WI-FI точка доступу працювала лише з ним, в той час як інші пристрої чекали своєї черги на передачу даних.

MU-MIMO розділяє канал на кілька менших OFDM півканалів для одночасної роботи з різними клієнтами, тим самим значно підвищуючи

ефективність використання мережі, що особливо критично в умовах великої кількості низько швидкісних абонентів.

Ще один плюс 802.11/ac – це опціональна підтримка beamforming технології, яка оптимізує енергоспоживання і підвищує стійкість бездротового з'єднання за рахунок динамічного управління діаграмою спрямованості. Принцип роботи beamforming складається в створенні ефекту підсилення інтерференції в зоні знаходження абонента за допомогою зсуву фази при передачі сигналу декількома антенами або випроміненням елементів антенної решітки. Спроби застосування beamforming технології в WI-FI були і раніше, але стандартизацію і, отже, сумісність при використанні обладнання від різних виробників вона отримала лише з виходом 802.11/ac.

Завдяки збільшенню ширини каналу, використання модуляції 256 QAM і підтримки до 8 просторових каналів, стандарт 802.11ac володіє дуже високим швидкісним потенціалом – до 7 Гбіт/с, а використання MU-MIMO забезпечить значний приріст продуктивності при роботі в великих мережах.

1.3 Частотне планування в бездротових мережах WI-FI

Мережі стандарту IEEE 802.11 працюють в спеціальному радіочастотному діапазоні 2,4 ГГц і 5 ГГц, які зарезервовані в більшості країн світу і не вимагають ліцензій для радіослужб. Це означає, що будь-яке обладнання, відповідним технічним вимогам, може передавати і приймати радіосигнали на цих частотах не отримуючи ліцензію на обладнання. На відміну від більшості радіослужб, які вимагають ліцензії на право ексклюзивного використання частоти і обмежують використання даної частоти певною частотою, то радіочастоти 2,4 ГГц і 5 ГГц є загальнодоступними, і кожен має рівні права на одну і туж ділянку спектра.

Теоретично технологія радіо з розподілом спектру уможливлює роботу з іншими користувачами без значних взаємних перешкод. За міжнародною угодою ділянку радіочастотного спектру близько 2,4 ГГц передбачається резервувати під неліцензовані промислові, наукові та медичні служби, включаючи бездротові

мережі для передачі даних з розширеним спектром. Однак в різних країнах частотні діапазони відрізняються один від одного.

Відмінності у розподілі частот не є особливо важливими, оскільки більшість мереж працюють цілком в межах однієї країни або регіону, а нормальна зона покриття сигналу зазвичай лежить в межах декількох сотень метрів.

У Північній Америці WI-FI пристрої використовують 11 каналів. Інші країни використовують 13 каналів, в Японії їх 14, а у Франції – тільки 4. У всьому світі набір номерів каналів один і той же, тому канал № 9 в Нью-Йорку використовує в точності таку ж частоту, що і канал № 9 в Токіо або Парижі. У таблиці 1.1 представлені канали різних країн і регіонів.

Таблиця 1.1 – Розподіл каналів WI-FI

Канал	**Частота (МГц) і місце розташування**
1	2412 (США, Європа, СНД і Японія)
2	2417 (США, Європа, СНД і Японія)
3	2422 (США, Європа, СНД і Японія)
4	2427 (США, Європа, СНД і Японія)
5	2432 (США, Європа, СНД і Японія)
6	2437 (США, Європа, СНД і Японія)
7	2442 (США, Європа, СНД і Японія)
8	2447 (США, Європа, СНД і Японія)
9	2452 (США, Європа, СНД і Японія)
10	2457 (США, Європа, Франція СНД і Японія)
11	2462 (США, Європа, Франція СНД і Японія)
12	2467 (Європа, Франція, СНД і Японія)
13	2472 (Європа, Франція, СНД і Японія)

Канада і деякі інші країни користуються тим же розподілом каналів, що і Сполучені Штати.

Помітно, що частота, певна для кожного з цих каналів, насправді є центральною частотою каналу шириною 22 МГц. Тому кожен канал перекриває кілька інших, розташованих вище і нижче його. Повний діапазон 2,4 ГГц має простір тільки для трьох непересічних каналів, тому, якщо одна мережа працює, скажімо, на четвертому каналі, а сусідня використовує п'ятий або шостий, кожна мережа буде детектувати сигнали з іншої як перешкоди. Обидві мережі будуть працювати, але ефективність (що відбивається в швидкості передачі даних) буде не оптимальною.

В міру можливостей кожна мережа повинна використовувати канали, які розділені, щонайменше, смугою 25 МГц.

Для усунення перешкоди між двома мережами, використовується один канал зі старшим номером, а інший з молодшим. У разі трьох каналів найкращим вибором будуть № 1, 6 і 11, як показано на рисунку 1.3. При роботі в більш ніж трьох мережах доведеться змиритися з деякою кількістю перешкод, але можна звести їх до мінімуму, призначивши новий канал в проміжку між наявною парою.

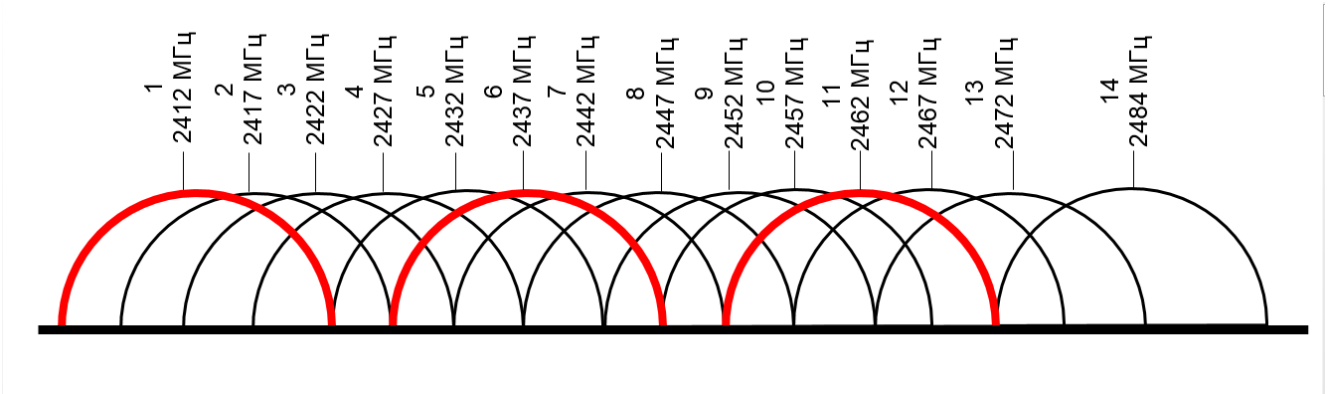


Рисунок 1.3 – Неперекриваючі частотні канали технології WI-FI

На практиці справа йде простіше. Можна оптимізувати ефективність мережі, тримаючись подалі від каналу, який використовується ким-небудь ще. Є ймовірність зіткнутися з проблемами перешкод від інших пристроїв, що використовують діапазон 2,4 ГГц, наприклад бездротових телефонів і мікрохвильових печей.

Специфікації 802.11 і різні національні органи державного регулювання (наприклад, Федеральна комісія зв'язку в Сполучених Штатах) ставлять обмеження на потужність передавача і коефіцієнта посилення антени, які мають можливості застосовувати бездротові пристрої. Специфікація спеціалізована для обмеження відстані, на яке має можливість вестися зв'язок і дозволяє найбільшою кількістю мереж діяти в одному з каналів у відсутності перешкод. Основна відмінність стандарту 802.11ac від 802.11n полягає в його продуктивності.

Швидкість передачі даних стандарту 802.11ac становить 1,3 Гбіт/с, що трикратно перевищує можливості стандарту 802.11n, який підтримує швидкість до 450 Мбіт/с. Розробка з'єднання каналів (Channel Bonding), що з'явилася ще в ідеалі 802.11n, дозволяє збільшити ймовірну ширину каналу по 40 МГц.

Для досягнення найбільшої пропускної здатності в 1,3 Гбіт/с в одному бездротовому осередку 802.11ac можливі канали шириною до 80 МГц.

На наступних етапах розвитку стандарту передбачається допомога каналів шириною 160 МГц, що дозволить в два рази наростити найбільшу швидкість передачі всередині бездротового осередку, однак чисельність синхронно застосовуваних осередків в цьому випадку зменшиться.

У частотному діапазоні 5 ГГц доступні 19 неперекриваючих каналів шириною 20 МГц, які, відповідно до стандарту 802.11ac, можна об'єднувати в канали шириною до 80 або навіть 160 МГц. (Для порівняння, технологія об'єднання каналів в стандарті 802.11n передбачає лише канали з максимальною шириною в 40 МГц.)

У таблиці 1.2 наведені дані в порівнянні досяжних швидкостей передачі даних в стандартах 802.11n і 802.11ac в залежності від ширини каналу (по горизонталі) і кількості просторових потоків (по вертикалі). Перший варіант стандарту 802.11ac дозволяє досягти швидкості 1,3 Гбіт/с (при трьох просторових потоках і ширині каналу 80 МГц).

Таблиця 1.2 – Порівняння швидкостей передачі даних в стандартах 802.11n і 802.11ac

Кількість просторових потоків	**802.11n 20 МГц**	**802.11n 40 МГц**	**802.11n 80 МГц**	**802.11n 160 МГц**
1	75 Мбіт/с	150 Мбіт/с	433 Мбіт/с	867 Мбіт/с
2	150 Мбіт/с	300 Мбіт/с	867 Мбіт/с	1,7 Гбіт/с
3	225 Мбіт/с	450 Мбіт/с	1,3 Гбіт/с	2,5 Гбіт/с

У середовищах, де число користувачів велике, застосування каналів шириною 160 МГц, швидше за все, не дасть ніяких переваг.

Більш висока продуктивність стандарту 802.11ac порівняно з 802.11n пояснюється ще і застосуванням істотно більш складного методу амплітудної модуляції. Квадратурна амплітудна модуляція (QAM) дозволяє шляхом накладення декількох хвиль описувати різні стани (наприклад, «0» або «1»). У стандарті 802.11n використовується метод 64-QAM, в той час як в 802.11ac можна реалізувати навіть 256 QAM.

Завдяки цьому кожен накладений сигнал дозволяє одночасно передавати вісім біт інформації замість шести, як раніше. Зараз для цього використовують не більше трьох просторових потоків (Spatial Stream), але очікується збільшення їх кількості до восьми.

1.4 Фактори, що впливають на поширення WI-FI сигналу

Бездротові мережі в якості середовища поширення сигналу використовують радіохвилі (радіоефір), і робота обладнання в мережі відбувається без використання кабельного з'єднання. У зв'язку з цим на роботу бездротових мереж впливає велика кількість різного роду перешкод. Однією з поширених проблем впливу на роботу бездротових мереж (IEEE 802.11b/g/n/ac), є працюючі в радіусі

дії обладнання. У бездротових мережах використовуються два частотні діапазони – 2,4 і 5 ГГц.

Бездротові мережі стандарту IEEE 802.11b/g працюють в діапазоні 2,4 ГГц, мережі стандарту IEEE 802.11a/ac – 5 ГГц, а мережі стандарту IEEE 802.11n можуть працювати як в діапазоні 2,4 ГГц, так і в діапазоні 5 ГГц. У смузі частот 2,4 ГГц для бездротових мереж доступні 13 каналів шириною 20 МГц (IEEE 802.11b/g/n) або 40 МГц (IEEE IEE 802.11n) з інтервалами 5 МГц між ними. Бездротовий пристрій, що використовує один з 13 WI-FI частотних каналів, створює значні перешкоди на сусідні канали. Наприклад, якщо точка доступу використовує канал 6, то вона надає сильні перешкоди на канали 5 і 7, а також, вже в меншому ступені, на канали 4 і 8. Для виключення взаємних перешкод між каналами необхідно, щоб їх несучі віддалялися один від одного на 25 МГц (5 між канальних інтервалів).

Колірне кодування (рисунок 1.4) позначає групи непересічних каналів – (1,6,11), (2,7), (3,8), (4,9), (5,10). Різні бездротові мережі, розташовані в межах однієї зони дії, слід налаштовувати на непересічні канали. Якщо бездротовий адаптер, встановлений на комп'ютері (ноутбуці, планшетному ПК, смартфоні), призначений для використання в США, на ньому можна буде використовувати тільки канали з 1 по 11.

Тому, якщо встановити номер каналу 12 або 13 (а також, якщо один з них був обраний алгоритмом автоматичного вибору каналу), бездротовий клієнт не побачить точку доступу. В цьому випадку необхідно вручну встановити номер каналу з діапазону з 1 по 11.

Bluetooth пристрої працюють в тому ж частотному діапазоні, що і WI-FI пристрої, 2,4 ГГц, отже, можуть впливати на роботу WI-FI-пристроїв.

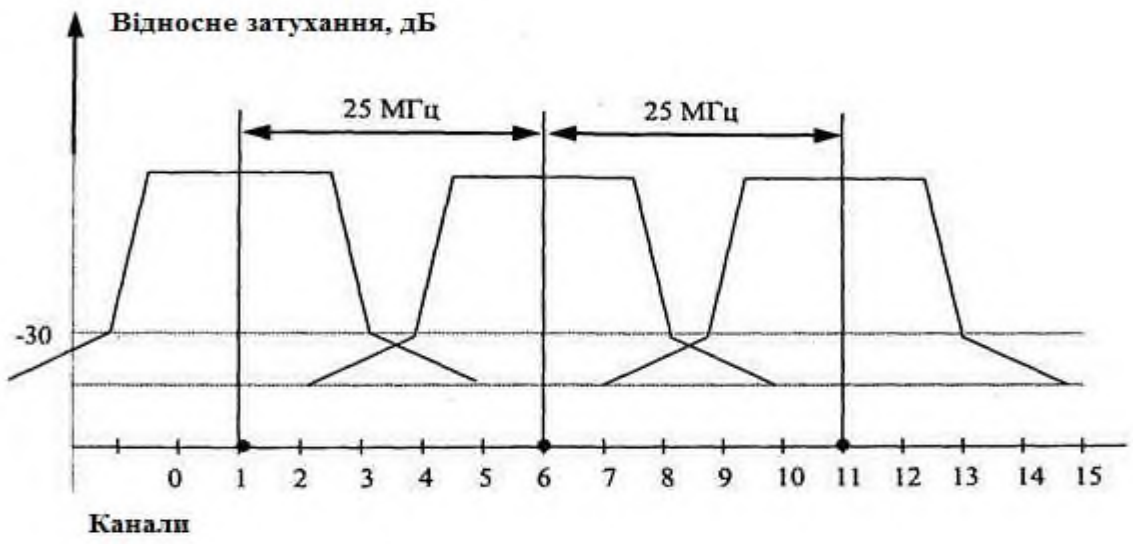


Рисунок 1.4 – Спектри 11 каналів

Великі відстані між WI-FI-пристроями.

Бездротові пристрої WI-FI мають обмежений радіус дії. Наприклад, домашній роутер з точкою доступу WI-FI стандарту 802.11b / g має радіус дії до 60 м в приміщенні і до 400 м поза приміщенням.

Всередині приміщення створювати перешкоди радіосигналу можуть дзеркала і тоновані вікна. У таблиці 1.3 показані втрати ефективності сигналу WI-FI при проходженні через різні середовища.

Ефективна відстань – означає, наскільки зменшиться радіус дії після проходження відповідної перешкоди.

Поза приміщеннями впливати на якість сигналу, що передається може ландшафт місцевості (наприклад, дерева, ліси, пагорби). Атмосферні перешкоди (дощ, гроза, снігопад) також можуть бути причиною зменшення продуктивності бездротової мережі (в разі, якщо радіосигнал передається поза приміщеннями).

Таблиця 1.3 – Ефективність сигналу WI-FI

Перешкода	Додаткові втрати (дБ)	Ефективна відстань
Відкритий простір	0	90%
Вікно без тонування (відсутнє металізоване покриття)	3	70%
Вікно з тонуванням (металізоване покриття)	5-8	50%
Дерев'яна стіна	10	30%
Міжкімнатні стіна (15,2 см)	15-20	15%
Бетонна підлога / стеля	20-25	10%
Монолітне залізобетонне перекриття	15-25	10-15%

Перерахуємо побутову техніку, яка може бути причиною погіршення якості зв'язку WI-FI:

– мікрохвильові НВЧ-печі, ці прилади можуть послаблювати рівень сигналу WI-FI, тому що зазвичай також працюють в діапазоні 2,4 ГГц;

– дитячі «няньки», ці прилади працюють в діапазоні 2,4 ГГц і дають наведення, в результаті чого погіршується якість зв'язку WI-FI;

– монітори з ЕПТ (електронно-променевої трубки), електромотори, бездротові телефони та інші бездротові пристрої.

1.5 Захист інформації в мережах WI-FI

Для захисту IEEE 802.11 стандартом передбачений комплекс заходів безпеки передачі даних під загальною назвою Wired Equivalent Privacy (WEP).

Він включає засоби протидії несанкціонованому доступу до мережі (механізми і процедури ідентифікації), а також запобігання перехопленню інформації. WEP, незважаючи на необов'язковість, доступний як механізм

першого покоління забезпечення захищеної взаємодії між вузлами і захисту потоків даних в бездротових мережах.

Основні цілі WEP – це:

– заборонити доступ до мережі неавторизованим користувачам, які не володіють відповідним WEP ключем;

– запобігти дешифрування захопленого трафіку без знання WEP ключа.

WEP – це механізм симетричного шифрування. Якщо WEP дозволений, передавач бере вміст кадру, тобто корисне навантаження, і запускає алгоритм шифрування на ньому. Потім оригінальний вміст кадру замінюється кодованою інформацією. Кадри даних, які були зашифровані, надсилаються з WEP бітом в контрольному полі MAC заголовку. Одержувач кадру з зашифрованими даними пропускає кадр через той же алгоритм шифрування, що і посильна сторона. В результаті виходить оригінальний кадр, який може бути переданий протоколам вищого рівня.

Продуктивність WEP залежить від виду реалізації – апаратної або програмної, а також від конкретного пристрою. Однак найчастіше, особливо при програмній реалізації, відбувається істотне зменшення продуктивності мережі.

WEP використовує потоковий шифр RC4. Це симетричний потоковий шифр, який підтримує різні довжини ключа. Симетричний шифр – це шифр, який використовує один і той же ключ для зашифровування і розшифрування. Він сильно відрізняється від блокових шифрів, які обробляють фіксоване число байт.

Ключ – це якась інформація, яка повинна бути доступна шифрувальній і дешифрувальній стороні.

Стандарт IEEE 802.11 описує використання алгоритму RC4 і ключів в бездротових мережах. Визначено два механізму вибору ключа для зашифровування і розшифрування кадрів.

Перший механізм полягає в установці чотирьох ключів за замовчуванням. Ключі за замовчуванням повинні бути відомі всім станціям бездротової підмережі. Гідність використання ключів за замовчуванням полягає в тому, що якщо станція

отримала ці ключі, вона може спілкуватися таємно з усіма іншими станціями підмережі.

Другий механізм, що забезпечується стандартом IEEE 802.11, дозволяє станції встановити взаємодію з кожною іншою станцією за певними різними джерелами (key mapping). Це, ймовірно, більш захищена форма роботи, тому що менше користувачів знають ключ. Однак, розподіл таких ключів проблематичний, якщо кількість станцій в мережі дуже багато.

WEP заголовок і контрольна сума додаються до зашифрованого тілу кадру. Номер ключа за замовчуванням, який потрібно використовувати для розшифрування кадру міститься в полі номер ключа заголовка кадру разом з ініціалізаційним вектором. Поле “контрольна сума” містить циклічний надлишковий код CRC-32 і призначений для контролю правильності переданого кадру.

Формат тіла кадру при використанні «WEP Ключ» складається з ініціалізації вектора і секретного «WEP ключа». Наприклад, 64 бітний ключ складається з 40-ка бітного «WEP ключа», що зберігається таємно, і 24 бітного ініціалізаційного вектора.

Секретний ключ, з'єднуючись з ініціалізаційним вектором, утворює початкове значення для генератора псевдо-випадкової послідовності (ПСП). На виході генератора утворюється послідовність байтів (ключ), що дорівнює по довжині кількості байтів даних для передачі. Процедура шифрування полягає в підсумовуванні ключа з відкритим текстом, доповненим контрольною сумою. В результаті утворюється повідомлення, що містить зашифровані тексти і ініціалізований вектор.

IEEE 802.11 ідентифікація і з'єднання

Ідентифікація – це процес перевірки посвідчення особи клієнта, що намагається під'єднатися до мережі. З'єднання – це процес з'єднання клієнта з цією точкою доступу до бездротової мережі.

У стандарті 802.11, в дійсності, існує три стани користувача:

– неавторизований і неприєднаний;

– авторизований і неприєднаний;

– авторизований і приєднаний.

IEEE 802.11 визначає два типи ідентифікаційних методів: відкрита система ідентифікації та ідентифікація з розділеним (shared) ключем. Вдале виконання фаз ідентифікації та з'єднання дозволяє вузлу бездротової мережі вдало увійти в бездротову мережу.

При ідентифікації з відкритим ключем весь ідентифікаційний процес проходить відкритим текстом. Це означає, що клієнт може приєднатися до точки доступу з неправильним WEP ключем або взагалі без WEP ключа.

Але, як тільки клієнт спробує послати або прийняти дані, він не зможе цього зробити, тому що для обробки кадрів необхідно знати правильний ключ. При ідентифікації з розділеним ключем в процесі ідентифікації використовуються зашифровані повідомлення. Якщо клієнт не володіє вірним ключем, то він не пройде стадію ідентифікації і не зможе приєднатися до точки доступу.

Вибір між методами ідентифікації проводиться вручну на кожному пристрої, але методи клієнта і сервера повинні збігатися, щоб ідентифікація пройшла успішно. За замовчуванням використовується відкрита ідентифікація.

Весь процес може бути розділений на три фази:

– фаза зондування. Коли клієнт ініціалізується, він спочатку посилає (зондує) запит по всіх каналах. Точки доступу, які «чують» цей запит, посилають станції відповідь на зондуючий запит. Відповідь містить таку інформацію, як SSID, який клієнт зберігає для визначення, яка точка доступу продовжує процес з'єднання;

– фаза ідентифікації. Після того, як клієнт визначить, яка точка доступу продовжує процес з'єднання, він починає процес ідентифікації на основі зондуючої відповіді. Ця фаза може бути виконана як у відкритому режимі, так і в режимі розділеного ключа. Обидві сторони сервер і клієнт повинні бути налаштовані на однаковий режим ідентифікації, інакше ідентифікація не пройде;

– фаза з'єднання. Якщо клієнт вдало пройшов фазу ідентифікації (наприклад, отримав позитивну ідентифікаційну відповідь від точки доступу), він починає

фазу з'єднання. Клієнт посилає запит на з'єднання точки доступу. Точка доступу аналізує інформацію в цьому запиті і якщо вона правильна, точка доступу додає клієнта в свою таблицю з'єднань. Потім вона посилає відповідь клієнту, і фаза з'єднання на цьому завершується.

Схема відкритої ідентифікації з розділеним ключем.

Клієнт посилає ідентифікаційний запит на точку доступу. Точка доступу обробляє цей запит і визначає (ґрунтуючись на власній конфігурації), дозволити або не дозволити клієнту перейти до фази з'єднання. Точка доступу посилає ідентифікаційну відповідь клієнту. Ґрунтуючись на типі відповіді (ідентифікація пройшла чи ні) від точки доступу, клієнт продовжує або припиняє процес з'єднання.

Схема відкритої ідентифікації Ідентифікація з розділеним ключем.

Клієнт посилає ідентифікаційний запит на точку доступу. Точка доступу обробляє цей запит, генерує і посилає зашифрований текст клієнту. Клієнт потім повинен розшифрувати повідомлення за допомогою секретного WEP ключа і послати пакет назад на точку доступу. Точка доступу визначає, чи вдалося клієнту вірно розшифрувати пакет. Ґрунтуючись на цьому тесті, точка доступу посилає позитивну або негативну ідентифікаційну відповідь клієнту, який визначає, чи дозволено клієнту продовжувати процес з'єднання.

Ідентифікація з розділеним ключем. Фаза з'єднання (Стандарт бездротових мереж 802.11) забезпечує досить високий рівень безпеки та надійності, при цьому, майже не знижуючи швидкодії мережі, що забезпечує широке поширення бездротових мереж по всьому світу. Однак цей стандарт не позбавлений ряду суттєвих недоліків, і зараз вже ведеться розробка стандарту безпеки другого покоління.

Один із способів вирішення проблеми безпеки – використання спрямованих антен, зокрема, адаптивних фазованих решіток, які виробники планують реалізувати в складі інтерфейсних чіпів. Але ця технологія не скасовує передбаченої в ранніх специфікаціях шифрування даних.

2 ПОСЛУГИ WI-FI В АЕРОПОРТАХ ТА ПРОБЛЕМА ПЕРЕШКОД

2.1 Специфіка аеропортів

Мобільний зв'язок в аеропортах потрібен, щоб не загубитися в численних людських потоках в терміналах, мати можливість поговорити з рідними і близькими або обговорити з колегами справи по роботі, а також читати пости в інтернеті, викладати відео в соцмережах, дивитися фільми, качати фотографії, слухати музику і радіо, грати в он-лайн ігри в години чекання рейсу.

Характерною особливістю найбільших аеропортів є те, що мобільний трафік тут постійно росте, розвивається, а значить, це питання знаходиться в зоні нашої уваги. Крім того, такі аеропорти є вузловими, концентрує в собі трафік пасажиропотоку. Перебуваючи на достатньому віддаленні один від одного, вони формують міжнародне і внутрішнє авіатранспортне повідомлення регіонів нашої країни.

Вузлові аеропорти – це особливі аеропорти, які виконують стикування і пересадку транзитних пасажирів між авіарейсами з інших аеропортів. Ці транспортні вузли отримали в галузі громадського транспорту ще одне, більш коротку назву - хаби. Розклад вильотів і прильотів в хабах, як правило, ретельно підібрано авіакомпаніями з метою мінімізації часу очікування рейсів пасажирами. Одним з таких хабів є Міжнародний аеропорт «Бориспіль» (рисунок 2.1).

Варто відзначити, що трафік пасажиропотоку формується не стільки аеропортами, вони лише обслуговують і підтримують його, скільки авіакомпаніями. Питання «приземлення» пасажирського трафіку в тому чи іншому аеропорту – це завжди непростий діалог аеропортів і авіакомпаній, так як «заманити» авіаперевізників в той чи інший аеропорт буває дуже не просто і необхідно домовлятися про взаємні преференції. Саме авіакомпанії формують пасажиропотоки, і від них залежить наповнюваність аеропортів пасажирами.

Рисунок 2.1 – Міжнародний аеропорт «Бориспіль»

Останнім часом у нас в країні став розвиватися децентралізований принцип розподілу навантаження на маршрутних мережах регіональних аеропортів. Шляхом введення різних регуляторних заходів щодо отримання субсидій авіаперевезень ситуація в сегменті регіональних поїздок пасажирів видозмінилася. Трафік пасажиропотоку став перерозподілятися і закріплюватися в менш великих регіональних аеропортах, що тільки сприяє впевненому розвитку цього виду громадського транспорту в нашій країні в цілому. За останні десять років транспортною галуззю була проведена велика робота з модернізації та вдосконалення інфраструктури аеропортів. На всю зростає регіональна маршрутна мережа, створюються нові напрямки, з'являються сучасні пасажирські термінали, розширюються ємності матеріально-технічної бази, збільшується інтенсивність польотів, що тільки відкриває нові горизонти для розвитку українських аеропортів.

Особливість проведеної останнім часом модернізації вузловими аеропортами полягає в тому, що пасажирські термінали в них стали розростатися і об'єднуватися в єдині аеровокзальні комплекси. Робиться це для того, щоб в

ключових аеропортах розвивалася повноцінна інфраструктура хаба, і пасажиропотік безперешкодно циркулював між терміналами при пересадці транзитних пасажирів на стикувальних рейсах. Очікується, що так економитимуться ресурси і час між рейсами авіакомпаній, коли їх щільність зросте подібно найбільшим хабам світового рівня.

Практично у всіх ключових аеропортах країни, слідом за зростанням пасажиропотоку почався зріст трафіка і на наших мобільних мережах, як від домашніх, так і від роумінгових абонентів. І що особливо характерно – істотно збільшився трафік мобільної передачі даних. Пасажиропотік в хабах створює досить велике навантаження на мобільну мережу. Тому необхідно реагувати на ці зміни в транспортній галузі, а значить встигати модернізувати і посилювати покриття в вузлових аеропортах для забезпечення пасажирів технологіями зв'язку 4G / 3G / 2G, а особливо технологією WI-FI. Так тема будівництва мобільних мереж і збільшення пасажиропотоків в аеропортах стала дуже важливою в наш час.

2.2 Wi-Fi в аеропортах

Бездротовий зв’язок, який найчастіше зустрічається через використання бездротової мережі (Wi-Fi) або мобільного телефону, став звичайним інструментом для повсякденного життя. Однак бездротовий зв’язок піддається радіочастотним (ВЧ) перешкодам. Зростаюче використання та важливість бездротових мереж не лише як пасажирських зручностей, але і як невід'ємної частини операцій аеропорту, робить його надійність та ефективність важливими для сучасних операцій в аеропорту. Безпека також є критичною, оскільки бездротовий зв'язок став потенційним вектором атаки – способом порушити роботу аеропорту. Таким чином, надійна захищена мережа, яка добре керується та модернізується відповідно до збільшення запитів та заявок – це головне питання для керівників аеропортів.

У рамках дослідження зібрана інформація з аеропортів щодо досвіду роботи з Wi-Fi, зокрема про проблеми з перешкодами, потужністю та продуктивністю. Які рішення були випробувані та чи були вони успішними. Включаючи процеси, методи, процедури та застосовні інструменти, які можна використовувати для виявлення причини перешкод та визначення їх рішення для пом’якшення проблеми. У цій главі також містяться рекомендації щодо альтернативних методів та ресурсів, до яких можна отримати доступ, коли проблема перевищує звичайні зусилля інженера.

Найбільш підходящі рішення для будь-якого аеропорту залежатимуть від цілей аеропорту щодо Wi-Fi сервісу та обсягу фінансування, доступного для усунення проблем та розширення потужностей.

Вимоги до рівня обслуговування Wi-Fi швидко перейшли до того, що послуга повинна відповідати очікуванням багатьох мандрівників, що бездротові мережі мають надійність та продуктивність, близькі до рівня дротової мережі. Сьогодні пасажири очікують сполучення скрізь, при цьому рівень обслуговування схожий на дротовий зв’язок або дорівнює бездротовому сервісу, яким вони користуються у своїх будинках. Оскільки аеропорти та їх орендарі інтегрують бездротове підключення у свої операції, навіть більш високі рівні обслуговування необхідні та виправдані.

Очікування від послуг Wi-Fi значно відрізняються як серед керівників аеропортів, так і подорожуючих. Деякі керівники аеропортів та мандрівники відносяться до мережі WiFi як частини необхідної інфраструктури. Вони очікують, що Wi-Fi буде працювати добре, як і вони очікують, що освітлення буде хорошим, а туалети будуть чистими та справними. З іншого боку, деякі менеджери аеропортів надають меншу важливість бездротовій мережі їх аеропорту, ніж інші питання управління, що вимагають уваги.

Мандрівники з великими сподіваннями на послугу Wi-Fi будуть оминати аеропорт, який не відповідає їхнім очікуванням на безперебійне обслуговування зв'язку. Крім того, оскільки менеджери аеропортів та мандрівники мають обмежені можливості домовитися та узгодити свої очікування, аеропорти, які не

забезпечують високоякісний Wi-Fi, можуть виявити, що відсоток мандрівників може вибрати інші аеропорти для вильоту або сполучення рейсів. Бізнес-мандрівники, зокрема, потребують надійного підключення до Інтернету, щоб виконувати роботу під час очікування рейсів, особливо, коли рейси затримуються або скасовуються, порушуючи бізнес-графіки.

2.3 Домовленості щодо управління мережею

Не дивно, що існують різноманітні механізми управління мережею. Деякі аеропорти управляють власним Wi-Fi та працюють безпосередньо з провайдерами стільникової мережі для забезпечення мобільного зв'язку в терміналі. Інші укладають контракти як на керування мережею Wi-Fi, так і на стільникову мережу, делегуючи стосунки з операторами стільникового зв’язку своїй обраній компанії з управління бездротовою мережею.

Після вибору компанії деякі аеропорти розглядають свою відповідальність за управління мережею як закінчену до наступних переговорів про контракти. Інші аеропорти виявили, що вони повинні все більше брати участь у управлінні мережею та мати тісні робочі стосунки зі своїм обраним постачальником. Однак у кількох найбільших відвідуваних аеропортах керівники аеропортів зазначили, що вони не мають рівня знань, необхідного для належного нагляду за роботою свого постачальника управління мережею. Ці аеропорти уклали контракти з іншими постачальником, який має поглиблені знання в галузі радіочастот і мереж, щоб забезпечити вимірювання та незалежний вклад функціонування мережі та наданий рівень обслуговування.

У багатьох аеропортах працюють паралельні служби. Безкоштовний сервіс пропонує обмежену швидкість передачі даних і часто вимагає від користувачів прослуховування рекламних роликів, перш ніж їм надавати доступ до Інтернету. Паралельно платна послуга надається за певну плату, оплачується як за примірник, так і за підписку. У мандрівників є вибір. Вони можуть отримати

доступ до Інтернету через свої мобільні пристрої та легко поділитися цим зв’язком із іншими пристроями.

2.4 Причини перешкод Wi-Fi та порушення роботи мережі

Що вважається радіоперешкодою? Це не так явно, як можна було б уявити. Для цього дослідження деградація продуктивності або порушення спілкування вважалися перешкодою. Порушення спілкування легко зрозуміти. Користувачі не можуть підключитися до мережі, але вони повинні мати можливість цього. Щось блокує або порушує спілкування. Якщо пакети втрачені через іншого передавача, це перешкода. Якщо зв’язок відбувається повільніше, ніж це має бути, коли інший пристрій передає, це також вважається перешкодою.

Існує різниця між перешкодами та перешкодами, що спричиняють проблеми. Деякі аеропорти виконують більше своїх функціональних обов’язків по мережі, і їм потрібні ці функції для надійної роботи. Інші конкурують з іншими аеропортами за пасажирів, і якість подорожей пасажирів надзвичайно важлива. Існує багато факторів, які впливають на очікування аеропорту щодо зв'язку.

Навмисне втручання.

Навмисне створення завад та втручання вже стало досить поширеним. Це зріст ризиків безпеки, які необхідно враховувати. У ході дослідження цього проекту один з аеропортів повідомив про те що іноді люди приходять в аеропорт і встановлюють гарячу точку, використовуючи сервісний набір ідентифікатора аеропорту (SSID) у спробі отримати інформацію про вхід та паролі людей. Шахрайські гарячі точки, можуть працювати на більш високій вихідній потужності, ніж дозволено в неліцензованому спектрі 2,4 ГГц, і при цьому викликати перешкоди. Керівники аеропортів повідомили, що їх оператори мережі мають методи, які дозволяють їм використовувати мережу для придушення цих точок шахрайства при їх виявленні. Імовірно, оскільки мережі регулярно відключають живлення, щоб уникнути перешкод, вони також можуть посилити їх

владу, щоб створити перешкоди для шахрайської точки доступу. Це доказує той факт, що люди з поганими мотивами можуть створювати втручання.

Оскільки бездротовий зв'язок стає все більш інтегрованим в роботу аеропорту, він також повинен стати частиною планування безпеки в аеропорту. Особливо це стосується камер безпеки та доступу пристроїв управління підключених бездротово, тому що кібератака може придушити бездротовий зв'язок. і тому обійти систему безпеки. Розмірковуючи над питаннями безпеки такого типу, типово думати про виявлення і запобігання таких проблем, та пом'якшення наслідків. Якщо буде створено навмисне втручання, як це буде виявлено і куди буде повідомлено? Що можна зробити, щоб запобігти навмисному втручанню? Якщо запобігти втручанню не вдається, що можна зробити, щоб пом’якшити її вплив? Пошук та реалізація відповідей на ці питання набуває все більшого значення, оскільки використання бездротового зв'язку зростає та розвивається, стає все більш глибоко інтегрована в інфраструктуру.

Суміжні перешкоди каналу.

Радіочастотні пристрої не мають ідеальних меж частоти. Поки вони призначені вкласти якомога більше своєї енергії в канал, який вони використовують, є вплив на пристрої, що працюють на сусідніх каналах. Для передавача Wi-Fi частина його енергії буде переходити в сусідні канали, що додаватиме шум цим каналам та знижує їх здатність до комунікаційного обміну між пристроями, до яких вони мають намір підключитися. При отриманні сигналу, фільтрації фронтальні радіочастотні схеми дозволяють надходити деяку енергію від передачі сусіднього каналу впливаючи на приймач Wi-Fi. На рисунку 2.2 показаний спосіб передачі енергії з сусіднього каналу Sion, який може впливати на Wi-Fi-приймач і часто є домінуючим впливом на продуктивність Wi-Fi-пристроїв

Коли два пристрої WiFi близькі і між ними хороша сила сигналу, з'являється операційний запас і вплив суміжних канальних передач буде набагато меншим, можливо незначним. Найгірша проблема виникає, коли пристрій Wi-Fi намагається спілкуватися на відстані, приводячи до слабкого призначеного

сигналу, але передача сусіднього каналу близька, внаслідок чого виникає перелив енергії значно вищий, часом досить високий, щоб повністю запобігти комунікації.

Як видно на рисунку 2.2, є два вкладники до сусідніх канальних перешкод. І тому й іншому необхідно, щоб пристрої Wi-Fi працювали надійніше. Передавачі Wi-Fi повинні зменшити значну кількість енергії, яку вони перекидають на інші канали. Однак одного цього буде недостатньо. Необхідно також, щоб приймачі Wi-Fi мали кращі фільтри, що забезпечує їм кращу стійкість суміжних каналів передач.

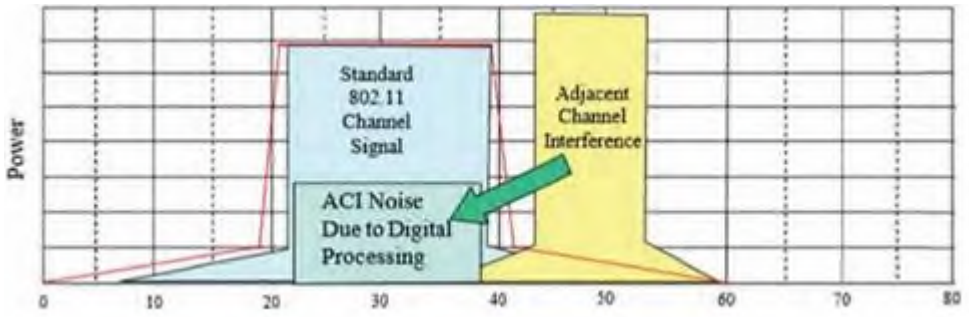


Рисунок 2.2 – Ефект перешкод сусідніх каналів (ACI)

Інші джерела втручання.

Нове джерело перешкод багато в чому створюється потребою підтримувати дві мережі у збільшеній кількості смуг частот. Як результат, антени для Wi-Fi та стільникових мереж часто розміщуються близько один від одного, а часом вони ділять ту саму антену в загальній розподіленій антенній системі. Сильні радіочастотні сигнали можуть створювати продукти інтермодуляціїі і різноманітні пов'язані з цим проблеми.

Ще один клас проблеми перешкод створюється завдяки змінам технології. У деяких випадках випадкові коливання, зменшені для перешкод, фактично призводять до більшої кількості перешкод. Приклад зміни технологій, що викликають перешкоди, є IEEE 802.11b. Новіші версії IEEE 802.11 відійшли від прямої послідовності модуляції розповсюдженого спектру до ортогональної модуляція частотного поділу (OFDM). Однак підтримка старшої IEEE802.11b був

необхідний для зворотної сумісності. У цьому дослідженні все ще не рідкість знайти пристрої IEEE 802.11b, які працюють, але коли вони це роблять, вони часто стають джерелами перешкод оскільки вони несумісні.

3 МЕРЕЖЕВІ СИМУЛЯТОРИ

3.1 Опис мережевого симулятора

Дана робота пов'язана з імітаційним моделюванням.

Імітаційне моделювання – представлення логіко-математичної моделі досліджуваного об'єкта у вигляді програмного комплексу для комп'ютера. Для цього існують безліч мережевих симуляторів. Перерахуємо кілька симуляторів і виберемо відповідний для даної роботи.

Мережевий симулятор – це програмне забезпечення, яке робить емуляцію поведінки комп'ютерної мережі. У мережевих симуляторах, комп'ютерна мережа, як правило, моделюється за допомогою пристроїв, зв'язків, додатків. Симулятор підтримує найпопулярніші протоколи і мережі, які використовуються сьогодні, наприклад, WLAN, WiMAX, TCP.

У більшості комерційних симуляторів є графічний інтерфейс, в той час як деякі мережеві симулятори мають інтерфейс у вигляді командного рядка. Конфігурація мережевої моделі описується станом мережі (вузли, маршрутизатори, комутатори) і подій (передача даних, помилки). Важливим підсумком моделювання є файли трасування. У файлах трасування враховується кожен пакет, кожна подія, що сталася під час симуляції і використовується для аналізу. Мережеві симулятори також можуть надати інші інструменти для полегшення візуального аналізу.

Мережеві симулятори служать найрізноманітнішим потребам. У порівнянні з тимчасовими, комерційними та іншими витратами на налаштування стендів, що містять кілька комп'ютерів, маршрутизаторів і каналів передачі даних, мережеві симулятори швидкі і недорогі. Вони дозволяють інженерам і дослідникам перевірити характеристики, які важко або дорого відтворювати за допомогою реального обладнання – наприклад, імітувати сценарій з декількома вузлами або експериментувати з новим протоколом в мережі. Мережеві симулятори особливо корисні при дослідженні та тестуванні нових мережевих протоколів, або зміні

існуючих протоколів передачі даних. Типовий мережевий симулятор охоплює широкий спектр мережевих технологій і може допомогти користувачам створювати складні мережі з основних будівельних блоків, таких як різні вузли і з'єднання. За допомогою симуляторів можна проектувати ієрархічні мережі, використовуючи різні типи вузлів, таких як комп'ютери, концентратори, мости, маршрутизатори, комутатори, з'єднання та інші.

Крім розробки нових протоколів або нової маршрутизації, користувачем за допомогою симулятора можуть бути змодельовані і проаналізовані різні типи WAN технологій, таких як TCP, ATM, IP та інші, а також (LAN) технології, такі як Ethernet, TokenRingi та інші.

Мережевих симуляторів безліч: від дуже простих до дуже складних. Мінімально мережевий симулятор повинен дозволяти користувачеві створювати топологію мережі, вузлів в мережі, зв'язку між цими вузлами і трафік між вузлами. Більш складні системи можуть дозволити користувачеві вказати всі протоколи, які використовуються для обробки трафіку в мережі. Графічні додатки дозволяють користувачам легко отримати результати моделювання. Симулятори, що використовують інтерфейс командної строки, забезпечують менш інтуїтивно зрозумілий інтерфейс, але більш професійне налаштування.

3.2 Приклади мережевих симуляторів

Існує багато мережевих симуляторів безкоштовних і платних, з відкритим та закритим кодом. Ось деякі приклади найпопулярніших мережевих симуляторів:

– Boson NetSim;

– NetSim;

– OPNET;

– OMNet++;

3.3 BosonNetSim

Симулятор BosonNetSim (рисунок 3.1), який зовсім недавно оновився до 9-ї версії випускається тільки під Windows, ціна коливається від 179 $ за CCNA (Cisco Certified Network Associate) для спеціалістів Cisco і до 349 $ за CCNP (Cisco Certified Network Professional) для професіоналів Cisco. Являє собою якийсь збірник лабораторних робіт, згрупованих за темами. Інтерфейс складається з декількох секцій: опис завдання, карта мережі, в лівій частині знаходиться список всіх лабораторних робіт. Закінчивши роботу, можна перевірити результат і дізнатися, чи все було зроблено. Є можливість створення власних топологій, з деякими обмеженнями.

Основні властивості BosonNetSim:

– підтримує 42 маршрутизатора, 6 комутаторів і 3 інших пристрої;

– симулює мережевий трафік за допомогою технології віртуальних пакетів;

– надає два різні стилі перегляду: режим Telnet та режим підключення до консолі;

– підтримує до 200 пристроїв на одній топології;

– створюйте свої власні лабораторії;

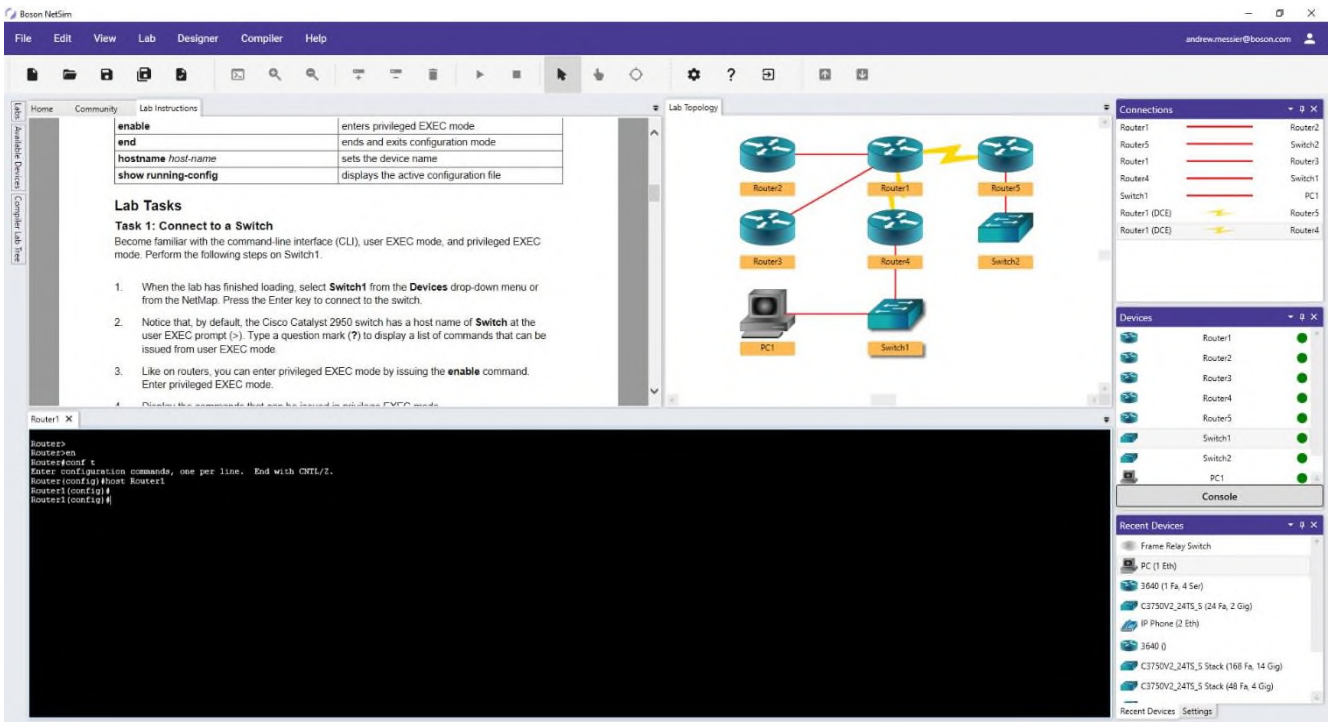


Рисунок 3.1 – Інтерфейс симулятору BosonNetSim

3.4 NetSim

NetSim є популярним мережевим симулятором, який використовується для мережевого проектування і планування. NetSim підтримує різні технології, такі як бездротові сенсорні мережі, бездротові локальні мережі, WiMAX, TCP, IPi та інші.

NetSim (рисунок 3.2) є стохастичним дискретно-подієвим симулятором. Він був розроблений Tetcosi Індійським інститутом науки, в червні 2002 року. NetSim надає показники продуктивності мережі на різних рівнях абстракції, таких як мережі, підмережі, вузли зв'язку, з докладним трасуванням пакетів і подій. NetSim надає готові різні мережеві технології і протоколи, включаючи Manet, Wi-Fi, Wi-Max, IP, MPLS, WSN, VoIP та інші. Наявність готових рішень може допомогти уникнути витрат часу на процес програмування, налаштування і конфігурації симулятора.

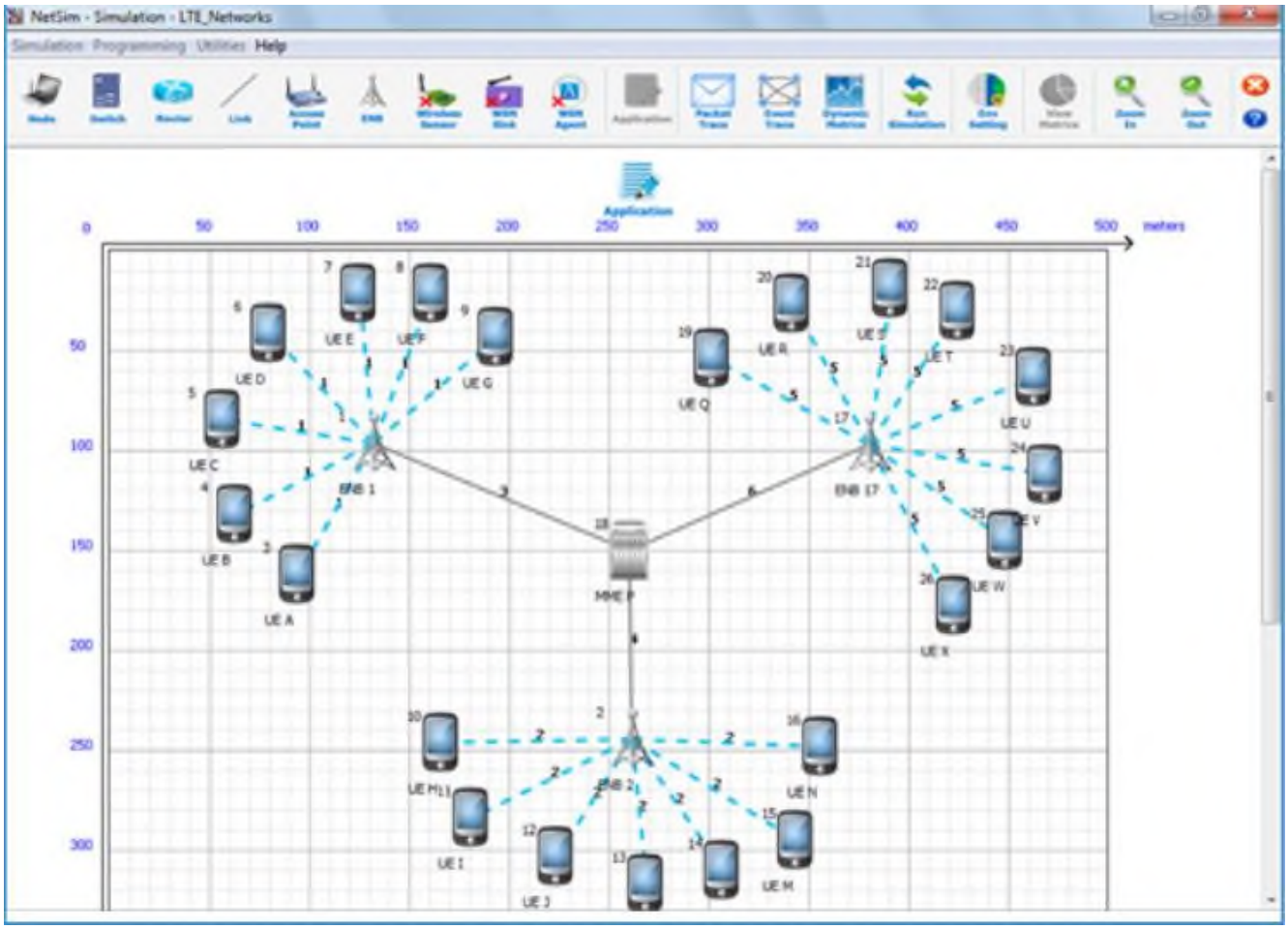


Рисунок 3.2 – Інтерфейс симулятору NetSim

3.5 OPNET

OPNET пропонує користувачам графічне середовище для створення, виконання та аналізу покрокового моделювання мереж зв'язку. Це зручне програмне забезпечення може бути використане для великого ряду завдань, наприклад, типове створення і перевірка протоколу зв'язку, аналіз взаємодій протоколу, оптимізація та планування мережі. Можливо зробити перевірку правильності аналітичних моделей і опису протоколів. В рамках, так званого, редактора проекту можуть бути створені палітри мережевих об'єктів, яким користувач може присвоїти різні форми з'єднання вузлів і зв'язку.

Автоматизоване створення мережевої топології – кільця, зірки, також підтримується і резервується утилітами для імпортованих мережевих топологій в різних форматах. Випадковий трафік може бути автоматично згенерований з алгоритмів, зазначених користувачем, а також імпортований з вхідних в стандартну комплектацію пакету форматів реальних трафіків ліній. Результати моделювання можуть бути проаналізовані, а графи і анімація трафіку будуть згенеровано автоматично.

Одним з плюсів створення моделі мережі за допомогою програмного забезпечення є те, що рівень гнучкості, що забезпечується ядром моделювання той же, але об'єктна побудова середовища дозволяє користувачеві набагато швидше робити розробку, удосконалення та виробляти моделі для багаторазового використання.

Є кілька середовищ редактора – по одній для кожного типу об'єкта. Організація об'єктів – ієрархічна, мережні об'єкти (моделі) пов'язані набором вузлів і об'єктів зв'язку, в той час як об'єкти вузла пов'язані набором модулів, типу модулів черговості, модулів процесора, передавачів і приймачів. Версія програмного забезпечення для моделювання радіоканалу містить моделі антени радіопередавача, антени приймача, об'єктів вузла що зміщуються (включаючи супутники).

Логіку поведінки процесора і модулів черговості визначає модель процесу, яку користувач може створювати і змінювати в межах редактора процесу. У редакторі процесу користувач може визначити модель процесу через комбінацію алгоритму роботи кінцевого автомата (finite-statemachine – FSM) і операторів мови програмування C / C ++.

Виклик події моделі процесу протягом моделювання управляється порушенням переривання, а кожне переривання відповідає події, яка повинна бути оброблено моделлю процесу.

Основа зв'язку між процесами – структура даних, яка називається пакетом. Можуть бути задані формати пакета, які можуть містити такі стандартні типи даних, як цілі числа, числа з плаваючою комою і покажчики на пакети. Структура даних, що викликає інформацію з контролю за інтерфейсом (interface control information – ICI), може бути розділена між двома подіями моделей процесу – це ще один механізм для міжпроцесорного зв'язку, що дуже зручно для команд моделювання і відповідає архітектурі багаторівневого протоколу. Процес також може динамічно породжувати дочірні процеси, які спростять функціональний опис таких систем, як сервери.

Кілька основних моделей процесу входять в базову комплектацію пакета, моделюючи популярні протоколи роботи з мережами та алгоритми, на зразок протоколу шлюзу кордону (bordergatewayprotocol – BGP), протоколу контролю передачі (TCP/IP), ретрансляції кадрів (framerelay), Ethernet, асинхронного режиму передачі (asynchronoustransfermode – ATM), і WFQ (weightedfairqueuing). Базові моделі корисні для швидкого розвитку складних імітаційних моделей загальних архітектур мережі, а також для навчання, щоб дати точний функціональний опис протоколу студентам.

Існує можливість супроводу коментарями і графікою (з підтримкою гіпертексту) моделей мережі, вузла або процесу (рисунок 3.3).

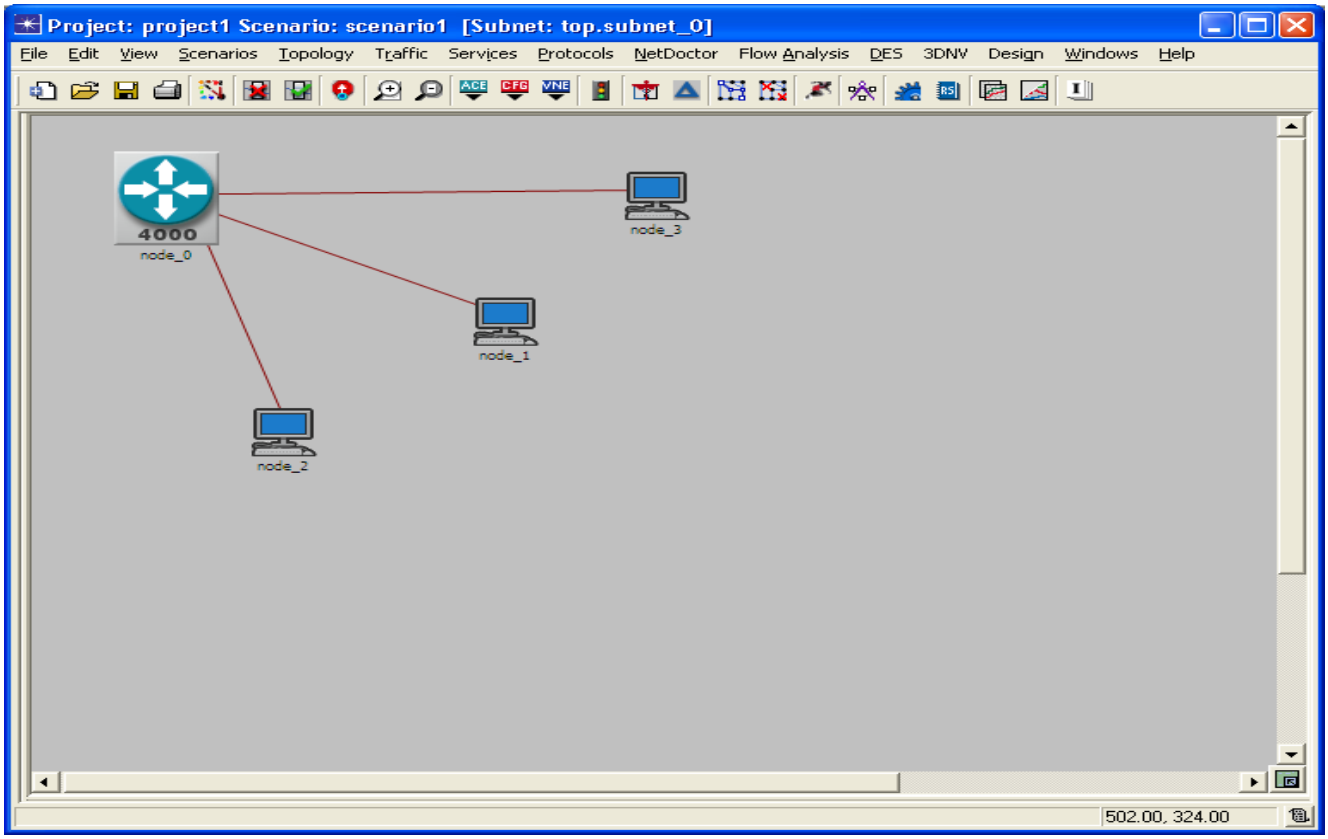


Рисунок 3.3 – Інтерфейс симулятору OPNET

3.6 OMNeT ++

OMNeT ++ являє собою систему моделювання на основі дискретних подій. Система моделювання в основному підтримує стандартні провідні та безпровідні мережі IP комунікацій, але існують також деякі розширення для бездротових сенсорних мереж (БСМ). OMNeT ++ є відомою системою, що розширюється і активно підтримується спільнотою своїх користувачів, які також створюють розширення для моделювання БСМ.

OMNeT ++ використовує мову C ++ для імітаційних моделей (рисунок 3.4). Імітаційні моделі в сукупності з мовою високого рівня NED збираються у великі компоненти і являють собою великі системи. Симулятор має графічні інструменти для створення моделей і оцінки результатів в режимі реального часу.

OMNeT ++ здатний запускати моделі TinyOS з допомогою програми NesCT, яке конвертує вихідний код TinyOS в симуляцію, сумісну з кодом C ++. Обмін симуляційним кодом NesCT між сенсорними платформами можливий, але тільки

в обмеженому вигляді, оскільки протокол і апаратна реалізація в симуляторі максимально спрощена, але не все обладнання підтримується. Симулятор добре масштабується для дуже великих мережевих топологій, де можливості обмежуються лише обсягом пам'яті комп'ютера або робочої станції. OMNet ++ не може моделювати операційну систему прикладного рівня з затримками часу виконання. Затримки для нижніх шарів, наприклад, MAC і бездротового каналу, визначені у договорі. Без відповідних імітаційних моделей і розширень (framework), симулятору не вистачає протоколів і належної якості моделювання сенсорних мереж, так як основна підтримка орієнтована головним чином в бік IP мереж.

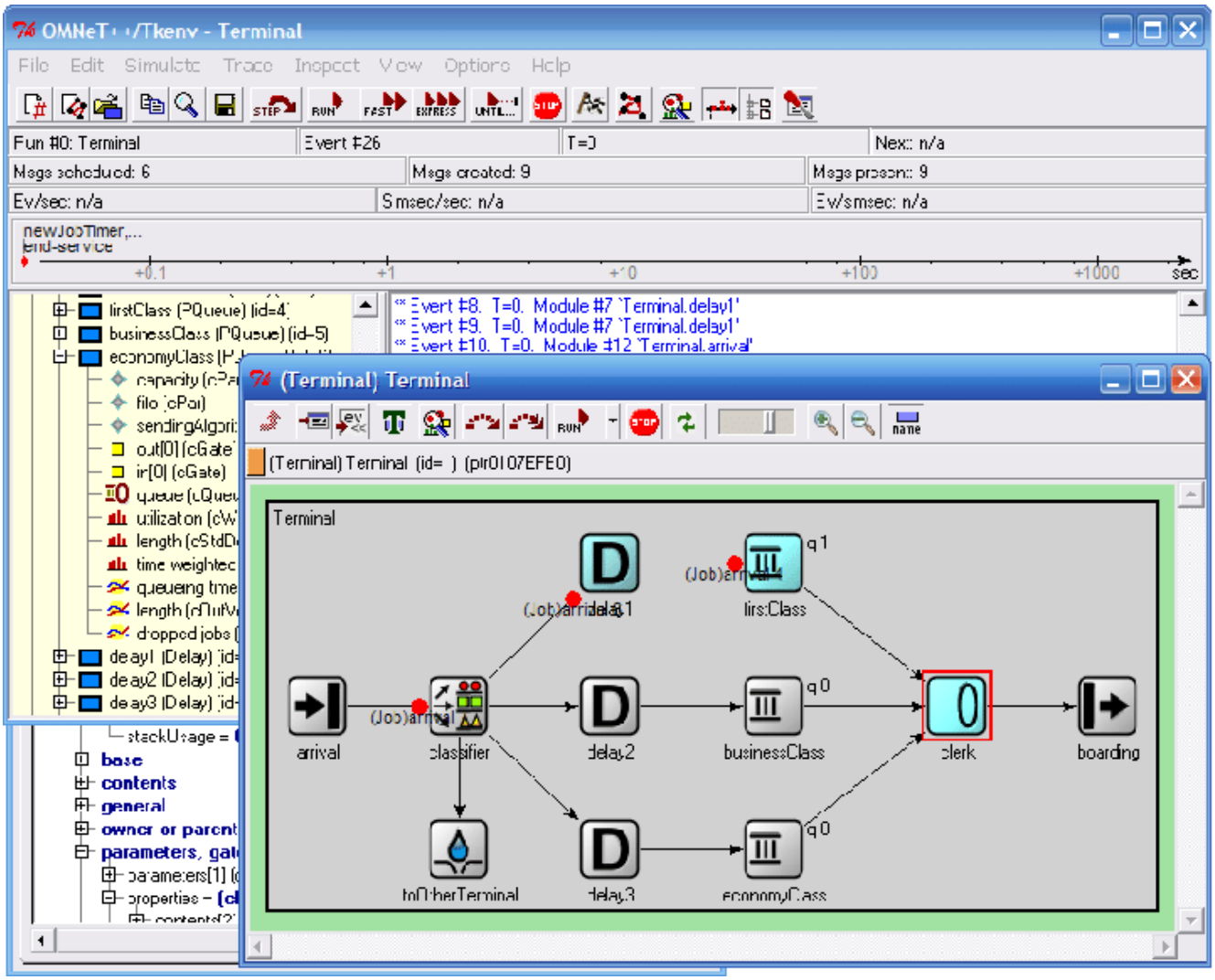


Рисунок 3.4 – Інтерфейс симулятору OMNet ++

Приділимо трохи уваги проектам, який є розвитком OMNeT ++ – Castalia. Castalia є середовищем моделювання для сенсорних мереж і побудований на платформі OMNeT ++. Castalia є модульною і розширюється. До її сильних сторін належить точність моделювання бездротового каналу і радіосигналів, включаючи MAC.

4 РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ МЕРЕЖІ ТА ЇХ АНАЛІЗ

4.1 Опис моделі

У пункті 4 описується спосіб проектування експерименту та його аналіз. Починається з постановки проблеми у цій тезі, включаючи змінні, якими маніпулюють, та ті, які зібрані для вимірювання наслідків атаки. Далі в розділі розроблені макети для кожного з показаних сценарієв, включаючи опис кожного з них.

Для моделювання був обраний мережевий симулятор OPNET. Він найкраще підходить для модуляції завдяки зручному інтерфейсу та своїм можливостям в аналізі створених моделей.

4.2 Модельна характеристика та система збору даних

Для цього дослідження вхідними змінними є: потужність передачі перешкод, взаємодія між пакетами швидкість і відстань між заклиначем і вузлами.

Потужність передачі перешкод буде розглянута в трьох дискретних значеннях [0,032 Вт, 0,066 Вт, 0,1 Вт]. 0,032 Вт – найпоширеніша потужність передачі, що використовується в поточних точках доступу 802,11 g; і хоча 0,066 Вт не використовується широко, це середня точка між найбільш використовуваною передачею потужності і максимально дозволеної потужністю передачі; і 0,1 Вт – максимальна потужність прийнята стандартом IEEE для WLAN.

Часи взаємозв'язку пакетів також будуть враховані в 3 дискретних безперервних значеннях: [0,01сек., 0,05сек, 0,1 сек.]

У першому сценарії відстань між перешкодами і приймачем буде постійно змінюватися через використання мобільного глушника всередині моделі. У решті сценаріїв відстань буде іншою.

Підсумками першого сценарію будуть графіки отриманої енергії, пропускної здатності та ймовірності частоти помилок бітів у часі. Для другого та третього сценаріїв результатами будуть графіки пропускної здатності, час, коли передавальні схеми точки доступу зайняті, і час коли приймаючі схеми точки доступу зайняті. Для четвертого сценарію результатом є пропускна здатність у вузлах, які знаходяться в межах і поза діапазоном передачі перешкод. Для п'ятого сценарію результатом є графік, який порівнює сукупну пропускну здатність в мережі, коли відсутній недоброзичливий вузол і коли він є.

4.2.1 Сценарій 1

Сценарій 1 імітує найпростішу з атак заклинення. Ця атака складається з єдиного передавач (tx), що надсилає дійсний трафік на приймач (rx), обидва вони без будь-якого протоколу MAC, і один заклик, який постійно випромінює випадкові недійсні пакети, намагаючись викликати зіткнення з дійсними пакетами для збільшення ймовірності помилок у них.

Установка моделювання така: модель має розмір 75 × 75 метрів, що є середнім покриттям, наданим AP використовуючи стандарт 802.11g. Зелена лінія на рисунку 4.1 показує траєкторію, за якою слідує мобільна заглушка.

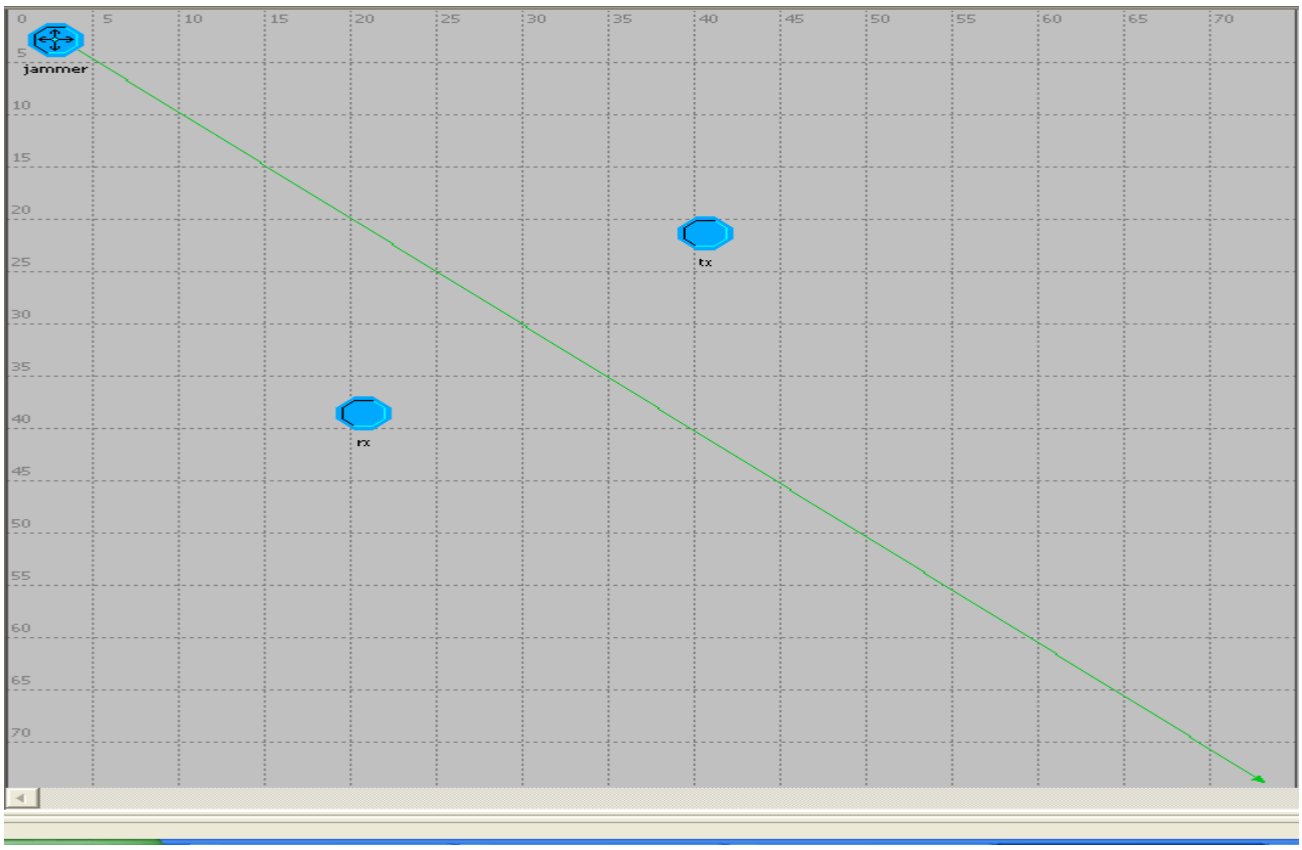


Рисунок 4.1 – Сценарій 1 (макет)

4.2.1.1 Характеристики глушилки

На рисунку 4.2 показані характеристики глушилки (джамера), він створений за допомогою моделі mrt_jam_ref . Цей мобільний джамер буде слідувати траєкторії, визначеній ' trayecto1_real ' (зелена лінія на рисунку 4.1),і з потужністю передачі 0,05 Вт.

На рисунку 4.3 показано, що внутрішня структура цього джамера складається з трьох внутрішніх модулів: перший – генератор трафіку, який підключений до радіомодулятора, який підключений до антени.

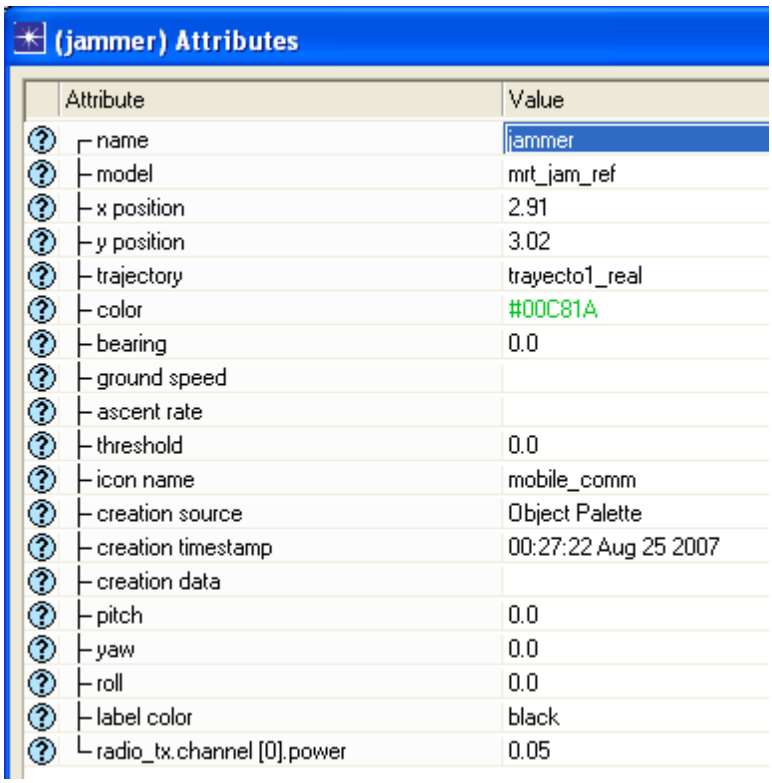


Рисунок 4.2 – Характеристики глушилки

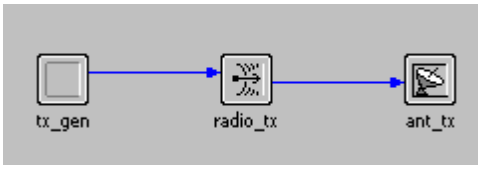


Рисунок 4.3 – Внутрішні модулі глушилки

У таблиці 4.1 показано, що джаммер посилає пакети для заклинювання з постійною довжиною 1024 біт та постійною швидкістю 1 пакет в секунду. Коли ці пакети надходять до модулятору вони перетворюються у відповідну форму для передачі антеною зі швидкістю 1024 біт/с потужністю 0,05 Вт. Бездротовий модулятор також вказує на модуляційну схему 'jammod' і всі процеси, які застосовуватимуться до цього пакету.

Таблиця 4.1 – Характеристики модулів глушилки

Характеристика генератору трафіка	Характеристика радіомодулятора	Характеристика антени
name: tx_gen process model: simple_jammer_source icon name: processor Packet Interarrival Time: constant (1.0) Packet Size: constant (1024) Start Time: 10.0 Stop Time: Infinity	name: radio_tx channel: (...) rows: 1 row 0 data rate (bps): 1,024 packet formats: all formatted, unformatted bandwidth (kHz): 10 min frequency (MHz): 30 spreading code: disabled power (W): 0.05 bit capacity (bits): infinity pk capacity (pks): 1,000 modulation: jammod rxgroup model: dra_rxgroup txdel model: dra_txdel closure model: dra_closure chanmatch model: dra_chanmatch tagain model: dra_tagain propdel model: dra_propdel icon name: ra_tx	name: ant_tx pattern: isotropic pointing ref. phi: 0.0 pointing ref. theta: 180 target latitude: 0.0 target longitude: 0.0 target altitude: 0.0 icon name: antenna

4.2.1.2 Характеристики передавача

Передавач (рисунок 4.4) складається з таких самих трьох модулів, що і у глушилки з точно таким же потоком трафіку, але з деякими різними характеристиками.

Передавач створюється за допомогою модуля 'simple_source', включеного в бібліотеки OPNET. Джерело трафіку створює пакети з часом взаємодії 1 пакет в секунду і постійною довжиною 1024 біт. Радіомодулятор використовує схему модуляції 'bpsk' для модулювання модуля сигналу (bpsk означає Binary Phase Shift Keying). Лише трафік з такою модуляцією буде вважатися дійсним трафіком.

Всередині джамера OPNET використовується спеціальний модуль під назвою simple_jammer_source , який генерує пакети з випадковими бітами і використовує модуль simple_source для генерації дійсного трафіку. Крім того, на боці джамера OPNET використовує спеціальний метод модуляції, який називається "jammod", що змушує OPNET інтерпретувати весь трафік з таким видом модуляції як перешкоди. Всі характеристики модулів передавача показані у таблиці 4.2.

Антена має точно такі ж характеристики, як і та, що використовується в глушилці.

Таблиця 4.2 – Характеристики модулів передавача

Характеристики генератора трафіку	Характеристики радіомодулятору
name: tx_gen process model: simple_source icon name: processor Packet Format: NONE Packet Interarrival Time: constant (1.0) Packet Size: constant (1024) Start Time: 10.0 Stop Time: Infinity	Attribute / Value name: radio_tx channel: (...) rows: 1 row 0 data rate (bps): 1,024 packet formats: all formatted, unformatted bandwidth (kHz): 10 min frequency (MHz): 30 spreading code: disabled power (W): 0.032 bit capacity (bits): infinity pk capacity (pks): 1,000 modulation: bpsk rxgroup model: dra_rxgroup txdel model: dra_txdel closure model: dra_closure chanmatch model: dra_chanmatch tagain model: dra_tagain propdel model: dra_propdel icon name: ra_tx

name	tx
model	mrt_tx_ref
x position	40.7
y position	21.5
threshold	0.0
icon name	fixed_comm
creation source	Object Palette
creation timestamp	00:27:25 Aug 25 2007
creation data	
label color	black

Рисунок 4.4 – Характеристики передавача

4.2.1.3 Характеристики приймача

На приймачі трафік протікає у зворотному напрямку, як показано на рисунку 4.5:

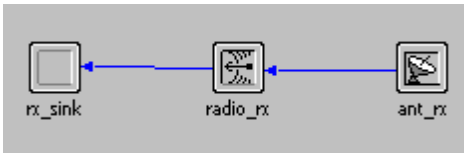


Рисунок 4.5 – Модулі приймача

Як видно з характеристики таблиці 4.3 приймач ловить радіосигнал за допомогою антени. Потім він передається радіомодулятору для демодуляції з параметрами сигналу, що підлягають аналізу. По завершенні сигнал відправляють у змішувач.

Таблиця 4.3 – Характеристики приймача

Характеристики генератора трафіку	Характеристики радіомодулятора

Attribute	Value
name	rx_sink
process model	sink
icon name	processor

Attribute	Value
name	radio_rx
channel	(...)
rows	1
row 0	
data rate (bps)	1,024
packet formats	all formatted, unformatted
bandwidth (kHz)	10
min frequency (MHz)	30
spreading code	disabled
processing gain (dB)	channel bw/dr
modulation	bpsk
noise figure	1.0
ecc threshold	0.0
ragain model	dra_ragain
power model	dra_power
bkgnoise model	dra_bkgnoise
inoise model	dra_inoise
snr model	dra_snr
ber model	dra_ber
error model	dra_error_all_stats
ecc model	dra_ecc
icon name	ra_rx

4.2.2 Сценарій 2

Сценарій 2 (рисунок 4.6) імітує мережу, використовуючи протоколи 802.11, реалізуючи протокол CSMA/CA в шар MAC. Мережа працює в режимі клієнт-сервер.

Цей сценарій буде надалі розділений на два під-сценарії; у першому під-сценарії моделюється постійний бітовий трафік, тоді як у другому під-сценарії моделюється HTML трафік.

У цьому сценарії моделюється 20 вузлів, 19 клієнтів та 1 сервер (node_8), усі вони створені з використанням вбудованої моделі 'wlan_wkstn' ; розмір сценарію такий же, як у сценарію 1.

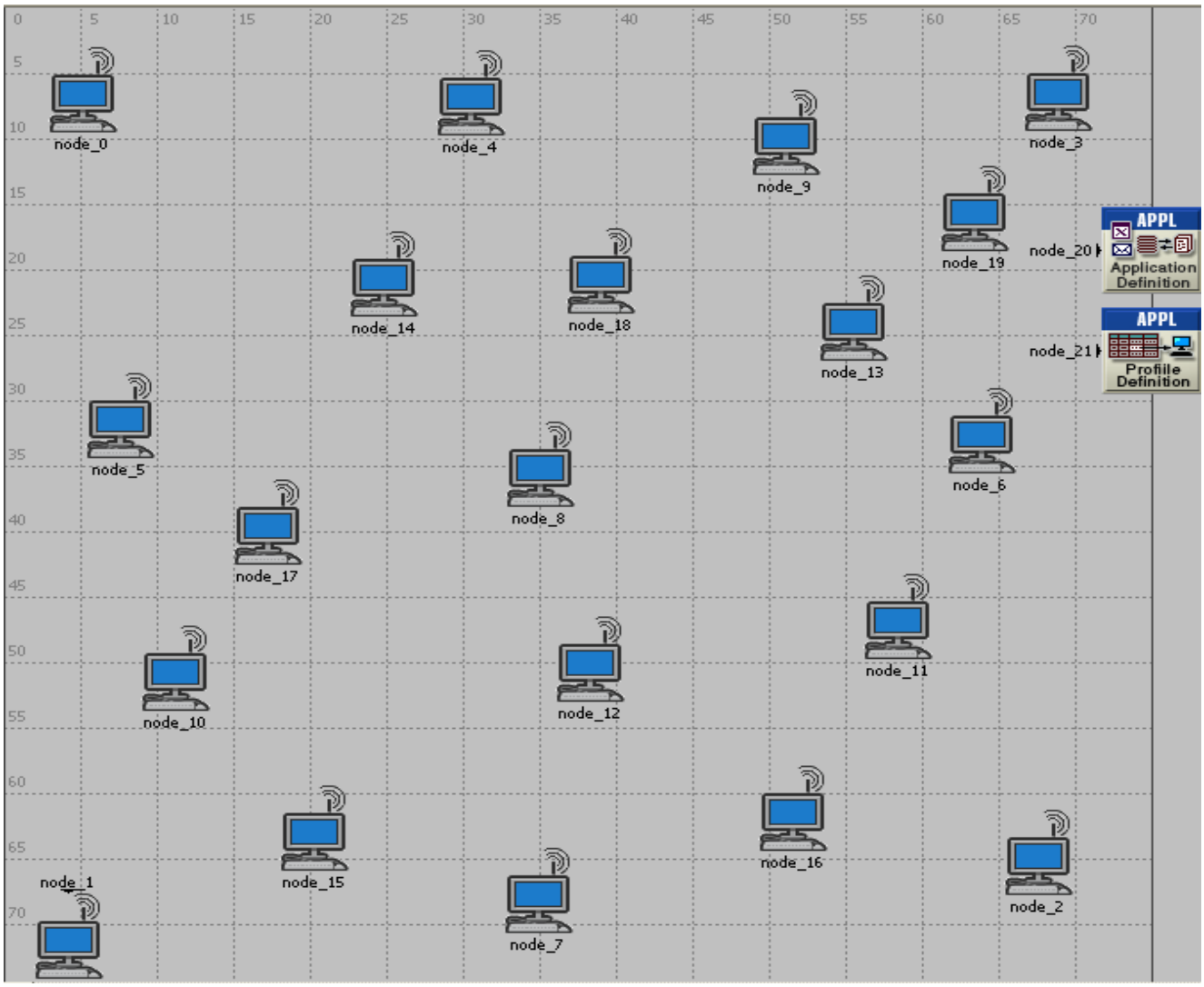


Рисунок 4.6 – Макет сценарію 2

4.2.2.1 Визначення додатків і визначення профілю характеристик

Модель «wlan_wkstn» вимагає створення профілю для трафіку в мережі. Це робиться за допомогою двох модулів: в першому модулі вказується тип програми,

що створює трафік, тобто для першого під-сценарію у цьому моделюванні створюється трафік CBR, для другого під-сценарію, трафік створюється за допомогою HTTP1.1 (табл. 4.4).

Таблиця 4.4 – Характеристики визначення профілю та програми

Характеристики визначення додатків	Характеристики визначення профілю

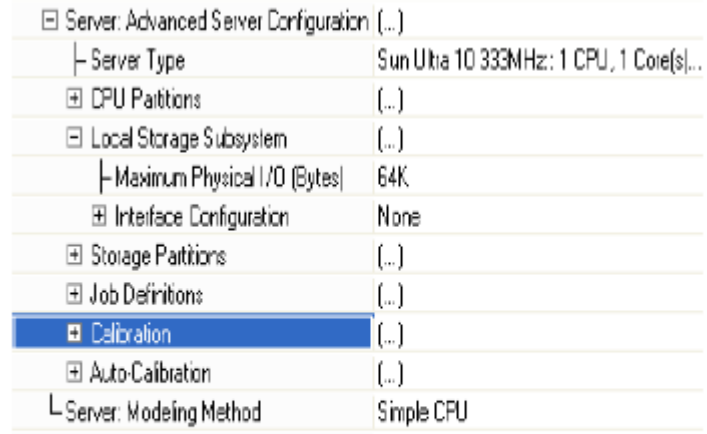
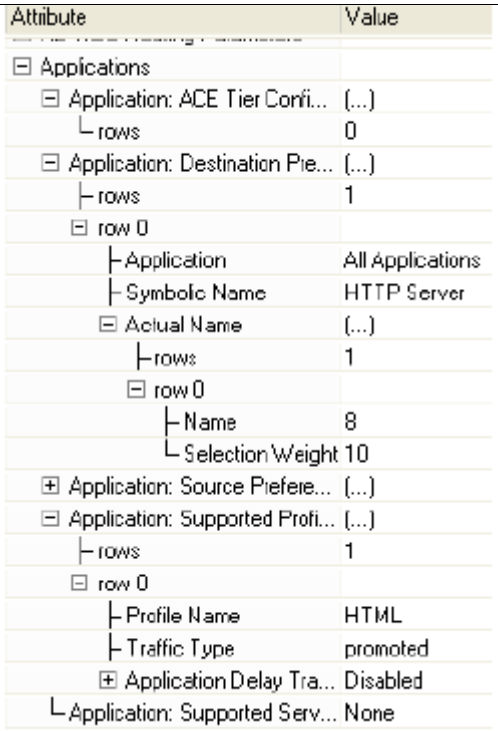
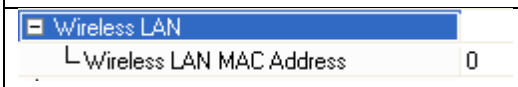
Attribute	Value
name	node_20
model	Application Config
x position	75
y position	18.6
threshold	0.0
icon name	util_app
creation source	Object Palette
creation timestamp	23:09:20 Aug 27 2007
creation data	
label color	black
Application Definitions	(...)
rows	1
row 0	
Name	HTML
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Image Browsing
Print	Off
Remote Login	Off
Video Conferencing	Off
Voice	Off
Voice Encoder Schemes	All Schemes
hostname	
minimized icon	circle/#708090
role	

Attribute	Value
name	node_21
model	Profile Config
x position	75
y position	26.3
threshold	0.0
icon name	util_profiledef
creation source	Object Palette
creation timestamp	23:09:24 Aug 27 2007
creation data	
label color	black
Profile Configuration	(...)
rows	1
row 0	
Profile Name	HTML
Applications	(...)
rows	1
row 0	
Name	HTML
Start Time Offset (seconds)	uniform (5,10)
Duration (seconds)	End of Profile
Repeatability	Unlimited
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
Repeatability	Once at Start Time
hostname	
minimized icon	circle/#708090
role	

4.2.2.2 Характеристика вузлів

Наступна таблиця (таблиця 4.5) показує поведінку вузла, коли він використовується як сервер. У цьому випадку він використовується як станція, що працює під управлінням Solaris як операційна система, з єдиним процесором і одним ядром. Параметри програми застосовують додаток та визначення профілю (у цьому випадку інтенсивно переглядає зображення за допомогою HTML 1.1)

Таблиця 4.5 – Характеристики вузлів

Характеристики сервера	Параметри програми
	
Бездротові характеристики	
	

Модулі вузлів (рисунок 4.7) – це стек реалізованих протоколів у стандарті 802.11.

Ці модулі є основою моделі; тому їх характеристики є ядром моделювання.

На наступних рисунках показані найбільш відповідні модулі, які використовуються для цієї дипломної роботи, це: MAC характеристики шару, модуль для передачі та модуль для прийому.

На рівні MAC найважливішими характеристиками є швидкість передачі даних, яка встановлюється в 11 мбіт/с, і поріг прийому, встановлений на рівні – 95 дБм (рисунок 4.8).

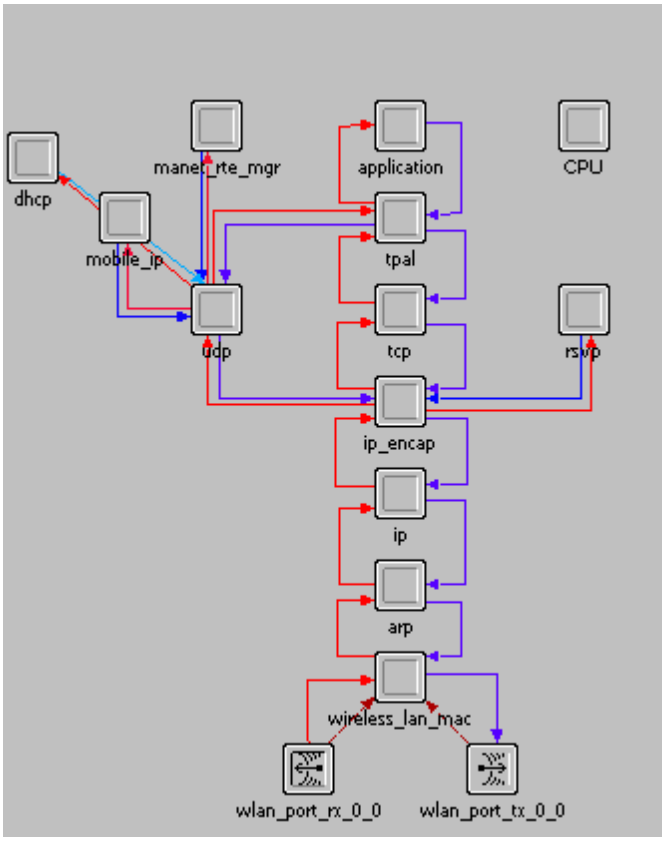


Рисунок 4.7 – Модулі вузла

Attribute	Value
name	wireless_lan_mac
process model	wlan_dispatch
icon name	processor
Wireless LAN	
Address	promoted
Wireless LAN Parameters	[...]
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
Channel Settings	[...]
Bandwidth (MHz)	Physical Technology Dependent
Min Frequency (MHz)	BSS Based
Transmit Power (W)	0.005
Packet Reception-Power Threshold (dBm)	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
PCF Parameters	Disabled
HCF Parameters	Not Supported

Рисунок 4.8 – Модуль Wireless_lan_mac

Приймач має мінімальну частоту 2401 МГц з пропускною здатністю 100 000 КГц, і використовує 'dpsk' в якості схеми модуляції. Всі інші характеристики показані на рисунку 4.9.

Attribute	Value
name	wlan_port_rx_0_0
channel	(...)
rows	1
row 0	
data rate (bps)	1,000,000,000
packet formats	unformatted, wlan_control, wlan_mac
bandwidth (kHz)	100,000
min frequency (MHz)	2,401
spreading code	disabled
processing gain (dB)	channel bw/dr
modulation	dpsk
noise figure	1.0
ecc threshold	0.0
ragain model	NONE
power model	wlan_power
bkgnoise model	dra_bkgnoise
inoise model	dra_inoise
snr model	dra_snr
ber model	wlan_ber
error model	wlan_error
ecc model	wlan_ecc
icon name	ra_rx

Рисунок 4.9 – Модуль Wlan_port_rx_0_0 module

Передавач має майже такі ж характеристики, як і передавач (збіг каналу), але він також включає потужність передачі, при якій передавач передає (рисунок 4.10).

Attribute	Value
name	wlan_port_tx_0_0
channel	(...)
rows	1
row 0	
data rate (bps)	1,000,000,000
packet formats	ip_dgram_v4, tcp_seg_v2, udp_dgram_...
bandwidth (kHz)	100,000
min frequency (MHz)	2.401
spreading code	disabled
power (W)	0.005
bit capacity (bits)	infinity
pk capacity (pks)	1,000
modulation	dpsk
rxgroup model	wlan_rxgroup
txdel model	wlan_txdel
closure model	dra_closure
chanmatch model	wlan_chanmatch
tagain model	NONE
propdel model	wlan_propdel
icon name	ra_tx

Рисунок 4.10 – Модуль Wlan_port_tx_0_0module

4.2.2.3 Характеристики глушилки

Використовуваний джамер (рисунок 4.11) був побудований на основі "jam_sb" (таблиця 4.6), включеного в Бібліотеки OPNET.

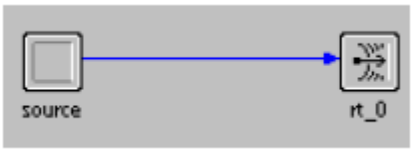


Рисунок 4.11 – Модулі джамера

Таблиця 4.6 – Характеристики модулів джамера

Характерні характеристики джамера	Rt_0 характеристики джамера

Attribute	Value
name	source
process model	simple_jammer_source
icon name	processor
Packet Interarrival Time	constant (0.01)
Packet Size	constant (1024)
Start Time	10.0
Stop Time	Infinity

Attribute	Value
name	rt_0
channel	(...)
rows	1
row 0	
data rate (bps)	1,000,000
packet formats	unformatted
bandwidth (kHz)	100,000
min frequency (MHz)	2,401
spreading code	1.0
power (W)	0.03
bit capacity (bits)	infinity
pk capacity (pks)	1,000
modulation	jammod
rxgroup model	dra_rxgroup
txdel model	dra_txdel
closure model	dra_closure
chanmatch model	dra_chanmatch
tagain model	NONE
propdel model	dra_propdel
icon name	ra_tx

4.2.3 Сценарій 3

Сценарій 3 – це варіант сценарію 2. Хоча постійний джамер використовується в сценарії 2, в сценарії 3 використовується випадковий джамер (також відомий як імпульсний джамер). Імпульсний джамер був змінений на

джамер, який на випадковий проміжок часу впадає в сон, замість використання фіксованого періоду, як це робиться в стандартній моделі OPNET.

4.2.3.1 Характеристики глушилки

Використовуваний імпульсний джамер (рисунок 4.12) має такі характеристики, які позначені у таблиці 4.7.

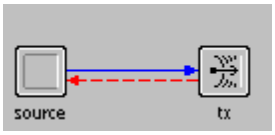


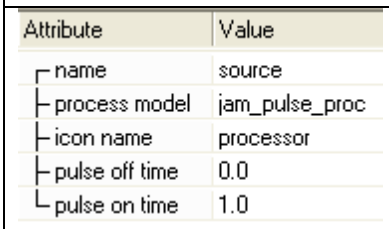
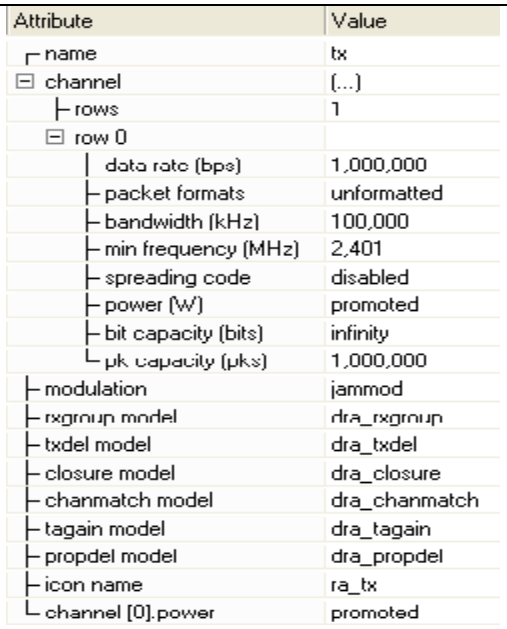
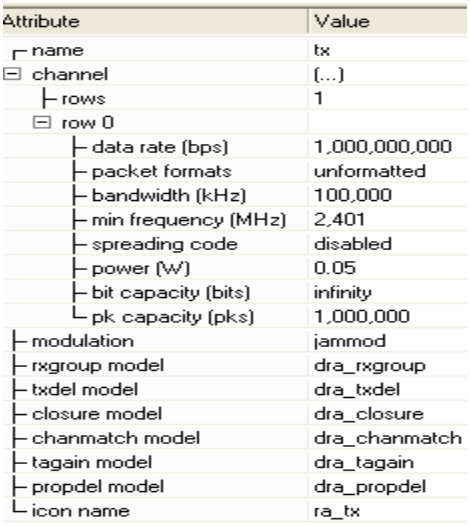
Рисунок 4.12 – Внутрішні модулі імпульсного джамера

4.2.4 Сценарій 4

Сценарій 4 імітує мережу, використовуючи протоколи 802.11 таким же чином, як у сценарії 2;сценарій 4 також використовує CSMA/CA на рівні MAC. Різниця полягає в тому, що в цьому сценарії мережа реалізується спеціально.

Макет для цього сценарію точно такий же, як у зображеного на рисунку 4.6 , з такою ж кількістю вузлів і однаковими моделями вузлів. Однак вузол, використаний у сценарії 2, як точка доступу (AP) використовується як простий спеціальний вузол у цьому сценарії. Вузли змінені щоб моделювати спеціальну мережу, використовуючи динамічну маршрутизацію джерела (DSR).

Таблиця 4.7 – Характеристики модулів імпульсного джамера

Характерні характеристики імпульсного джамера	Tx характеристики імпульсного джамера
	 

4.2.4.1 Характеристика вузлів

Усі характеристики вузлів такі ж, як і у вузлів для сценарій 3, за винятком спеціальних параметрів маршрутизації (рис. 4.13).

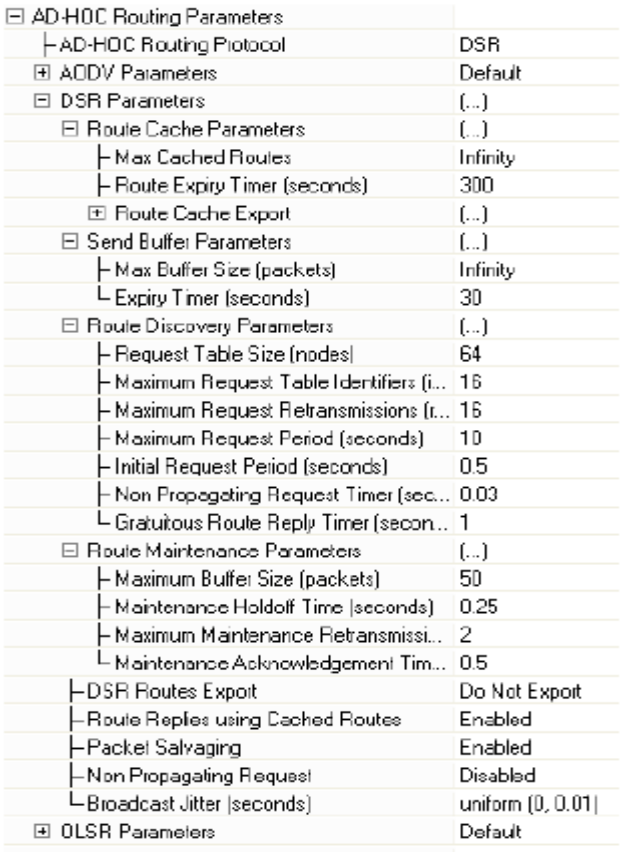


Рисунок 4.13 – Спеціальні характеристики

4.2.5 Сценарій 5

Сценарій 5 імітує недоброзичливий вузол у мережі. У цьому випадку немає глушилки – є лише дійсні вузли та один вузол, який погано працює. Погано працює в тому сенсі, що цей вузол не відчуває канал і чекає випадкового періоду часу. Він безпосередньо вводить трафік в канал, отримуючи несправедливу перевагу перед іншими вузлами.

Вузол був створений на основі попередньо побудованої моделі 'wlan_wkstn_adw' , але без модуля 'wireless_lan_mac', який відповідає за протоколи MAC. Отримана внутрішня структура показана на рисунку 4.14. Внутрішній код модуля TCP був модифікований для імітації постійного бітового трафіку (див. додаток Б).

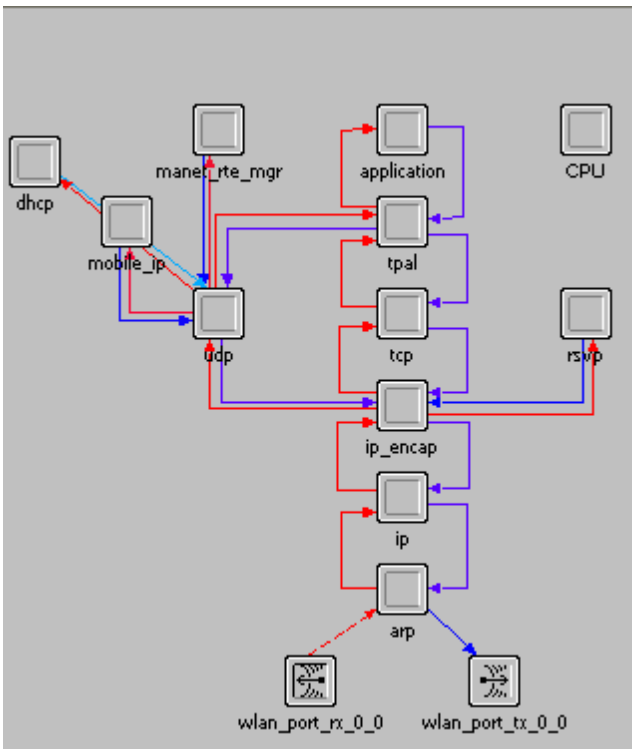


Рисунок 4.14 – Порушення внутрішньої структури вузла

Моделювання буде виконуватися двічі, перший із лише трьома вузлами, двома добре діючими вузлами та одним несправним вузлом. Другий запуск буде модульований за допомогою густої мережі з 15 вузлів. Обидва випадки будуть імітовані за допомогою клієнт-сервера.

4.3 Аналіз моделювання

Аналізуємо результати, отримані за кожним із описаних у вище сценаріїв. Результати моделювання показані на графіках, кожен з яких супроводжується деталізованими поясненнями.

4.3.1 Сценарій 1

Як описано в розділі 4.2, симуляції були розділені на п'ять різних сценаріїв. Перший сценарій являє собою площу 75 × 75 метрів з 3 різними вузлами (рисунок 4.15); верхній-лівий вузол являє собою рухливий джамер, який йде по прямій

(зеленій лінії) протягом 90 хвилин(тривалість моделювання). Вузол праворуч від зеленої лінії представляє чесний передавач з характеристиками, описаними в підрозділі 4.2.1 ; вузол зліва – чесний приймач.

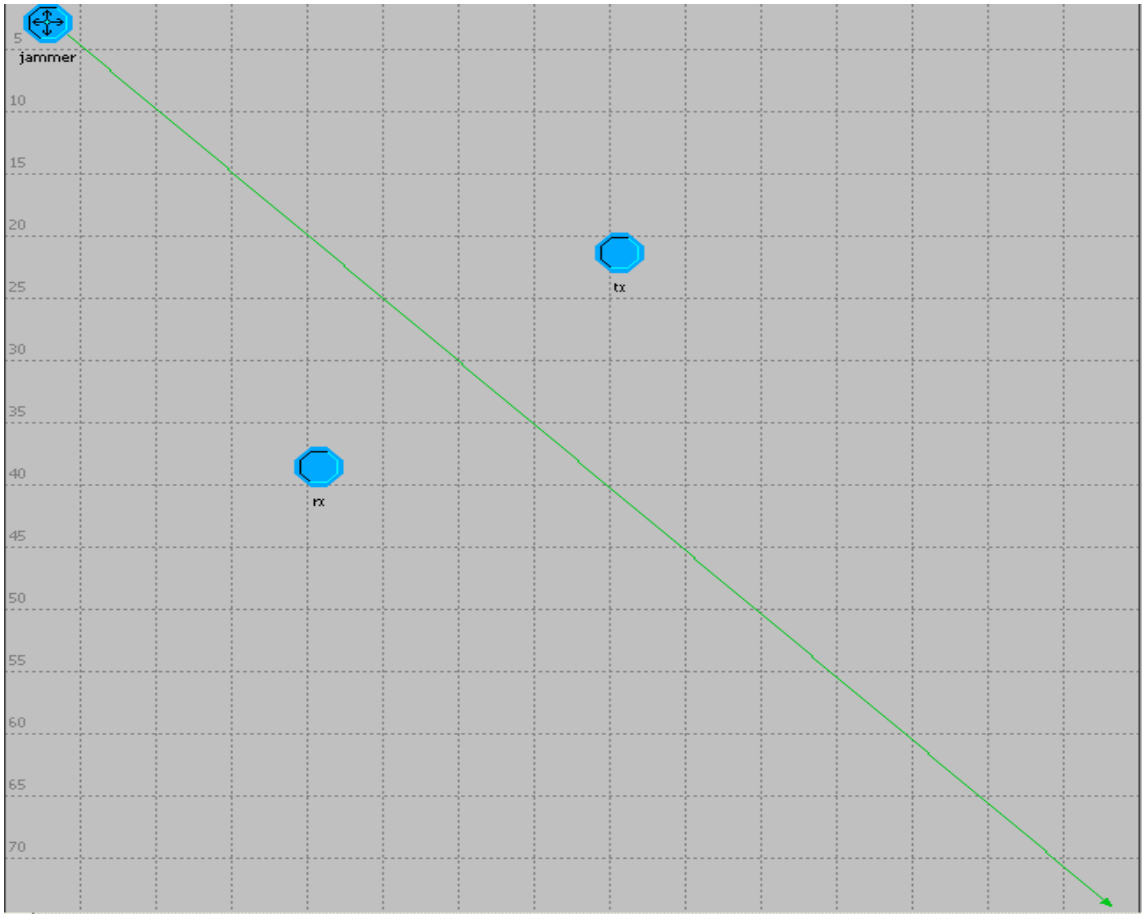


Рисунок 4.15 – Макет сценарію 1 (75 × 75 метрів)

В симуляції представлено рухому атаку зловмисника або терориста на мережу аеропорту. Також симуляцію можна представити в вигляді нестандартної постійної перешкоди від не санкціонованої апаратури.

За звичайних обставин трафік за цим сценарієм досягає пропускної здатності 100%, тому що ідеальний сценарій немає перешкод, фоновий шум значно низький, і це єдине джерело шуму, яке приймає до уваги OPNET

На рисунку 4.16 представлена швидкість помилки бітів, отримана потужність, співвідношення сигнал/шум і значення пропускної здатності при нормальних обставинах, потужність передавача: 0,032 Вт і має час взаємодії пакетів 1 пакет в секунду

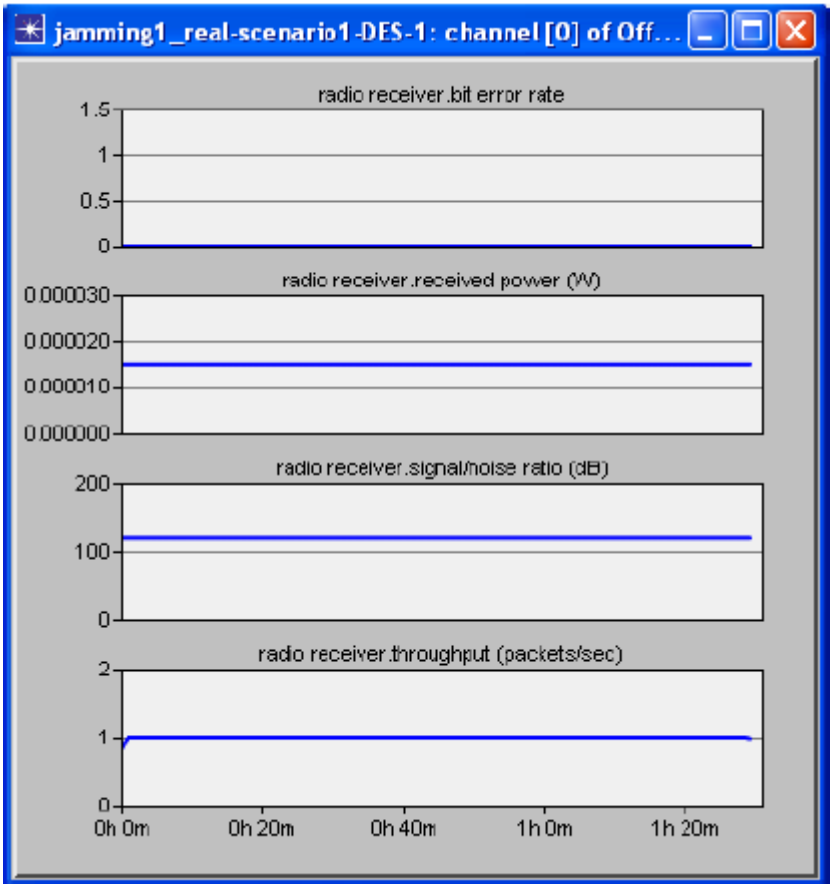


Рисунок 4.16 – Характеристики трафіку за звичайних обставин

Після цього в сценарій вводиться джамер. Цей джамер посилає пакети з енергією рівною енергії створеною передавачем. У пакетах джамера використовується спеціальний вид модуляція, реалізований в OPNET, називається "jammod".

Після того як передавач відправляє пакет, він приймається на антену приймача і класифікує цей пакет як дійсний. Паралельно з цим закликом, який був вже представлений, джамер постійно надсилає недійсні пакети. Тому приймач отримує два пакети одночасно. Пакет, надісланий джамером, класифікується як перешкода.

На наступному етапі відбувається запис пакетів, які надійшли в той же час в і той же канал приймача.

Коли пакет А надходить до антени приймача одночасно з пакетом В, класифікує пакет А як шум для пакету В і навпаки. Крім того, ядро резервує

атрибут даних передачі (DTA), значення якого збільшується щоразу, коли дійсний пакет приходить на приймач, а цей приймач заважає іншому пакету.

На наступному рисунку (рис. 4.17) показано, що відбувається, коли дросель із потужністю передачі 0,032 Вт вставляється в сценарій. Передавач зберігає свою потужність передачі 0,032 Вт використовує 'bpsk' як схему модуляції.

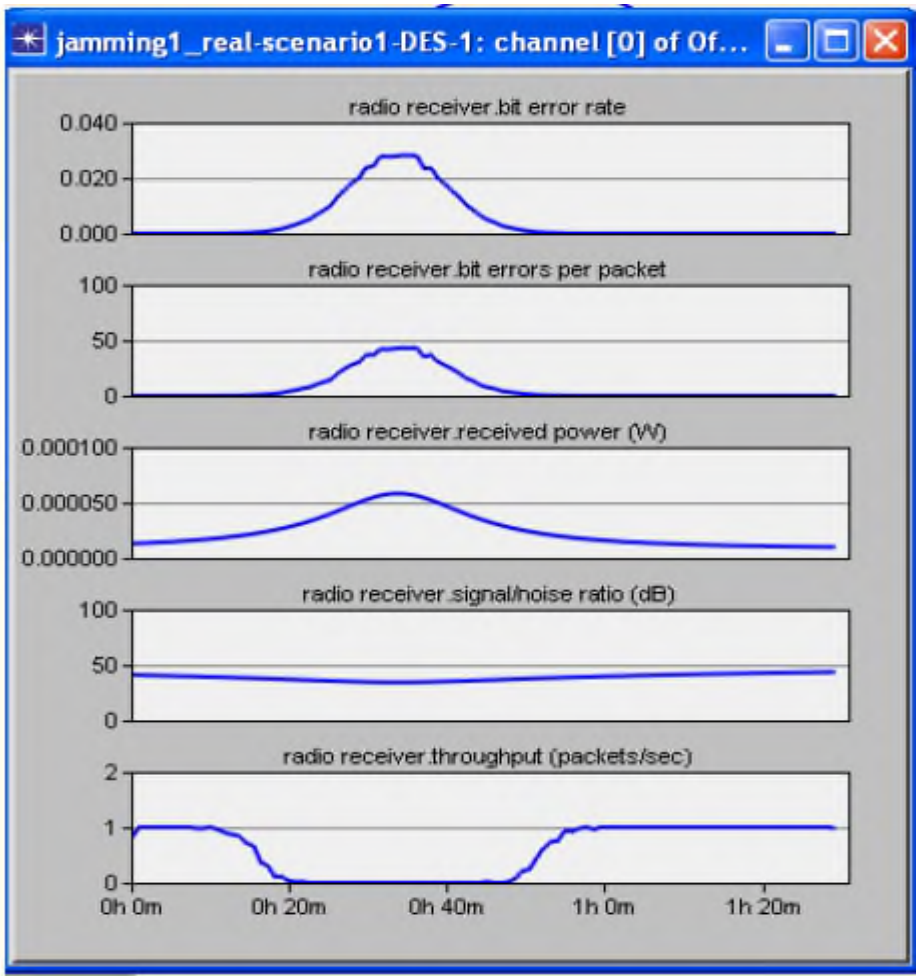
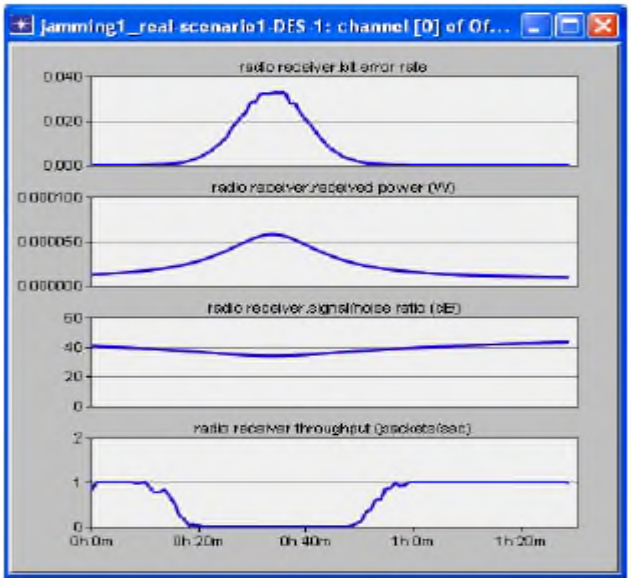


Рисунок 4.17 – Характеристики трафіку під час дії глушилки

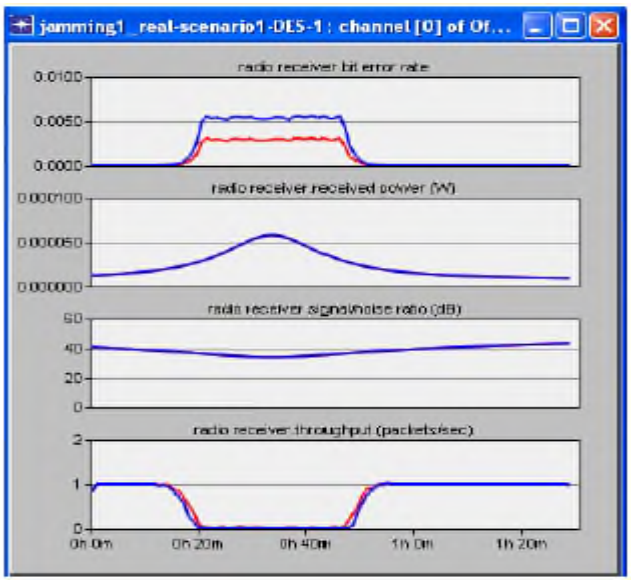
Як видно з графіка (рис. 4.17), коли джамер вставлений у сценарій, ймовірність частоти помилок бітів значно зростає, досягаючи майже до 4% від ймовірності помилки на біт. Хоча ця ймовірність здається недостатньо високою, щоб викликати помилку в кожному біті, але в графіку під назвою "бітові помилки на пакет" демонструє, що в деяких випадках більше 50 біт зіпсовані. Слід також нагадати, що іноді потрібно змінити лише пару біт щоб змусити відмовити весь пакет. Показник бітових помилок в OPNET не моделюється – він обчислюється з

таблиці, що входить до ядра OPNET. Третій графік показує, що потужність у приймачі також збільшується при введенні джамера, але сигнал/шум значно зменшується, збільшуючи ймовірність помилок у пакетах; які приймач не може виправити, що призводить до зниження пропускної здатності до нуля приблизно на 30 хвилин, доти, поки джамер не буде подалі від відправника та одержувача, і тоді вони зможуть відновити нормальну роботу.

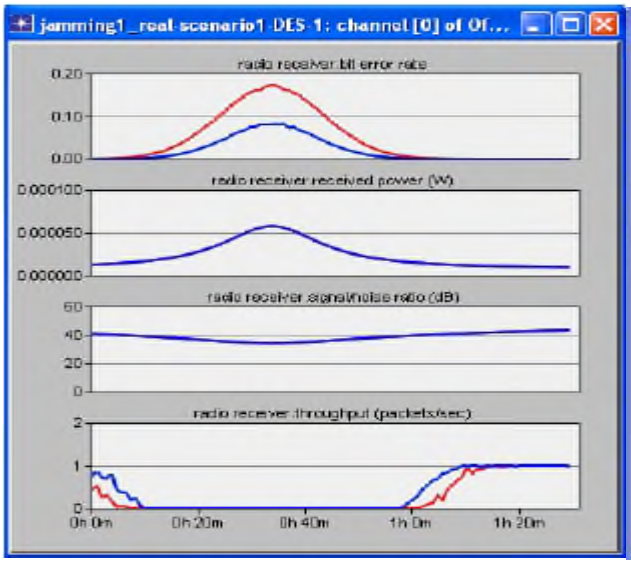
Інші набори моделювання виконувались з використанням різних видів модуляцій, таких як: двійкова фазова маніпуляція (bpsk) та bpsk_pch; додаткове введення коду (cck11 icck55); подвійний фазовий зсув (dpsk); частотний зсуву та його варіанти; частотна модуляція Гауса з мінімальним зрушенням (gmsk); мінімальний зсув (msk); фазовий зсув (psk) та його варіанти; модуляція методом квадратичної амплітуді (QAM) та її варіація; квадратурна фазова маніпуляція (QPSK). Ці графіки виконувались із вимкненим ‘spread code’ атрибутом. Наступний набір графіків (рис. 4.18) показує результати, отримані для вибраної схеми модуляції (щоб побачити результати для кожної схеми модуляції, перейдіть у додаток А). Вони показують, що схема модуляції, яка використовується для передачі інформації, дійсно важлива.



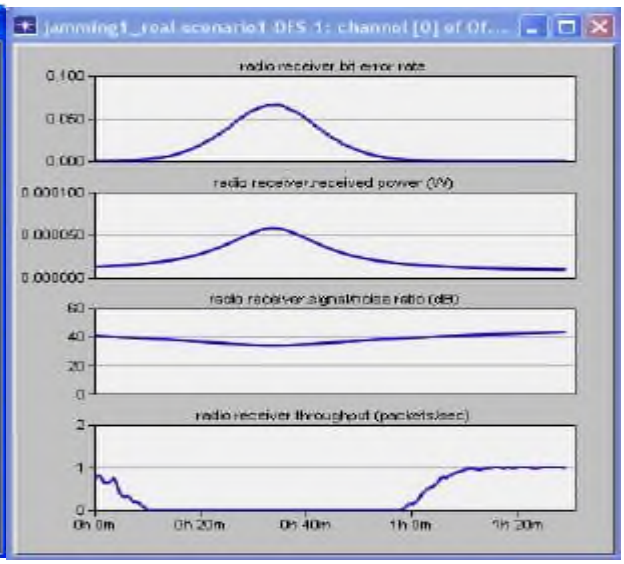
Bpsk синім кольором



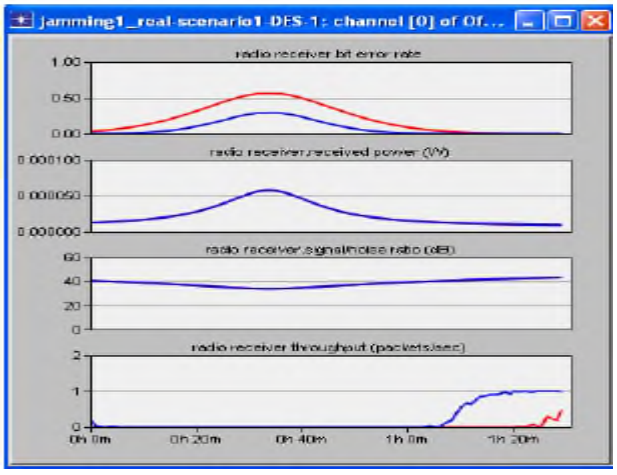
Cck11 синім кольором, cck55 червоним кольором



Fsk2 синім кольором, fsk2_ncoh червоним кольором



Psk8 синього кольору



Qam16 синього кольору, Qam64 червоного кольору

Рисунок 4.18 – Різні схеми модуляції під час дії глушилки.

Попередні графіки показали, що існують деякі схеми модуляції, які є більш здатними протидії завадам від джамера, наприклад, можна помітити, що qpsk, bpsk, gmsk, msk та cck є більш стійкими і мають пропускну здатність 0 лише приблизно 30 хвилин, а quam16, qam64 і fsk мають пропускну здатність нуля більше 50 хвилин. M – модуляція одночасно модулює n бітів інформації з використанням 2^n формою хвилі. Це означає, що поріг (відстань) між кожною з хвиль (амплітуда, кут, частота) зменшується, коли кількості хвиль збільшується. Тому коли є багато хвиль, так як у Qam64, навіть найменша зміна фонового шуму каналу викликає багато бітових помилок, це головна причина чому Qam 64 працює гірше проти дії глушилки. У випадку qpsk, bpsk, gmsk, msk та cck, які використовують дуже малу кількість сигналів для передачі даних, поріг (відстань) між кожним із цих сигналів більший, отже, вони більш підготовлені до зміни сигналу фонового шуму, викликаним глушилкою.

Якщо включений ‘spread code’, різниці в результатах немає.

Однією з найважливіших вхідних змінних, яку необхідно враховувати, є потужність, яку джамер використовує, для наступного показника потужність джамера була збільшена до 0,1 Вт.

На рисунку 4.19 видно, що частота ймовірність помилок бітів зростає до неприйнятного майже 10%, через що помилка трохи більше ніж 100 біт на пакет; отримана потужність на приймач також значно збільшена; хоча графіки тепер показує великі зміни, в результаті пропускна здатність показує, що ця невелика різниця має великий вплив, на пропускну здатність протягом 1 години 10 хвилин.

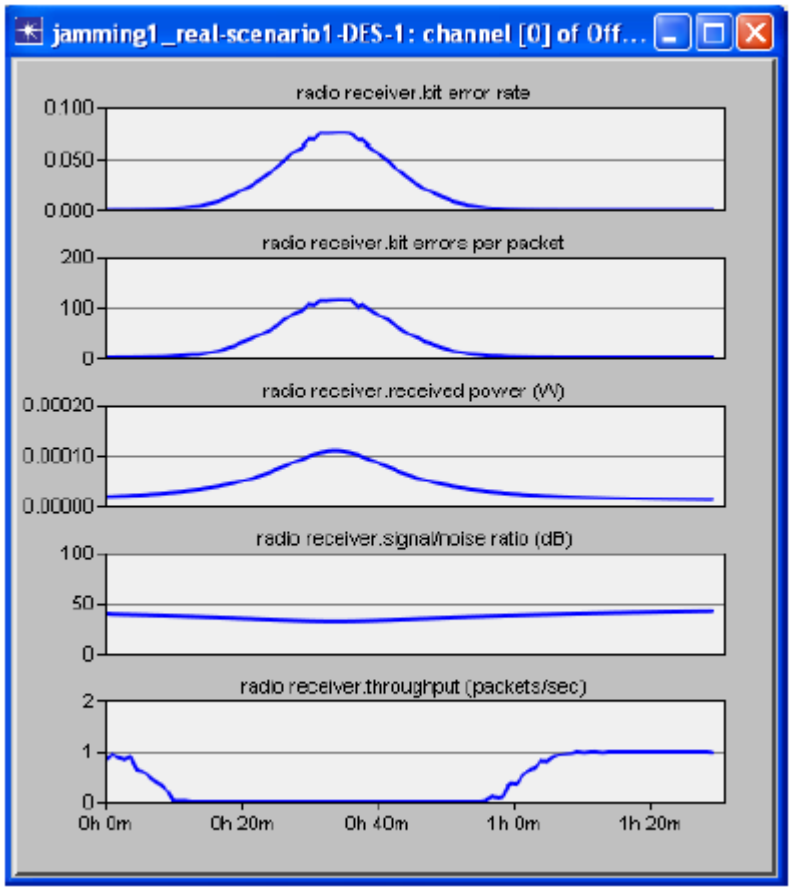


Рисунок 4.19 – Збільшено потужність у джамері до 0,1 Вт

4.3.1 Сценарій 2

У цьому випадку фокус робиться на зв'язок між двома вузлами клієнт-сервер. Цей сценарій розділений на дві частини, перша імітується за допомогою постійної швидкості передачі бітів, у другий моделюється за допомогою протоколу HTTP під час перегляду веб-сторінок.

В симуляції представлено спрямовану атаку зловмисника або терориста на AP мережі аеропорту. Також симуляцію можна представити в вигляді нестандартної спрямованої перешкоди від не санкціонованої апаратури та антен аеропорту.

В обох сценаріях джамер спочатку чекає 10 секунд, щоб дозволити AP досягти стійкого стану, а потім повертає свій радіопередавач і починає розсилати пакети з дійсними, але недоцільними пакетами.

Найважливіші вхідні змінні: швидкість взаємодії джамера, потужність передачі і відстань між джамером і AP (точкою доступу).

Вихідними змінними, які необхідно дотримуватися, є:

– пропускна здатність в AP : оскільки в цьому сценарії в мережі є лише одна AP, весь трафік повинен пройти через нього;

– час зайняття передавача : це час, який вузол витрачає на передачу своїх даних;

– час прослуховування одержувачем : це час, коли вузол витрачає на прослуховування, чекаючи доступу.

Другий сценарій складається з 19 хостів, які розподіляються випадковим чином і 1 точка доступу (AP) розташований посередині; цей сценарій був розроблений так, що кожен вузол знаходиться в точці доступу передачі (рис. 4.20).

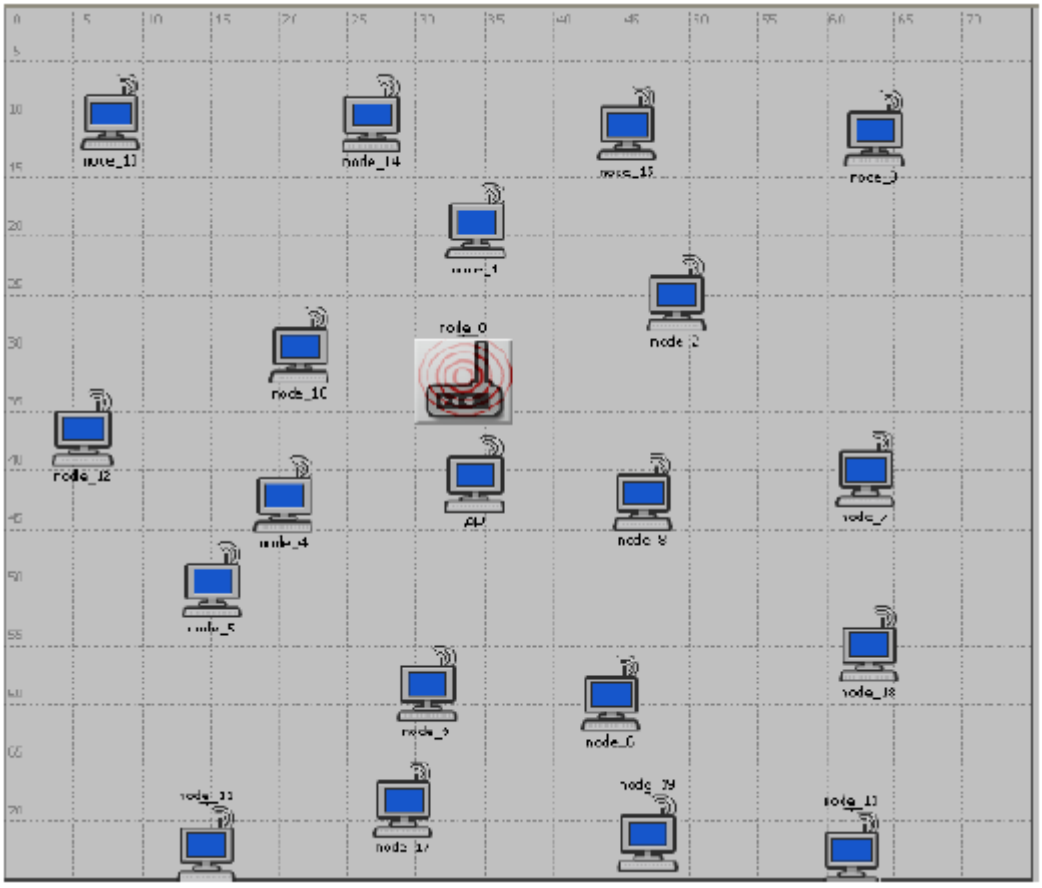


Рисунок 4.20 – Макет сценарію 2

На рисунку 4.21 показано трафік мережі за звичайних обставин.

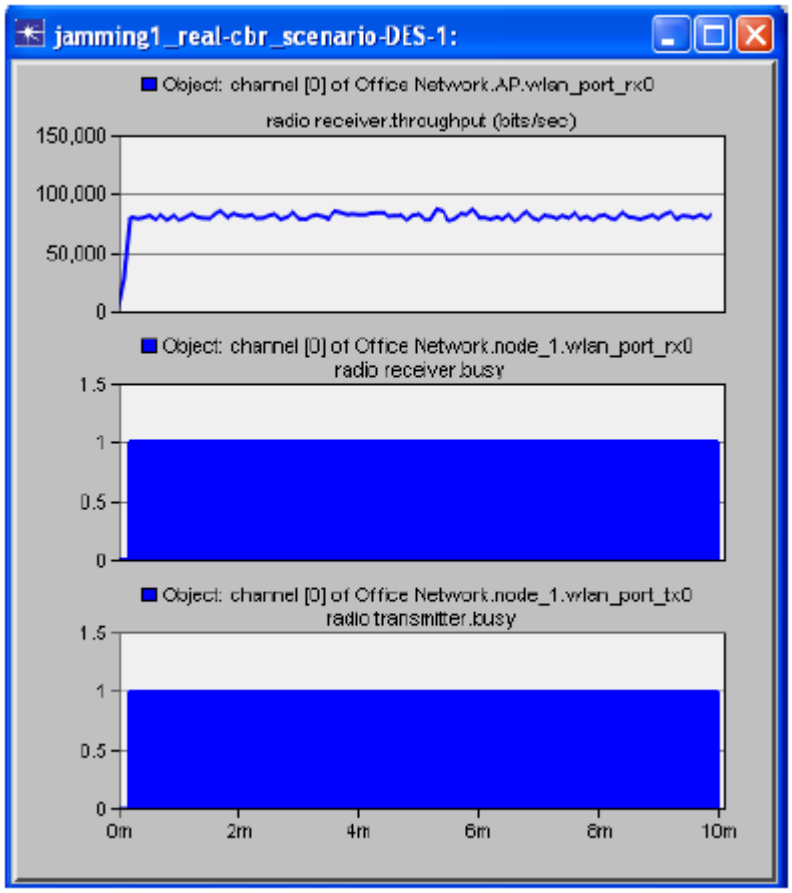


Рисунок 4.21 – Трафік без завад

На рисунку видно, як пропускна здатність в AP становить приблизно 80 кбіт/с через те, що є лише один AP на 19 вузлів, і тому виникає багато зіткнень. Можна побачити що передавач завжди зайнятий, що означає, що він приймає і відправляє трафік.

На рисунку 4.22 представлений 30-секундний крупний план вузла, який показує, як вузол може чергувати посилання з отриманням повідомлень.

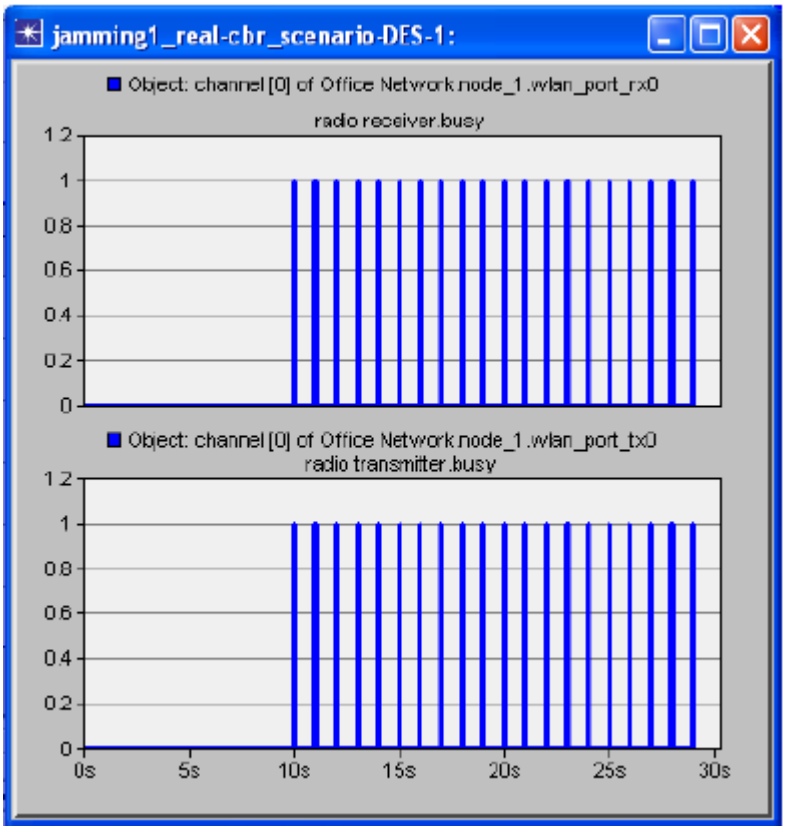


Рисунок 4.22 – 30-секундний план

Два важливих аспекти відіграють важливу роль у цьому сценарії. Перше, що джамер повинен створювати пакети швидше, ніж чесні вузли, щоб запобігти їх переключенню на прослуховувальний режим передачі. Друга полягає в тому, що потужність вузла повинна бути достатньо високою, щоб охопити всі вузли у мережі, якщо використовується лише один джамер, тому він повинен мати більшу потужність живлення, ніж чесні вузли, для цього моделювання ми припускаємо, що у джамеру і у всіх вузлів є необмежена енергія (тобто акумулятор не розряджається).

На рисунку 4.23 видно, що введення джамера – верхній графік показує, що джамер знижує трафік AP до нуля; на графіку в середині видно, що джамер зберігає вузли, які слухають весь час, і останній графік показує, що вузли не можуть передавати жоден пакет.

Оскільки джамер постійно вводить пакети з дійсним заголовком, AP змушений отримувати всі пакети, але AP не може всі ці пакети зберегти, тому їх скидає. Ось чому AP підтримується у режимі прослуховування весь час.

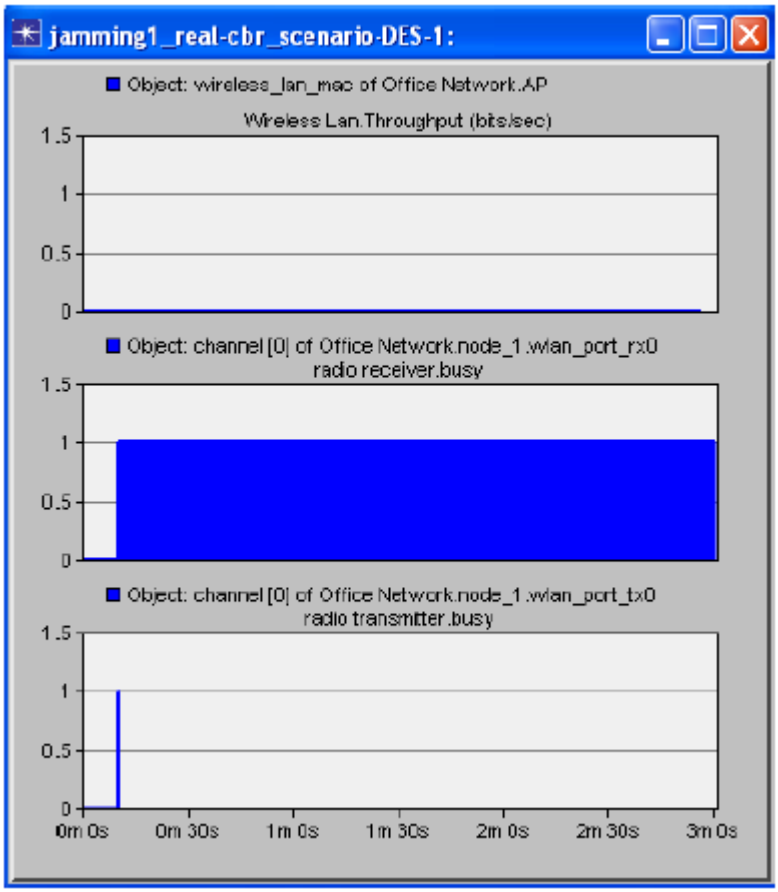


Рисунок 4.23 – Трафік при введенні джамера

30-секундний знімок (рис. 4.24) був зафіксований, щоб показати, що приймач завжди активно сприймає канал, він весь час зайнятий, тому не може перейти в режим передачі.

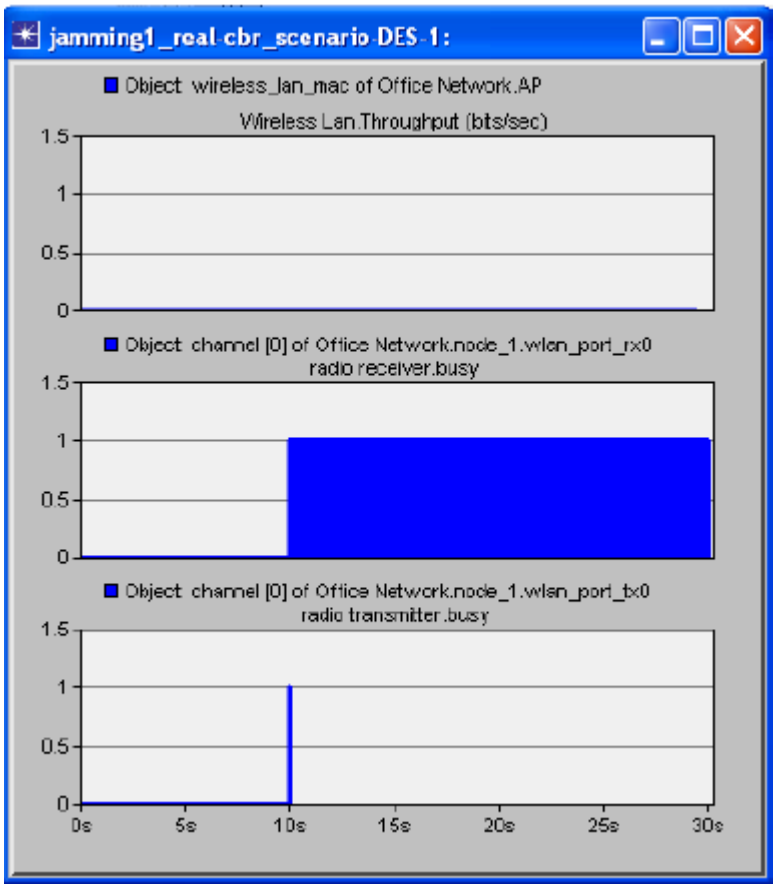


Рисунок 4.24 – 30-секундний крупний план при введенні джамера

Був запущений інший набір моделювання, але замість моделювання трафіку за допомогою CBR значення додатку та профіля було змінено на сценарій перегляду веб-сайтів із великим експоненціальним розподілом замість звичайного розподілу.

Цей під-сценарій було вирішено використовувати, оскільки в реальних умовах трафік майже ніколи не постійний. Тому трафік HTTP вважався хорошим прикладом реального генератора світового трафіку.

На рисунку 4.25 показана характеристика трафіку до та після введення джамера. У лівому графіку можна побачити, що трафік з експоненціальним розподілом і як і передавач, і як приймач постійно зайняті; з іншого боку, на графіку праворуч ми можемо побачити, що незважаючи на той факт, що приймач завжди зайнятий, пропускної здатності у вузлі немає.

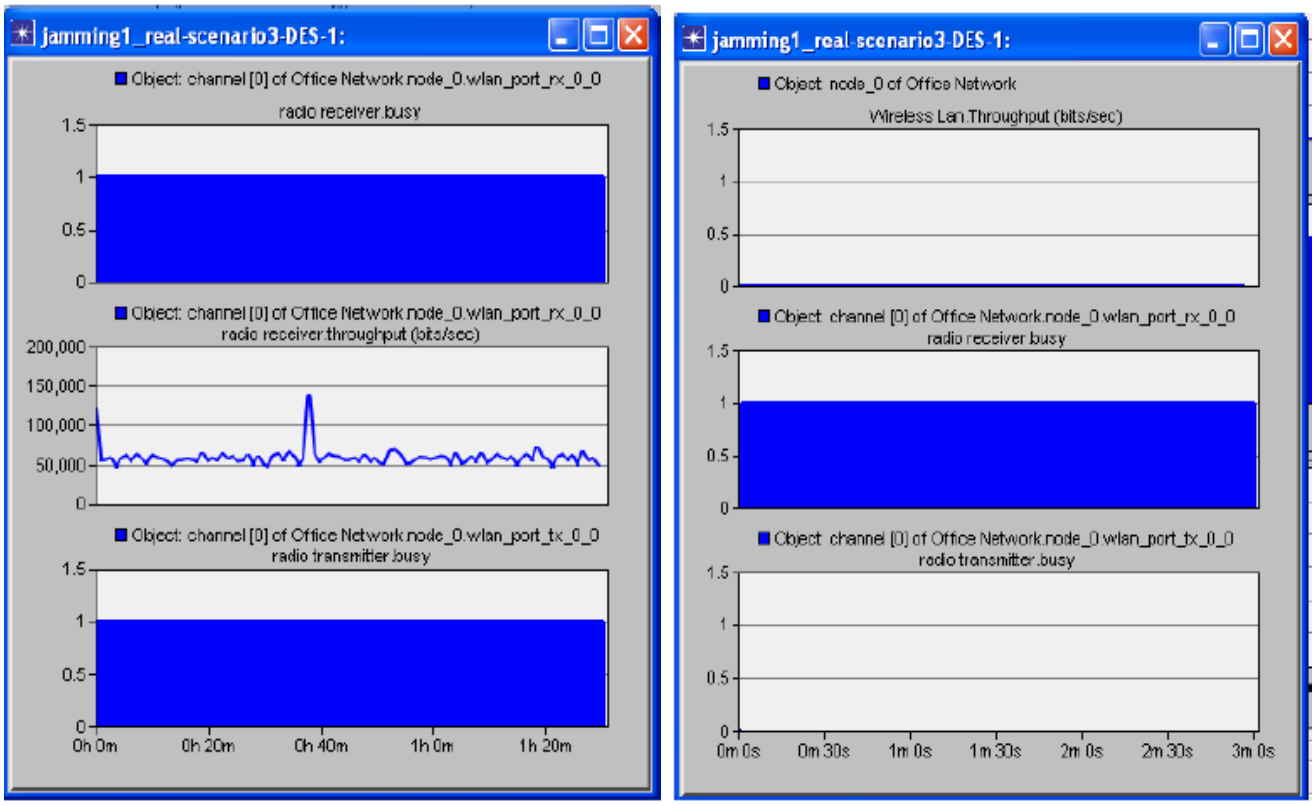


Рисунок 4.25 – До і після введення джамера

На рисунку 4.26 показано 30-секундне закриття, і можна помітити, що приймач не встигає перейти з режиму прослуховування в режим передавача.

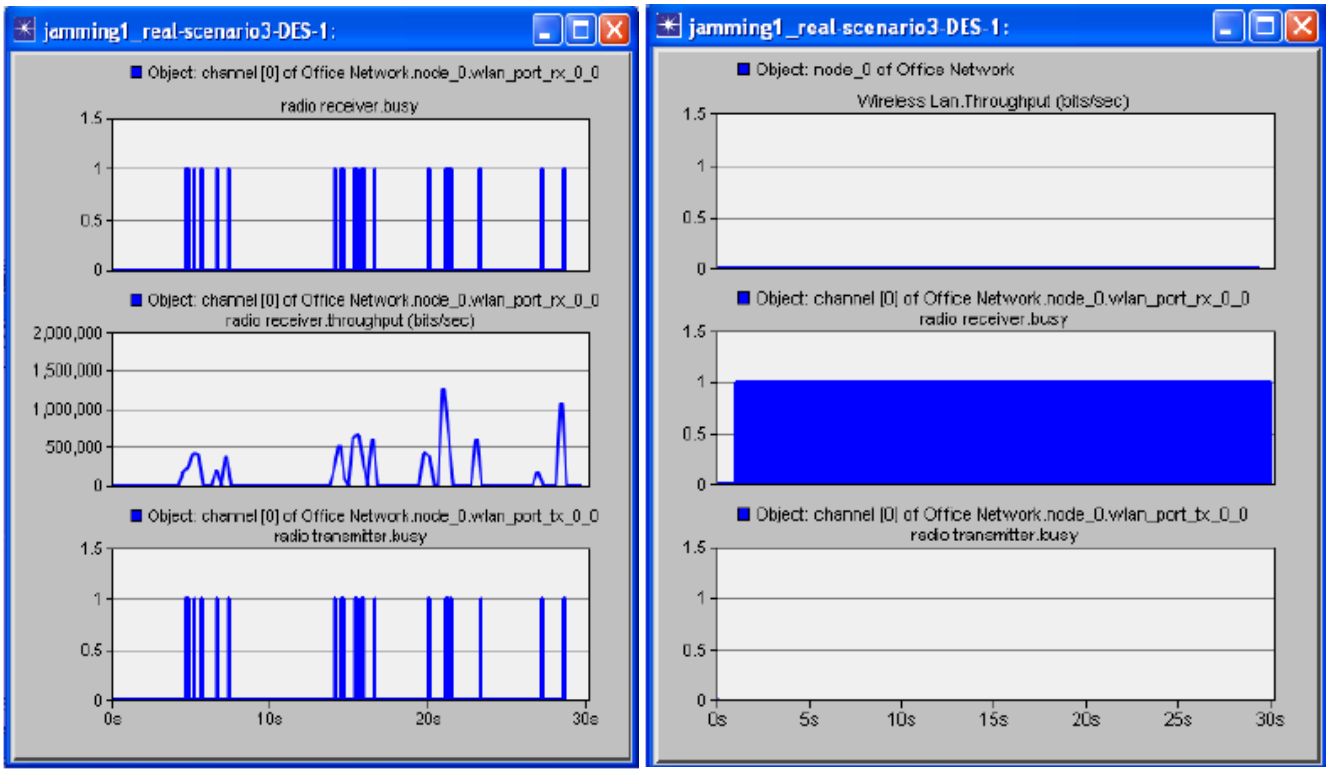


Рисунок 4.26 – 30-секундний план

4.3.3 Сценарій 3

Всі попередні сценарії були зосереджені на аналізі наслідків постійних та оманливих завад в мережі клієнт-сервер. Цей сценарій фокусується на аналізі випадкових завад в мережі клієнт-сервер.

В симуляції представлено випадкову атаку перешкодами на мережу Wi-Fi в аеропорту, спричиненими технікою та спеціальною апаратурою аеропорту.

Макет той самий, що використовується для мережі за сценарієм 1; у всіх вузлів однакові характеристики, але не як в сценарії 2. Єдина відмінність полягає в тому, що в цьому сценарії джамер, замість того, щоб постійно вводити пакети в мережу, надсилає пакети лише на випадковий період часу, а потім лягає спати в ще один випадковий проміжок часу.

Ціль такого типу завад – не падіння пропускної здатності до нуля, а значно зменшити пропускну здатність протягом більш тривалого періоду часу.

Як видно з графіку (рис. 4.27), пропускна здатність перед джамером в деяких точках досягає 2,4kbps (синя лінія); при введенні випадкового імпульсного джамера пропускна здатність падає значно аж до 800 bps.

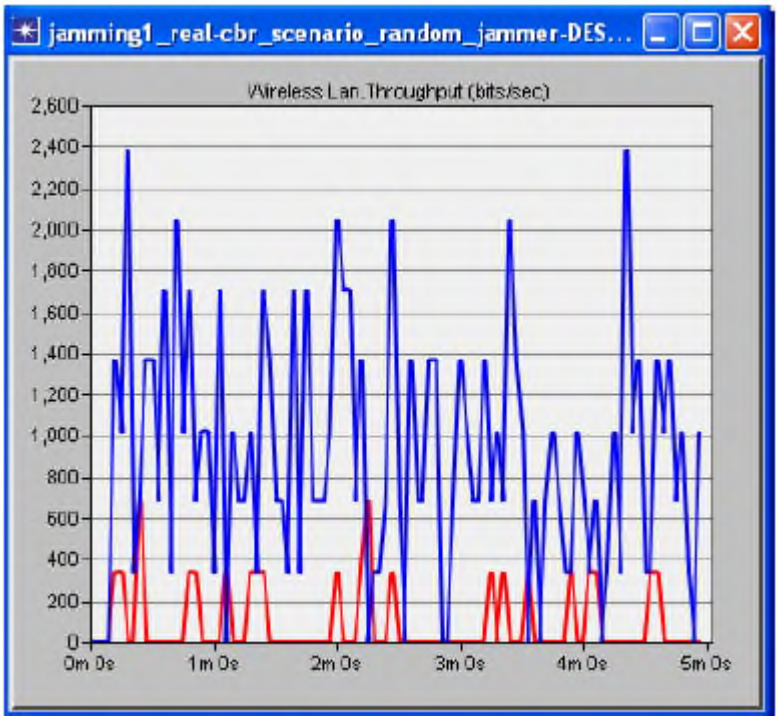


Рисунок 4.27 – Трафік до (синій) та після (червоний) випадкової завади

4.3.4 Сценарій 4

Як було сказано в підрозділі 4.2.4, цей сценарій зосереджений на зв'язку між вузлами в спеціальному режимі. Кожен вузол зберігає постійну швидкість передачі бітів, щоб краще демонструвати ефект атаки завад.

В симуляції представлено атаку перешкод на мережу Wi-Fi, яка знаходиться на території аеропорту. За перешкоду представляємо літак, а також можна представити за перешкоду завади від вишки аеропорту.

Цей сценарій був вирішений на 10 × 10 кілометрів (рис. 4.28), щоб можна було показати два ефекти: перший це ефект, який має атака завад в спеціальній мережі, і друга, щоб показати мережевий зв’язок пошкоджений через атаку, якщо відстань досить велика, не всі вузли можуть бути забитими, і тому деяка комунікація все ще існує в мережі.

Сценарій складається з 20 вузлів з експоненціальним-міжопераційним трафіком та динамічною маршрутизацією від джерела (DSR) як алгоритм маршрутизації (на рисунку 4.26 показане компонування). У цьому сценарії приймачі вибираються випадковим чином. Також в центрі сценарію є джамер з максимальною потужністю 0,1 Вт. Коло, що оточує вузол, – це дальність передачі джамера.

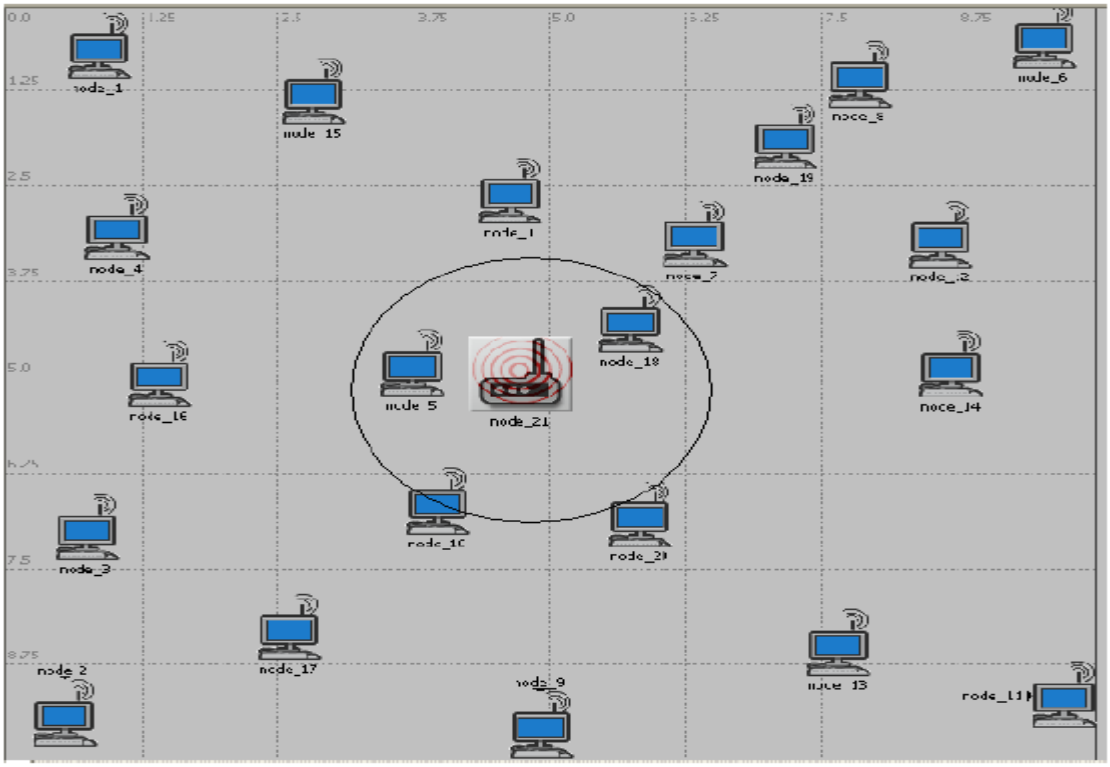


Рисунок 4.28 – Схема для сценарію 4

Ця спеціальна мережа використовує CSMA як протокол MAC. Це означає, що якщо відправник хоче відправити деякий трафік у мережу, він спочатку перевіряє канал, і якщо він вільний, він надсилає туди трафік. Інакше він відключиться на випадковий проміжок часу перед повторною спробою. Коли джамер запускається, він тримає середовище каналу зайнятим і тому відправник ніколи не буде мати змогу отримати доступ до каналу.

Наступний рисунок (рис. 4.29) показує трафік у чотирьох різних вузлах мережі, коли мережа не атакується. Ці чотири вузли були обрані через їх відстань до джамера: вузли 1, 6 і 12 були обрані тому, що вони відносно далекі від джамера; а вузол 5, тому що він розташований відносно близько до джамера.

Графік зліва на рисунку 4.29 показує експоненціально розподілений трафік у кожному з чотирьох вузлів перед атакою завад від джамера; з іншого боку, графік праворуч показує, як трафік в кожному вузлі змінюється. Можна помітити, що оскільки вузли 1 і 6 дійсно далекі від завад трафік залишається недоторканим, таким чином показуючи, що хоча деякі вузли були порушені, де які послуги все ще можуть надаватися.

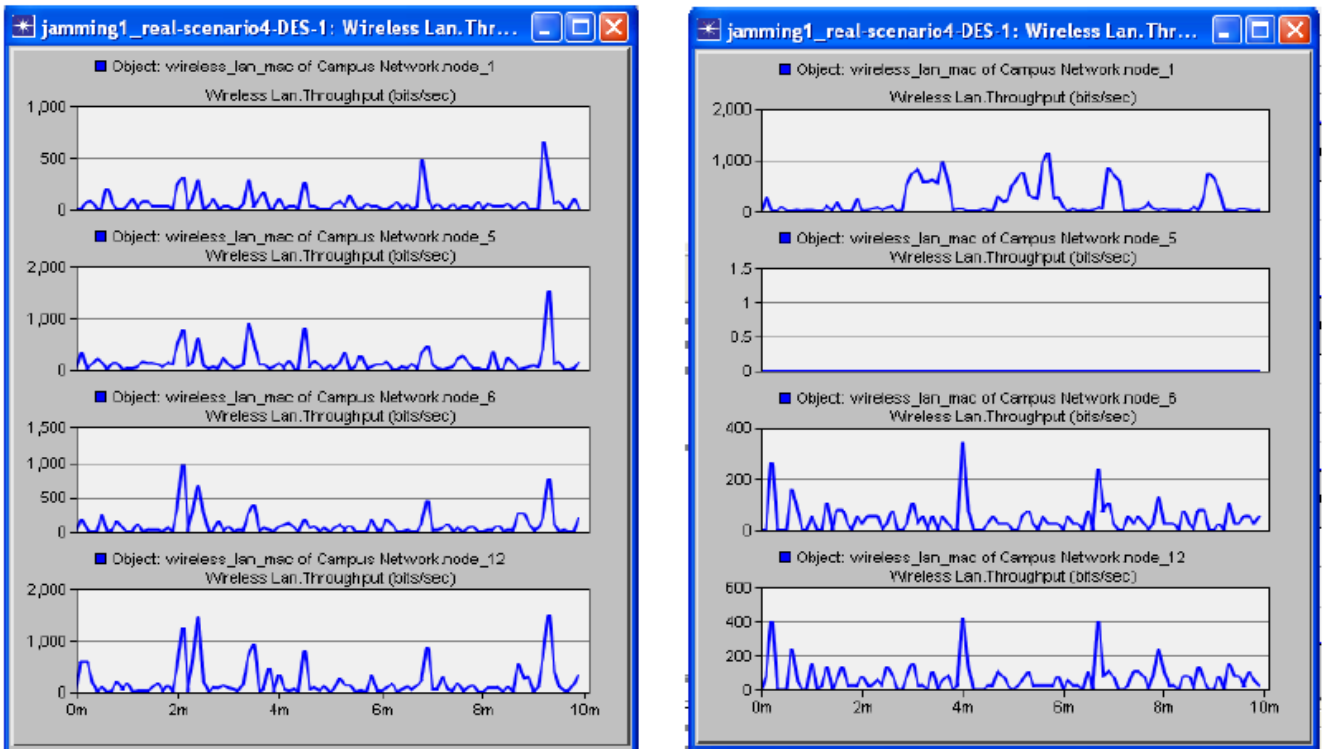


Рисунок 4.29 – Трафік у 4 вузлах до та після включення завд

4.3.5 Сценарій 5

У цьому сценарії імітується несправний вузол. Вид симуляції поведінки полягає в тому, що вузол не відповідає протоколу MAC; він передає трафік, як тільки йому це знадобиться. З іншого боку, інші вузли – працюють нормально; вони чекають, поки канал для передачі стане вільним.

Перша частина сценарію складається з трьох вузлів, двох добре діючих вузлів, що обмінюються трафіком і один несправний вузол (вузол-3). Використовуємо топологію клієнт-сервер. Три вузли генерують постійний трафік. На рисунку 4.30 показаний макет сценарію.

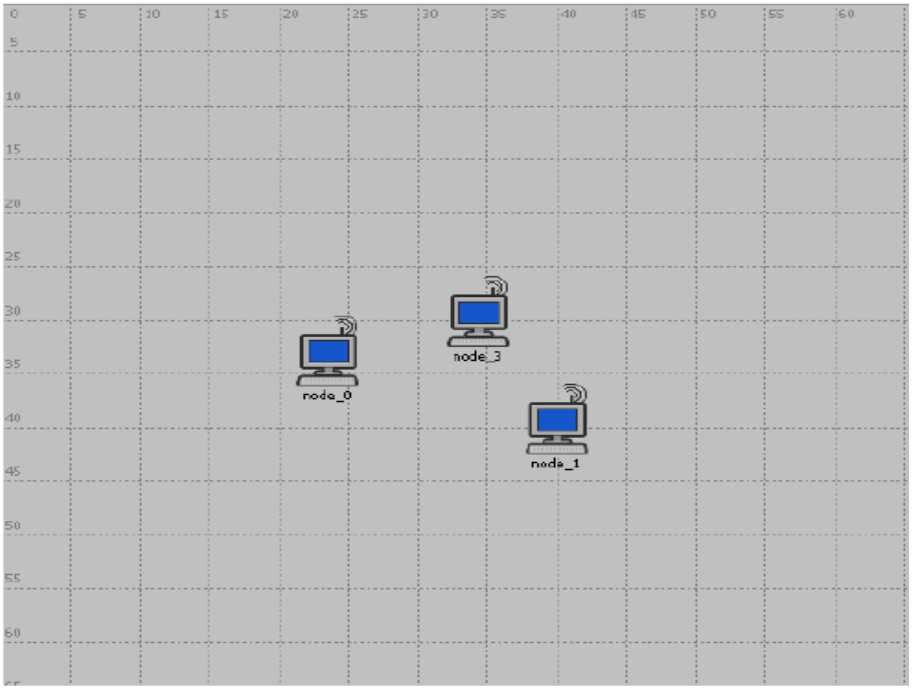


Рисунок 4.30 – Макет сценарію 5

На рисунку 4.31 видно, що при несправному вузлі в мережі немає всього трафіку; в цьому сценарії жодна інша загроза безпеці не передбачається. Після введення несправного вузла, трафік значно скорочується.

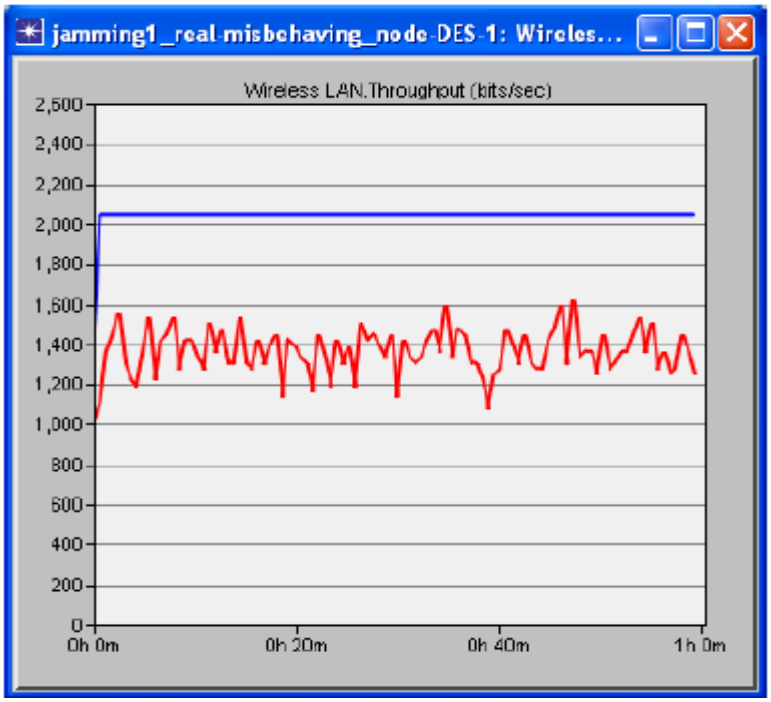


Рисунок 4.31 – До (синій) та після (червоний) введений неправильно діючого вузла

Цей же експеримент був проведений з 15 добре працюючими вузлами та одним несправним вузлом, близьким до AP, рисунок 4.32 показує, що результати були аналогічні тим, які представлені на рисунку 4.31.

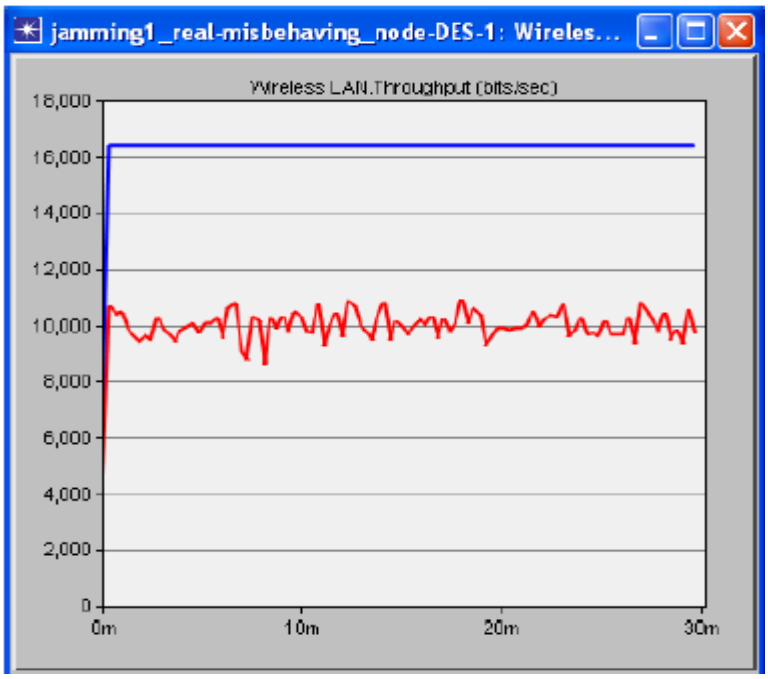


Рисунок 4.31 – До (синій) та після (червоний) введений неправильно діючого вузла в більшу мережу

Трафік значно падає з трьох причин:

– вузол, що погано працює, розташований близько, тому AP може вводити свої пакети безпосередньо до нього;

– оскільки несправний вузол має нечесну перевагу, він викликає затримки на сусідніх вузлах (більшість з них сусіди AP);

– зіткнення, спричинені поганим вузлом, якщо сусід послав пакет перед ним.

5 ЕКОНОМІЧНІ РОЗРАХУНКИ

5.1 Обґрунтування актуальності теми з позиції маркетингу

Бездротовий зв’язок, який найчастіше зустрічається через використання бездротової мережі (Wi-Fi) або мобільного телефону, став звичайним інструментом для повсякденного життя. Однак бездротовий зв’язок піддається радіочастотним (ВЧ) перешкодам. Зростаюче використання та важливість бездротових мереж не лише як пасажирських зручностей, але і як невід'ємної частини операцій аеропорту, робить його надійність та ефективність важливими для сучасних операцій в аеропорту. Безпека також є критичною, оскільки бездротовий зв'язок став потенційним вектором атаки – способом порушити роботу аеропорту. Таким чином, надійна захищена мережа, яка добре керується та модернізується відповідно до збільшення запитів та заявок – це головне питання для керівників аеропортів.

У рамках дослідження зібрана інформація з аеропортів щодо досвіду роботи з Wi-Fi, зокрема про проблеми з перешкодами, потужністю та продуктивністю. Які рішення були випробувані та чи були вони успішними. Включаючи процеси, методи, процедури та застосовні інструменти, які можна використовувати для виявлення причини перешкод та визначення їх рішення для пом’якшення проблеми. У цій главі також містяться рекомендації щодо альтернативних методів та ресурсів, до яких можна отримати доступ, коли проблема перевищує звичайні зусилля інженера.

Мандрівники з великими сподіваннями на послугу Wi-Fi будуть оминати аеропорт, який не відповідає їхнім очікуванням на безперебійне обслуговування зв'язку. Крім того, оскільки менеджери аеропортів та мандрівники мають обмежені можливості домовитися та узгодити свої очікування, аеропорти, які не забезпечують високоякісний Wi-Fi, можуть виявити, що відсоток мандрівників може вибрати інші аеропорти для вильоту або сполучення рейсів. Бізнес-мандрівники, зокрема, потребують надійного підключення до Інтернету, щоб

виконувати роботу під час очікування рейсів, особливо, коли рейси затримуються або скасовуються, порушуючи бізнес-графіки.

Всі ці проблеми з мережею зв’язку в аеропорті, можуть спричинити не тільки погіршення роботи самого аеропорту, а ще фінансові проблеми з мандрівниками, які можуть обрати конкурентів, у котрих не будуть проблем з Wi-Fi. Тому цей проект є економічно вигідним для керівників аеропорту.

5.2 Визначення трудомісткості та тривалості роботи

Основною умовою раціонального планування дослідження є скорочення строків виконання при мінімальних витратах трудових, матеріальних та грошових ресурсів. Для цього вирішуються такі питання: визначення трудомісткості та тривалості витрат і ефективності дослідження.

Комплекс науково–дослідницьких робіт може бути поділений на етапи. Для кожного етапу необхідно вказати його найменування, трудомісткість, виконавців і тривалість робіт. В даній роботі беруть участь один молодший науковий співробітник і один старший науковий співробітник. Результати розподілу наведені в таблиці 5.1.

Через те, що важко встановити трудомісткість виконання робіт, у зв'язку з елементами незвичайності, в процесі виконання більшості науково-дослідницьких робіт, використовується ймовірнісний метод. При цьому використовують дві або три вірогідних оцінки часу. Ці оцінки є вихідними для розрахунку очікуваного часу виконання роботи за формулою 5.1:

$$t_{оч} = \frac{3 \cdot t_{min} + 2 \cdot t_{max}}{5} \tag{5.1}$$

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

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

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

Таблиця 5.1 – Оцінка довготривалості та трудомісткості етапів робіт

№	Етапи роботи	Часова оцінка, дн.			Дис - персія	Виконавці		Тривалість, днів
		t_{min}	t_{max}	$t_{оч}$		Спеціа-льність	Кіл-сть, чол.	
1	2	3	4	5	6	7	8	9
1	Отримання технічного завдання	1	2	2	0,2	Молодший науковий співробітник	1	2
2	Огляд літературних джерел	3	7	5	0,8	Молодший науковий співробітник	1	5
3	Аналіз основних принципів організації	2	4	3	0,4	Молодший науковий співробітник	1	3
4	Підготовчий (техніко- економічне обґрунтування) етап	14	20	17	1,2	Молодший науковий співробітник	1	14
5	Написання програми	13	15	14	0,4	Старший науковий співробітник	1	14
6	Аналіз результатів програми	13	19	16	1,2	Старший науковий співробітник	1	11

Продовження таблиці 5.1

1	2	3	4	5	6	7	8	9
7	Вибір необхідного обладнання та матеріалів	2	4	3	0,4	Молодший науковий співробітник	1	3
8	Експериментальні дослідження	20	22	21	0,6	Молодший науковий співробітник	1	21
9	Аналіз отриманих даних, коригування програми	5	7	6	0,4	Старший науковий співробітник, Молодший науковий співробітник	2	6
10	Висновки та пропозиції	8	10	9	0,4	Старший науковий співробітник	1	7
11	Складання та обговорення технічного звіту	2	2	2	0,0	Старший науковий співробітник	1	2
12	Впровадження результатів	2	2	2	0,0	Молодший науковий співробітник	1	2
	Усього	85	114	100	—	—	—	90

Ступінь правильності визначення перевіряється розрахунком дисперсії – різниці між мінімальною та максимальною оцінками часу, що визначається за формулою (5.2):

$$\sigma = \frac{t_{max} - t_{min}}{5} \tag{5.2}$$

Розраховані значення для кожного етапу занесені у табл. 5.1.

Дана дипломна робота повинна виконуватися поетапно, у лінійній послідовності, так без отримання необхідних результатів дослідів не можна виконувати наступний пункт. Використовуючи дані табл. 5.1, збудуємо лінійний календар (рис. 5.1):

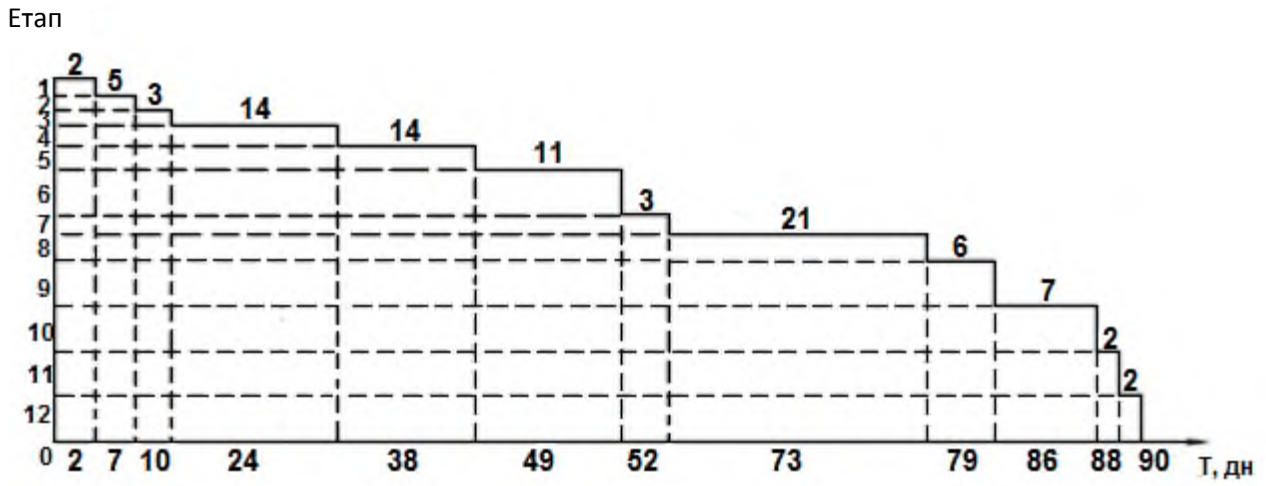


Рисунок 5.1 – Лінійний календарний графік

5.3 Розрахунок кошторису витрат на практичну реалізацію дипломного проекту

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

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

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

5.3.1 Розрахунок вартості матеріалів

До статті витрат на матеріали включаються вартість основних та допоміжних матеріалів, необхідних для розробки проекту. За період проведення науково-дослідницьких робіт співробітниками будуть використані наступні матеріали (табл. 5.2)

Таблиця 5.2 – Розрахунок вартості матеріалів

Матеріал	Марка, ГОСТ, ДСТУ, ТУ	Кількість	Ціна за одиницю, грн/шт.	Витрати за матеріали	Частка, %
Папір А4	UNI Office A4	500	0,3	150	10,72
Папір А2	Xerox A2	4	306	1224	87,49
Папір А1	Xerox A1	50	0,5	25	1,79
Усього	–	–	–	1399	100

5.3.2 Спеціальне устаткування

У цій статті враховуються витрати на оренду, доставку і монтаж лабораторних установок, вимірювальних та регулювальних пристроїв, приладів, випробувальної апаратури тощо (табл. 5.3).

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

Таблиця 5.3 – Витрати на спеціальне устаткування

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

5.3.3 Розрахунок заробітної плати

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

Розрахунок заробітної плати ведеться на основі даних про трудомісткість (табл. 5.1). Результати розрахунків зведені в табл. 5.4.

Додаткову заробітну плату приймаємо рівною 10% від основної заробітної плати. Розрахунок основної та додаткової заробітної плати наведено в табл. 5.5.

Таблиця 5.4 – Розрахунок основної заробітної плати

Посада виконавця	Кіль-кість людей	Місячний оклад, грн	Середньоденна зар. плата, грн.(22 р.дн.)	Кількість робочих днів	Сума зар. плати, грн.
Старший науковий співробітник	1	6000	272,70	40	10908
Молодший науковий співробітник	1	4800	218,18	50	10909
Усього	2	—	—	90	21817

Таблиця 5.5 – Основна та додаткова заробітна плата

Спеціальність виконавця	Додаткова заробітна плата, грн.(10%)	Сума основної та додаткової заробітної плати, грн.
Старший науковий співробітник	1090,8	11998,8
Молодший науковий співробітник	1090,9	11999,9
Усього	2181,7	23998,7

5.3.4 Відрахування на соціальне страхування

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

Таким чином, відрахування на соціальне страхування становить:

$$Відр = (ЗП_{осн} + ЗП_{доп}) \cdot 0{,}22 \quad (5.3)$$

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

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

$$Відр = 23998{,}7 \cdot 0{,}22 = 5279{,}70 \text{ грн.}$$

5.3.5 Загальновиробничі витрати

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

ЗВВ становлять 80% від основної заробітної плати співробітників, що в нашому випадку становить:

НВ=21817·0,8=17453,6 грн

5.3.6 Бальна оцінка економічної ефективності проекту

З метою визначення витрат на реалізацію проекту складено кошторис витрат (табл. 5.6).

Таблиця 5.6 – Кошторис витрат на реалізацію проекту

Статті витрат	Умовне позначення	Сума	
		грн.	частка, %
Матеріали, покупні вироби і напівфабрикати (за відрахуванням відходів, що реалізуються)	М	1399	2,02
Спеціальне устаткування для реалізації проекту	СУ	21000	30,38
Основна і додаткова заробітна плата виробничого персоналу	ЗП	23998,7	34,71
Відрахування на соціальне страхування	ОТЧ	5279,7	7,64
Загально виробничі витрати (ЗВВ)	НВ	17453,6	25,25
Усього витрат на реалізацію проекта	-	69131	100

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

Бальна оцінка проводиться за наступними показниками:

– важливість розробки К1=1, обирається з табл. 5.7;

Таблиця 5.7 – Шкала для оцінки важливості розробки $К_1$

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

- можливість використання результатів розробки $К_2$=8 (табл. 5.8);

Таблиця 5.8 – Шкала оцінки можливості використання результатів розробки $К_2$

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

– теоретична значимість і рівень новизни дослідження $К_3$=2 (табл. 5.9);

Таблиця 5.9 – Шкала оцінки теоретичної значимості й рівня новизни дослідження $К_3$

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

– складність розробки $К_4$=3 (табл. 5.10).

Таблиця 5.10 – Шкала оцінки показників складності дослідження $К_4$

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

Загальна оцінка встановлюється за добутком коефіцієнтів:

$$Пс=К1 \cdot К2 \cdot К3 \cdot К4, \quad (5.4)$$

$$Пс=1 \cdot 8 \cdot 2 \cdot 3=48 \text{ балів.}$$

Питомий ефект на кожний бал (умовно приймаємо) – 2 000 грн.

Загальний ефект від розробки складає:

$$Е=Пс\cdot 2\ 000\cdot К1\cdot К2\cdot К3\cdot К4, \quad (5.5)$$

$$Е=2\ 000\cdot 1\cdot 8\cdot 2\cdot 3=96\ 000 грн.$$

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

$$КВ=Е/Кндр, \quad (5.6)$$

$$КВ=96000/69131=1,38.$$

В даному розділі було проведено аналіз і обґрунтування економічної ефективності науково–дослідницької роботи. Розраховано, що для проведення дослідження необхідно близько 90 днів. При цьому сумарні витрати на дослідження становлять 69131 грн., з них:

– заробітна плата – 23998,7 грн., що становить 34,71% від загальної кількості витрат;

– загальновиробничі витрати – 17453,6 (25,25%);

– спеціальне обладнання для реалізації проекту – 21000грн. (30,38%);

– відрахування на соціальне страхування – 5279,70 (7,64%);

– витратні матеріали, куповані вироби і напівфабрикати - 1399 грн. (2,02%).

Обґрунтованість ефективності дослідження підтверджується розрахованим коефіцієнтом економічної ефективності, який становить норму > 1 (1,38).

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Аналіз потенційних небезпек

Оскільки магістерська робота передбачає роботу у приміщенні, обладнаному персональними комп'ютерами з візуальними дисплейними терміналами, необхідно розглянути заходи щодо забезпечення безпеки, виробничої санітарії, гігієни праці та пожежної безпеки приміщень з персональними комп'ютерами.

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

Потенційні небезпеки фізичного характеру:

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

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

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

Потенційні небезпеки психофізіологічного характеру:

– недотримання режиму роботи за ПК, розумове перенапруження, перенапруження аналізаторів та емоційні перевантаження, що призводять до

підвищення стомлюваності, зниження уваги і, як наслідок, до можливості травмування працівника.

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

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

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

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

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

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

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

Потенційні небезпеки, пов’язані з проявом наслідків надзвичайних ситуацій: отримання травм і матеріальних втрат, через неправильну поведінку персоналу при НС.

До шкідливих виробничих факторів відносяться:

– підвищена або знижена температура, вологість і рухливість повітря;

– підвищена запиленість і загазованість повітря;

– відсутність чи недолік природного світла; недостатня освітленість робочої зони; знижена контрастність об'єктів порівняно з фоном; прямі відблиски (прожекторне освітлення територій виробництв, світло фар автотранспорту) і відображені відблиски (від пролитої води та інших рідин на поверхні територій виробництв);

– підвищена пульсація світлового потоку;

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

6.2 Заходи по забезпеченню техніки безпеки

Під час проектування систем електропостачання, монтажу силового електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог ПВЕ, ПТЕ, ПБЕ, СН 357-77 «Инструкция по проектированию силового осветительного оборудования промышленных предприятий», затверджених Держбудом, ГОСТ 12.1.006, ГОСТ 12.1.030 «ССБТ. Электробезопасность. Защитное заземление, зануление», ГОСТ 12.1.019 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты», ГОСТ 12.1.045, ВСН 59-88 Держкомархітектури «Электрооборудование жилых и общественных зданий. Нормы проектирования», Правил пожежної безпеки в Україні, цих Правил, а також розділів СНиП, що стосуються штучного освітлення та електротехнічних пристроїв та вимог нормативно-технічної і експлуатаційної документації заводу-виробника ЕОМ.

Для виключення ураження електричним струмом передбачено:

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

– технічні заходи: встановлення аварійного резервного вимикачу, який може повністю вимкнути електричне живлення приміщення, окрім освітлення; використовується підключення до мережі пристроїв за допомогою справних штепсельних з’єднань і електророзеток заводського виготовлення; проведено електромережу штепсельних розеток для живлення пристроїв уздовж стін приміщення, по підлозі поряд зі стінами приміщення, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану

розміщення обладнання та технічних характеристик обладнання; відповідність усіх пристроїв вимогам чинних в Україні стандартів, нормативних актів з охорони праці, а також пристрої закордонного виробництва додатково відповідають вимогам національних стандартів держав-виробників і мають відповідну позначку на корпусі, в паспорті або іншій експлуатаційній документації; використання захисного заземлення та занулення згідно «Правил устрою електроустановок» («ПУЕ»).

Для виключення ураження статичним струмом та впливу електромагнітного поля застосовується:

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

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

Загальні заходи з техніки безпеки:

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

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

– дотримання режиму роботи з ПК та іншими приладами.

6.3 Заходи по забезпеченню виробничої санітарії та гігієни праці

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

Приміщення з ВДТ та ПЕОМ обладнані системами опалення, кондиціювання повітря або припливно-витяжною вентиляцією відповідно до СНиП 2.04.05-91 «Отопления, вентиляция и кондиционирование».

Параметри мікроклімату, іонного складу повітря, вміст шкідливих речовин на робочих місцях, оснащених відео терміналами, відповідають вимогам пункту 2.4 СН 4088-86 «Санитарные нормы микроклимата производственных помещений», затверджених Міністерством охорони здоров'я СРСР (табл.6.1), ГОСТ 12.1.005-88 «ССБТ Общие санитарно-гигиенические требования к воздуху рабочей зоны», СН 2152-80 «Санитарно-гигиенические нормы допустимых уровней ионизации воздуха производственных и общественных помещений» (табл.6.2).

Таблиця 6.1 – Норми мікроклімату у приміщенні

Пора року	Категорія робіт згідно ГОСТ 12.1005-88	Температура повітря, град. С	Відносна вологість повітря, %	Шкідливість руху повітря, м/с
		Оптимальна	Оптимальна	Оптимальна
Холодна	легка -1 а	22 - 24	40 - 60	0,1
	легка -1 б	21 - 23	40 - 60	0,1
Тепла	легка -1 а	23 - 25	40 - 60	0,1
	легка -1 б	22 - 24	40 - 60	0,2

Таблиця 6.2 – Рівні іонізації повітря приміщень

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

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

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

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

Площа, виділена для одного робочого місця з відеотерміналом або персональною ЕОМ, повинна складати не менше 6 м2, а обсяг – не менше 20 м3. Робочі місця з відеотерміналами відносно світлових прорізів повинні розміщуватися так, щоб природне світло падало збоку, переважно зліва.

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

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

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

– відстань між тильною поверхнею одного відеотермінала та екраном іншого не повинна бути меншою 2,5 м.

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

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

При розташуванні відеотерміналів ЕОМ за периметром приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями (табл.6.3).

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

Таблиця 6.3 – Норми освітленості в кабінетах і класах з ПК

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

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

– світильники прямого світла – П;

– переважно прямого світла – Н;

– переважно відбитого світла – В.

Приведемо розрахунок штучного освітлення для приміщення, розміри якого: довжина 10м, ширина 6м, висота 3,8м.

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

Розрахунок освітлення методом коефіцієнта використання виконується по формулі:

$$\Phi = \frac{E \cdot S \cdot k \cdot z}{N \cdot \eta}, \tag{6.1}$$

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

E – нормативна мінімальна освітленість, лк;

k – коефіцієнт запасу, вибирається;

S – освітлювана площа, м2;

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

N – число світильників у приміщенні;

η – коефіцієнт використання світлового потоку.

Приймаємо: E =200 лк; k =1,5; z=1,1.

Освітлювана площа приміщення визначається по формулі:

$$S = A \cdot B, \tag{6.2}$$

де S – освітлювана площа;

A – довжина приміщення, м;

B – ширина приміщення, м.

Отримуємо $S=10*6=60$ м^2.

Кількість рядів:

$$Np = \frac{B}{(H-hp)*\lambda} = \frac{6}{(3.8-0.8)*1.4} = 1{,}5 \rightarrow 2 \text{ рядів} \tag{6.3}$$

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

Найбільш вигідне співвідношення відстані між світильниками до розрахункової висоти підвісу:

$$\lambda = \frac{L}{h}, \tag{6.4}$$

Примітка. Приймається по таблиці у залежності від типової кривої сили світла світильника. Для люмінесцентних ламп при косинусоїдальному типові кривої вибираємо λ = 1,4.

Знаходимо розрахункову висоту підвісу по наступній формулі:

$$h = H - h_{\_‰} - h_p, \tag{6.5}$$

де H – висота приміщення, м;

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

h_p – висота робочої поверхні над підлогою, м.

Приймаємо: H=3,8 м, h_p =0,8 м.

Відстань між світильниками визначаємо з формули (6.5):

$$L = \frac{B}{Np} \tag{6.6}$$

$$L = \frac{6}{2} = 3 \text{ м.}$$

Визначаємо кількість світильників для установки в приміщенні:

$$N = \frac{S}{L^2}, \tag{6.7}$$

$$N = \frac{60}{3^2} = 6{,}66 \approx 8 \text{ шт.}$$

Для визначення коефіцієнта використання η знаходимо індекс приміщення i:

$$i = \frac{A \cdot B}{h \cdot (A + B)}, \tag{6.8}$$

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

h – розрахункова висота підвісу, м.

Отримуємо:

$$i = \frac{10 * 6}{3 * (10 + 6)} = 1{,}25$$

Отримане значення i округляємо до найближчого табличного значення і приймаємо i = 1,25.

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

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

Вибираємо світильник типу ПВЛМ-Д, для якого η =49%. По формулі (6.1) визначаємо необхідний світловий потік ламп у кожнім світильнику:

$$\Phi = \frac{200 * 60 * 1{,}5 * 1{,}1}{8 * 2 * 0{,}49} = 2525{,}51 \text{ лм.}$$

З довідкової літератури вибираємо необхідну лампу. Тип обраної лампи – ЛБ 40-4, Ф=2850 лм, які розміщені в два ряди. У приміщенні встановлюємо 8 світильники по 2 лампі у кожному.

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

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

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

– застосуванням звукоізолюючих пристроїв для ізоляції шумних агрегатів;

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

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

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

Потужність експозиційної дози рентгенівського випромінювання на відстані 0,05 м від екрана та корпуса відеотермінала при будь-яких положеннях регулювальних пристроїв відповідно до Норм радіаційної безпеки України (НРБУ-97), затверджених постановою державного санітарного лікаря Міністерства охорони здоров'я України від 18.08.97 № 58, не повинна перевищувати 7,74×10~12 А/кГ, що відповідає еквівалентній дозі 0,1 мбер/год. (100 мкР/год.).

6.4 Заходи з пожежної безпеки

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

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

Відповідальність за прийняття протипожежних заходів в організаціях покладається персонально на їх керівників без права передовіряти цю відповідальність іншим, підлеглим їм особам, вони здійснюють загальне керівництво роботою в галузі пожежної безпеки підприємств і організацій.

На підприємстві встановлюються первинні засоби пожежогасіння відповідно до вимог Правил пожежної безпеки України. У приміщеннях з комп'ютерами використовуємо системи автоматичної пожежної сигналізації для виявлення пожежі та оповіщення працівників. Для приміщення, по якому проводиться розрахунок, влаштовуємо місця утримання засобів пожежогасіння

вогнегасників порошкових типу ОПУ–5 з вільним доступом у випадку необхідності їх використання.

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

Для даного класу пожежі підходять декілька типів вогнегасників, такі як: порошкові, хладонові та вуглекислі вогнегасники. Використовуючи ці дані згідно з НАПБ Б.03.001-2004 «Типові норми належності вогнегасників» і так як площа приміщення складає 60 м^2 достатньо двох порошкових вогнегасників об’ємом 5 літрів.

6.5 Заходи безпеки у надзвичайних ситуаціях

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

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

– евакуацію населення із зон НС;

– використання засобів індивідуального захисту органів дихання та шкірних покровів;

– проведення заходів медичного захисту;

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

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

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

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

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

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

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

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

Проведення заходів медичного захисту. Заходи медичного захисту населення при НС слід проводити з метою запобігання або зниження тяжкості

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

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

Першу медичну допомогу потерпілим до їх евакуації в лікувальні установи надають безпосередньо в осередках ураження в ході рятувальних та інших невідкладних робіт. Надання цієї допомоги слід здійснювати за участю заздалегідь сформованих для такої мети з самого населення санітарних постів і санітарних дружин, до складу яких слід включати осіб, спеціально навчених загальним прийомам надання само- і взаємодопомоги і здатних організувати практичне виконання населенням цих прийомів в екстремальних умовах.

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

Проведення аварійно-рятувальних та інших невідкладних робіт у зонах НС. Аварійно-рятувальні та інші невідкладні роботи в зонах НС слід проводити з

метою термінового надання допомоги населенню, яке піддалося безпосереднього або опосередкованого впливу руйнівних і шкідливих сил природи, техногенних аварій та катастроф, а також для обмеження масштабів, локалізації або ліквідації виниклих при цьому НС.

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

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

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

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

Завчасна підготовка і введення в дію планів захисту населення в НС, зумовлених природними стихійними лихами, техногенними аваріями, катастрофами, а також застосуванням сучасної зброї, повинні передбачати

проведення узгоджених за часом, цілям і засобам робіт з планування і здійснення комплексу організаційних, інженерно-технічних і спеціальних заходів цивільної оборони, а також формування необхідних для цього сил і засобів.

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

ВИСНОВКИ

У магістерській роботі були проаналізовані основні фактори завад по бездротовим мережам в умовах аеропорту в мережевому симуляторі OPNET.

Сценарій 1: в цій симуляції було представлено рухому атаку зловмисника або терориста на мережу аеропорту, та було виявлено що мережа на деяких схемах модуляції є більш стійкою до постійних завад, які випромінює глушилка в межах аеропорту; MSK продемонстрував себе як найбільш стійкою схемою модуляції до завад, тоді як 64-QAM був тим, хто надав менший опір. Тому краще за все використовувати qpsk, bpsk, gmsk, msk та cck як методи модуляції мережі в аеропорту.

У Сценарії 2 було продемонстровано, що завади можуть тримати канал зайнятим та знижувати пропускну здатність до нуля; він також продемонстрував ступінь тяжкості атаки завадами – у цьому випадку вузли взагалі не змогли спілкуватися. В симуляції представлено спрямовану атаку зловмисника або терориста на AP мережі аеропорту. Також симуляцію можна представити в вигляді нестандартної спрямованої перешкоди від не санкціонованої апаратури та антен аеропорту. Для запобігання цих проблем потрібно більше приділяти уваги охороні основних точок доступу до мережі, та наймати на роботу професійних системних адміністраторі та охоронців, а також професійного менеджера з кібербезпеки.

У Сценарії 3 було введено імпульсний джамер для імітації випадкової атаки завадами. Це продемонструвало, що хоча трафік не падає до нуля, він все ще має великий вплив на загальну пропускну здатність. В симуляції представлено випадкову атаку перешкодами на мережу Wi-Fi аеропорту, спричиненими технікою та спеціальною апаратурою аеропорту. Для боротьби з цими завадами потрібно екранувати термінали аеропорту, для захисту мережі Wi-Fi від випадкових завад.

У Сценарії 4 була встановлена спеціальна мережа з постійним завадами в середині сценарію. В симуляції представлено атаку перешкод на мережу Wi-Fi,

яка знаходиться на території аеропорту. За перешкоду представляємо літак, а також можна представити за перешкоду завади від вишки аеропорту. Сценарій продемонстрував, що не можна зробити всю мережу непрацюючої з огляду на особливі властивості спеціальних мереж; вони прагнуть шукати нові маршрути, коли виникає збій у мережі. Тому на території аеропорту необхідно планувати мережу Wi-Fi з нелінійною архітектурою.

Сценарій 5 продемонстрував, що несправний вузол, може також діяти як завада, коли не відповідає протоколу MAC, але це не так критично, якщо є альтернативні вузли для передачі інформації. Тому в аеропорті потрібно завжди мати альтернативні методи передачі, тобто мати альтернативні вузли для передачі.

Дотримуючись даних рекомендацій можна значно підвищити завадостійкість мережі Wi-Fi в аеропорті, а також підвищити безпеку мережі від зловмисників та терористів, а стандарту 802.11g достатньо для функціювання мережі.

OPNET продемонстрував, що є потужним інструментом моделювання, який легко дозволяє моделювати різного роду бездротові мережі; він, безумовно, також підходить для імітації різних видів шумів та завад. У ньому є багато вбудованих моделей для імітації: глушилок, оманливих глушилок, випадкових завад не тільки для бездротових вузлів, але і для супутникового зв'язку. Однак OPNET як інструмент не є ідеальним, йому не вистачає певної гнучкості; наприклад, коли є потреба у створенні нового виду завад або в зміні коду деяких функції, модулів, характеристики, що доволі складно.

OPNET запропонував можливість автоматичного збору статистичних даних та їх відповідності в графіках. У цьому аспекті його ефективність досить хороша, але важливим недоліком є те, що якщо користувач хоче виміряти аспект мережі, який не входить до списку речей OPNET, буває дуже складно це зробити, а інколи не можливо виміряти. OPNET пропонує багато деталей та моделей, але це також призводить до повільних моделювань.

ПЕРЕЛІК ПОСИЛАНЬ

1. Беспроводные сети WI-FI. – М.: Интернет – университет информационных технологий, Бином. Лаборатория знаний, 2013. – 216 с.

2. Брэгг, Р. Безопасность сетей: полное руководство [Текст] / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М.: Эком, 2015. – 912 с.

3. Ватаманюк, А. И. Беспроводная сеть своими руками [Текст] / А.И. Ватаманюк. – М.: Книга по Требованию, 2011. – 194 с.

4. Гайер, Дж. Беспроводная сеть за 5 минут. От выбора оборудования до устранения любых неполадок [Текст] / Дж. Гайер, Э. Гайер, Дж.Р. Кинг. – М.: НТ Пресс, 2012. – 176 с.

5. Гайер, Дж. Беспроводные сети. Установка и устранение неполадок за 5 минут [Текст] / Дж. Гайер, Э. Гайер, Дж.Р. Кинг. – М.: НТ Пресс, 2015. – 176 с.

6. Колисниченко, Д. Беспроводная сеть дома и в офисе [Текст] / Д. Колисниченко. – М.: БХВ – Петербург, 2015. – 997 с.

7. Кюнель Samba: интеграция Linux/Unix– компьютеров в сети Windows [Текст] / Кюнель, Йенц. – М.: Мн: Новое знание, 2012. – 399 с.

8. Майника, Э. Алгоритмы оптимизации на сетях и графах [Текст] / Э. Майника. – М., 2012. – 334 с.

9. Мерритт, М. Безопасность беспроводных сетей [Текст] / М. Мерритт. – М.: Книга по Требованию, 2015. – 282 с.

10. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов [Текст] / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – Санкт-Петербург : «Питер», 2014. –944 с.

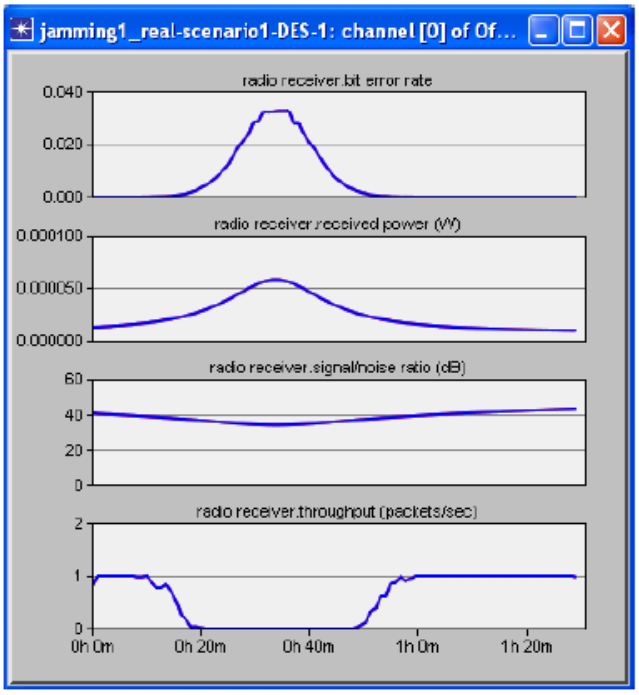
11. Радке, Хорст Дитер. Wireless Law Easy [Текст] / Хорст Дитер Радке, Йеремиас Радке.– изд-во: НТ Пресс, 2014, 320 с.

12. Семенов, Ю.А. Протоколы и ресурсы Интернет [Текст] / Ю.А. Семенов. – М.: Радио и связь, 2011. – 320 с.

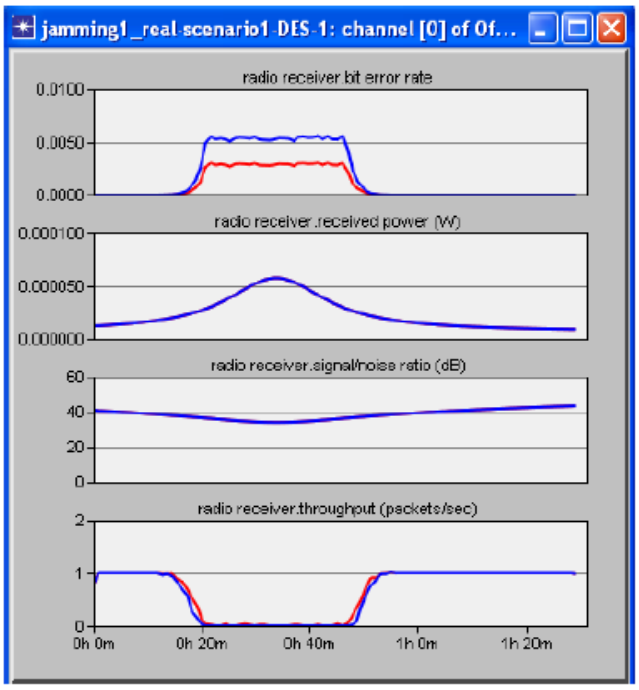
13. Тарасов, В.Н. Проектирование и моделирование сетей ЭВМ в системе OPNET Modeler [Текст] / В.Н. Тарасов. – Самара, 2008.

14. Лоу, А.М. Имитационное моделирование. Классика CS [Текст] / А.М. Лоу, В.Д. Кельтон – 3-е изд. – Санкт-Петербург: Питер; Киев: Издательская группа BHV, 2005. – 847 с.

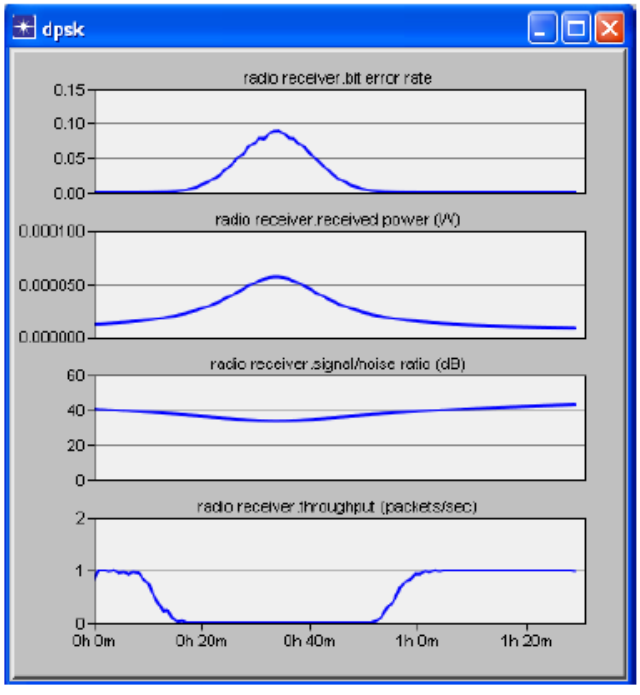
ДОДАДОК А



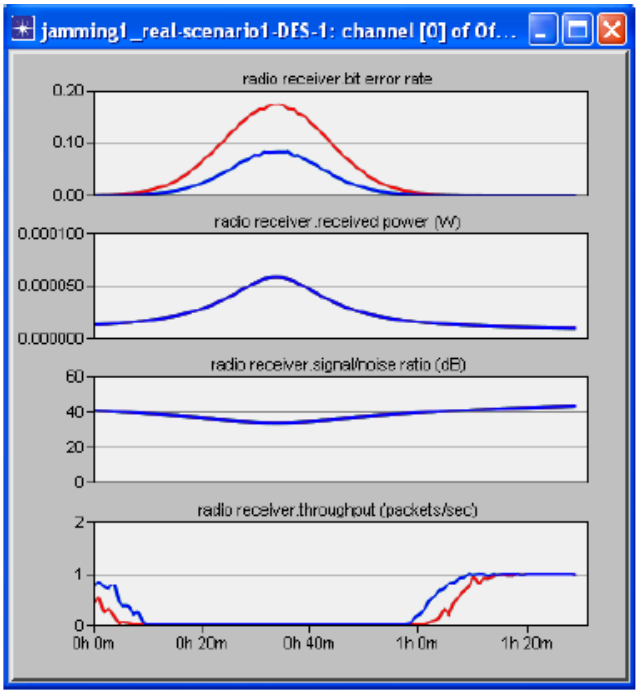
Bpsk



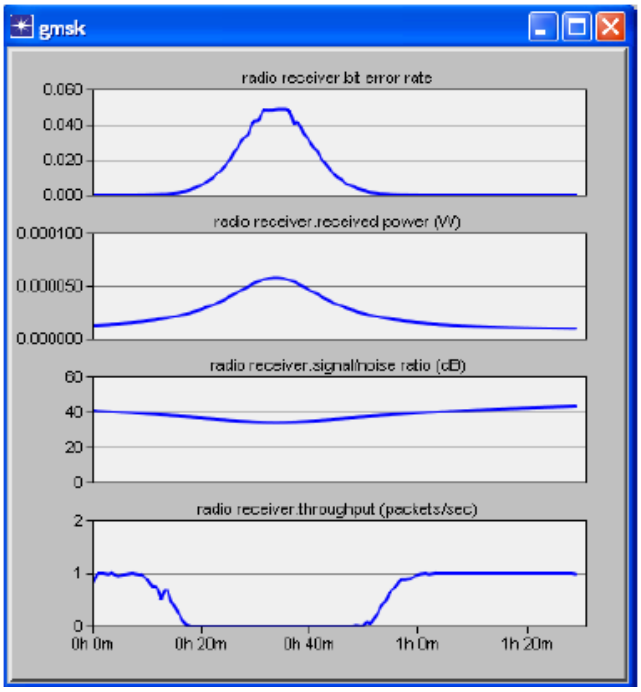
Cck11 синім кольором, cck55 червоним кольором



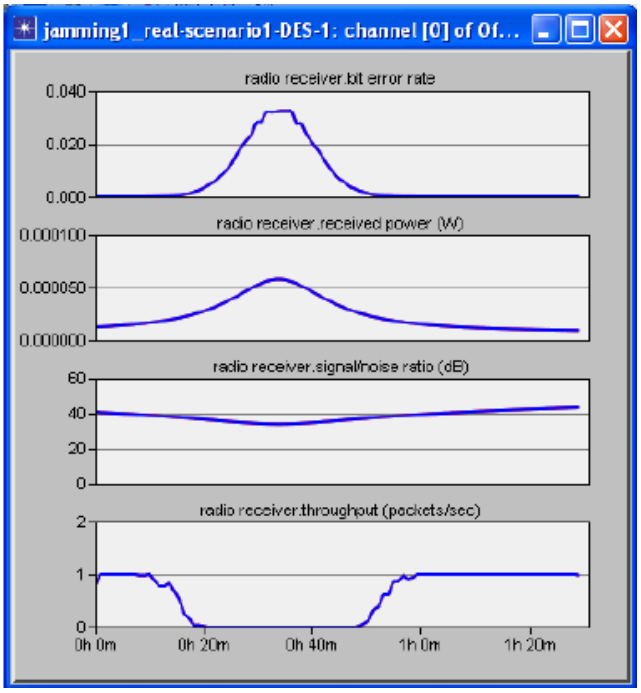
Dpsk



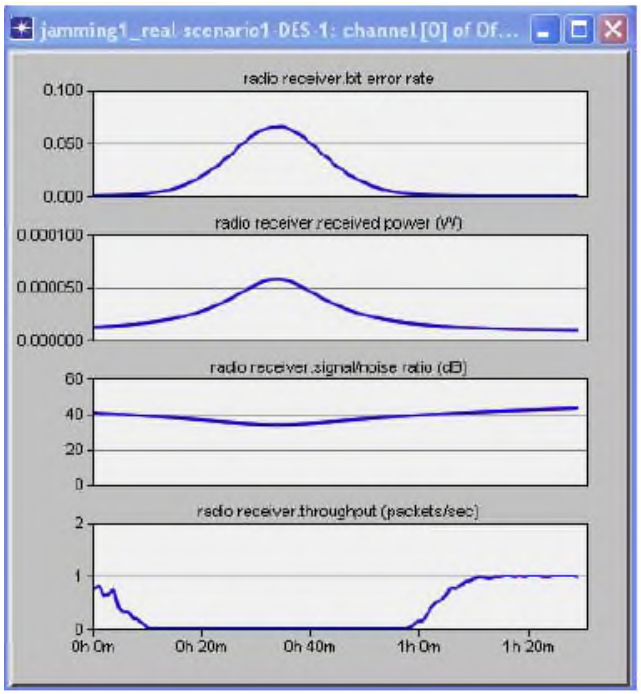
Fsk2 синім кольором, fsk2_ncoh червоним кольором.



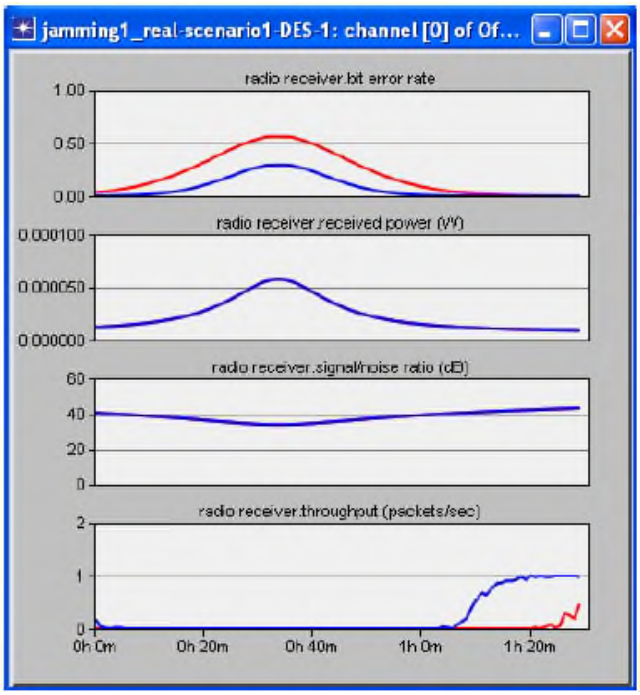
Gmsk



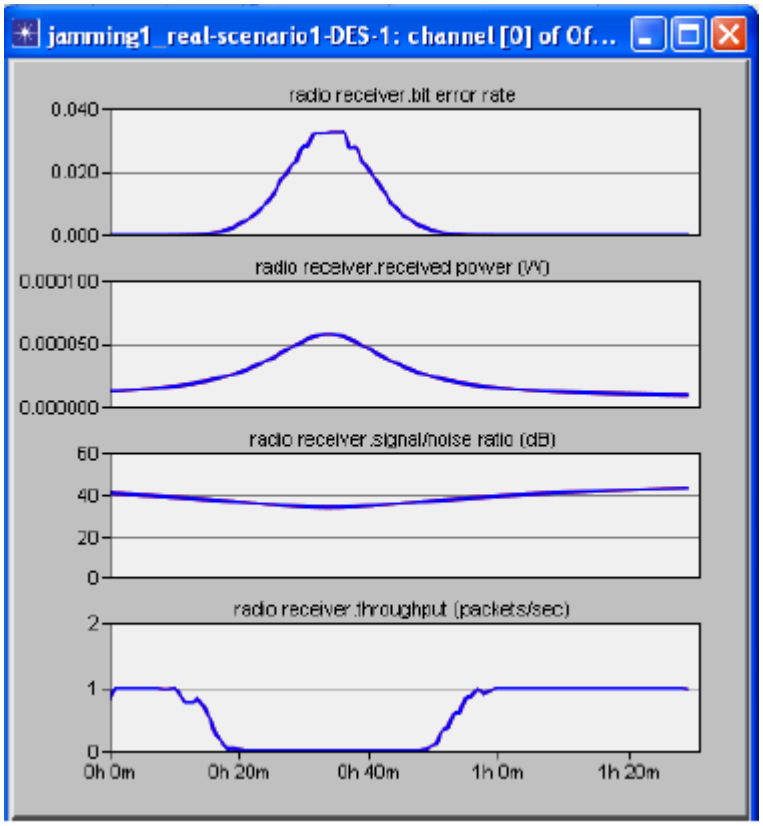
Msk у синьому кольорі та msk_pch у червоному кольорі.



Psk8



Qam16 синього кольору та Qam64 червоного кольору


jamming1_real-scenario1-DES-1: channel [0] of Of...
radio receiver.bit error rate
0.040
0.020
0.000
radio receiver.received power (W)
0.000100
0.000050
0.000000
radio receiver.signal/noise ratio (dB)
60
40
20
0
radio receiver.throughput (packets/sec)
2
1
0
0h 0m
0h 20m
0h 40m
1h 0m
1h 20m

Qpsk

ДОДАТОК Б

Init:

```
/* The initialization of this process model relies on */
/* the completion of initialization of lower layers. */
if (lower_layer_init_intrpt_count < GNAC_LOWER_LAYER_INIT_INTRPT_COUNT)
{
/* Schedule a self-interrupt to allow lower layers */
/* to be configured. */
evh = op_intrpt_schedule_self (0.0, GNAC_LOWER_LAYER_INIT_WAIT);
/* Generate error if the lower layer synchronization event */
/* event not be scheduled. */
if (op_ev_valid (evh) == OPC_FALSE)
gna_clsvr_mgr_error ("Unable to schedule self interrupt to wait for lower layer initialization.");
/* Increment the count of initialization interrupts */
/* observed. */
lower_layer_init_intrpt_count++;
}
else
{
/* Schedule an interrupt to move on to performing */
/* its own initialization. */
evh = op_intrpt_schedule_self (op_sim_time (), GNAC_SELF_INIT_START);
/* Generate error if the lower layer synchronization event */
/* event not be scheduled. */
if (op_ev_valid (evh) == OPC_FALSE)
gna_clsvr_mgr_error ("Unable to schedule self interrupt to initialize itself.");
/* Initialize the index used of identifying custom managers */
global_custom_mgr_index = 0;
}
```

Generate:

```
/* At the enter execs of the "generate" state we schedule the */
/* arrival of the next packet. */
next_intarr_time = oms_dist_outcome (interarrival_dist_ptr);
```

```
/* Make sure that interarrival time is not negative. In that case it */
/* will be set to 0. */
if (next_intarr_time <0)
{
next_intarr_time = 0;
}
next_pk_evh = op_intrpt_schedule_self (op_sim_time () + next_intarr_time, SSC_GENERATE);
```

Wait:

```
/** The server process can be operating in two modes, depending on **/
/** whether it supports the Custom MTA service. **/
/** 1. Support MTA: In this mode, it can be acting as a server (to **/
/** model remote client to server transactions) or as a client **/
/** session manager to to manage spawned client processes which **/
/** communicate with other servers. **/
/** 2. Does not support MTA: Only acts as server. Here it just **/
/** provides service back to the source end clients. There **/
/** exists session for each of the remote clients. **/
/* Get the current simulation time */
current_sim_time = op_sim_time ();
/* Check for an ODB trace label. */
trace_active = op_prg_odb_ltrace_active ("gna") || op_prg_odb_ltrace_active ("client_server");
trace_arch_active = op_prg_odb_ltrace_active ("gna_arch");
/* Get interrupt parameters. */
intrpt_type = op_intrpt_type ();
if (intrpt_type != OPC_INTRPT_STRM)
{
intrpt_code = op_intrpt_code ();
}
else
{
intrpt_code = NASC_INVALID;
}
/* We want to go to Arrival state from Wait state in all cases */
/* except when this a video or voice session. */
```

```
Wait_To_Arrival = OPC_TRUE;
switch (intrpt_type)
{
case OPC_INTRPT_PROCESS:
case OPC_INTRPT_SELF:
case OPC_INTRPT_ENDSIM:
/* Do nothing. */
break;
case OPC_INTRPT_REMOTE:
case OPC_INTRPT_STRM:
{
/* Extract the session information from this interrupt. */
/* The lower layer (or a client process spawned by this */
/* server) installs this information in the ICI */
/* associated with this interrupt. */
ici_ptr = op_intrpt_ici ();
if ( sip_intrpt_is_for_sip (ici_ptr) == OPC_TRUE)
{
/* Redirect the interrupt to the SIP process */
sip_redirect_intrpt_to_sip (ici_ptr);
/* Reset the interrupt codes to avoid any */
/* transition condition errors. */
intrpt_type = NASC_INVALID;
intrpt_code = NASC_INVALID;
}
else if ( gna_sup_intrpt_is_for_sup (ici_ptr) == OPC_TRUE)
{
/* Redirect the interrupt to the SIP process */
gna_sup_redirect_intrpt_to_dest_proc (ici_ptr);
/* Reset the interrupt codes to avoid any */
/* transition condition errors. */
intrpt_type = NASC_INVALID;
intrpt_code = NASC_INVALID;
}
else if ( traf_engine_intrpt_is_for_traf_engine (ici_ptr) == OPC_TRUE)
```

```
{
/* Redirect the interrupt to the SIP process */
traf_engine_redirect_intrpt_to_traf_engine (ici_ptr);
/* Reset the interrupt codes to avoid any */
/* transition condition errors. */
intrpt_type = NASC_INVALID;
intrpt_code = NASC_INVALID;
}
else if (is_intrpt_for_remote_storage_access (ici_ptr) == OPC_TRUE)
{
/* interrupt to be handled by either the remote storage access */
/* server or client. */
redirect_intrpt_to_remote_storage_access (rsa_mgr_prohndl, ici_ptr);
/* Reset the intrpt type and code to indicate that this intrpt */
/* has been handled. No more processing required. */
intrpt_type = NASC_INVALID;
intrpt_code = NASC_INVALID;
}
else
{
if ((ici_ptr == OPC_NIL) ||
(op_ici_attr_get (ici_ptr, "Application ID", &sess_ptr) == OPC_COMPCODE_FAILURE) ||
(op_ici_attr_get (ici_ptr, "Sess Type", &sess_type) == OPC_COMPCODE_FAILURE) ||
(op_ici_attr_get (ici_ptr, "Application Type", &app_type) == OPC_COMPCODE_FAILURE))
{
gna_clsvr_mgr_error ("Unable to get session information from ICI.");
}
/* Check if this interrupt is for the case when this */
/* server process is acting as the manager for spawned */
/* client processes (to talk to other client/server */
/* processes) */
if (((sess_type == GNAC_SESSION_TYPE_ACTIVE)) ||
((app_type == GnaC_App_Type_Video_Conferencing) && (intrpt_code !=
TPALC_EV_IND_OPEN)) ||
((app_type == GnaC_App_Type_Voice) && (intrpt_code != TPALC_EV_IND_OPEN)) ||
```

```
(app_type == GnaC_App_Type_Ace))
{
/* Even when the server is acting as the manager, */
/* it handles two cases where the interrupt is for */
/* itself (i.e., the server): */
/* 1. A session termination (this interrupt is */
/* scheduled by the managed client.) */
/* 2. Modeling request time delay (again this is */
/* scheduled by the managed client) -- this */
/* facilitates modeling of the server busy */
/* condition for modelign the request delays. */
if ((intrpt_code == GNAC_IND_SESS_OPEN_FAILED) || (intrpt_code ==
GNAC_IND_SESS_CLOSED)
|| (intrpt_code == GNAC_MODEL_REQUEST_TIME))
{
/* Do nothing. The transition conditions will */
/* figure out how to transition. */
cli_sess_ptr = (GnaT_Cli_Mgr_Session *) sess_ptr;
}
else
{
/* Invoke the session process using the process */
/* handle from the session record. */
cli_sess_ptr = (GnaT_Cli_Mgr_Session *) sess_ptr;
/* Check whether the client process is still alive. */
if (cli_sess_ptr != OPC_NIL)
{
if (op_pro_valid (cli_sess_ptr->prohndl) == OPC_TRUE)
{
if (op_pro_invoke (cli_sess_ptr->prohndl, OPC_NIL) == OPC_COMPCODE_FAILURE)
{
gna_clsvr_mgr_error ("Could not invoke session process to handle received interrupt.");
}
}
}
```

```
else
{
/* Process model doesn't exist any more. */
if (intrpt_type == OPC_INTRPT_STRM)
{
/* If interrupt is stream interrupt, destroy packet. */
op_pk_destroy (op_pk_get (op_intrpt_strm ()));
}
}
/* Reset the interrupt codes to avoid any */
/* transition condition errors. */
intrpt_type = NASC_INVALID;
intrpt_code = NASC_INVALID;
}
}
/* If this is a video or voice session, do not go into arrival */
/* state. */
if ((app_type == GnaC_App_Type_Video_Conferencing) ||
(app_type == GnaC_App_Type_Voice))
{
Wait_To_Arrival = OPC_FALSE;
}
}
break;
}
default:
{
gna_clsvr_mgr_error ("Received unexpected interrupt in wait state.");
break;
}
}
```