НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп‘ютерних систем

«До захисту допущено»
Завідувач кафедри
_____ В.П. Тарасенко
«___»_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.050102 «Комп'ютерна інженерія»

на тему: «Комп’ютерна мережа технології LTE-A»

Виконала:
студентка IV курсу, групи КВ-51
Курій Катерина Андріївна _____

Керівник:
Доцент кафедри СПСКС, к.т.н., доцент,
Орлова М.М. _____

Консультант з нормоконтролю:
Доцент кафедри СПСКС, к.т.н., доцент,
Клятченко Я.М. _____

Рецензент:
Професор каф. ОТ, д.т.н., проф.,
Ю.О.Кулаков _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студентка _____

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут» імені Ігоря Сікорського

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп‘ютерних систем

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки **6.050102 «Комп'ютерна інженерія»**

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Тарасенко В.П.
(підпис) (ініціали, прізвище)
«___»_____201_ р.

ЗАВДАННЯ
на дипломний проект студентці
Курій Катерині Андріївні

1. Тема проекту «Комп’ютерна мережа технології LTE-A», керівник проекту Орлова Марія Миколаївна, старший викладач, затверджені наказом по університету від «__»_____ 201_ р. №____

2. Термін подання студентом проекту 6 червня 2019 р.

3. Вихідні дані до проекту: див. Технічне завдання.

4. Зміст пояснювальної записки
- аналіз існуючих рішень та обгрунтування теми бакалаврського проекту;
- розробка структури безпроводової комп’ютерної мережі;
- алгоритми захисту та передачі інформації;
- опис розробленого програмного продукту.

5. Перелік графічного матеріалу (із зазначенням обов’язкових креслеників, плакатів, презентацій тощо)
- Структура мережі. Схема структурна.
- Алгоритм шифрування. Схема алгоритму.
- Алгоритм цілісності. Схема алгоритму.
- Алгоритм роботи програми. Схема структурна.
- Презентація за темою роботи.

6. Консультанти розділів проекту*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Клятченко Я.М., доцент		

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломного проекту	Термін виконання етапів проекту	Примітка
1.	Вивчення літератури за тематикою проекту	15.11.2018	
2.	Розроблення та узгодження технічного завдання	30.11.2018	
3.	Аналіз існуючих рішень	05.02.2019	
4.	Підготовка матеріалів першого розділу дипломного проекту	05.05.2019	
5.	Підготовка матеріалів другого розділу дипломного проекту	07.05.2019	
6.	Підготовка матеріалів третього розділу дипломного проекту	10.05.2019	
7.	Підготовка матеріалів четвертого розділу дипломного проекту	14.05.2019	
8.	Підготовка графічної частини дипломного проекту	20.05.2019	
9.	Оформлення документації дипломного проекту	23.05.2019	
10.	Попередній огляд матеріалів диплому на кафедрі	27.05.2019	

Студент _____ Курій К.А.
(підпис)

Керівник проекту _____ Орлова М.М.
(підпис)

_____

АНОТАЦІЯ

Кваліфікаційна робота включає пояснювальну записку (55 с., 28 рис., 4 додатки).

Об’єкт розробки – аналіз особливостей побудови безпроводових комп`ютерних мереж технології LTE-A та розробка на цій основі структури безпроводової мережі, яка дозволяє виконувати обмін повідомленнями в захищеному режимі.

Розроблена безпроводова мережа дозволяє:

- зареєструватись та авторизуватись за допомогою логіну та паролю;
- надсилати повідомлення іншим користувачам мережі;
- переглядати повідомлення, які були отримані від інших користувачів.

В розробці передбачені механізми захисту цілісності інформації, а також її шифрування. В процесі розробки була використана мова програмування C# з використанням фреймворку .NET та середовище розробки VisualStudio. Для роботи з базою даних використовувалась SQL.

В ході виконання дипломного проекту:

- проведено аналіз існуючих рішень розробки безпроводових мереж;
- розроблено архітектуру мережі;
- розроблено структуру бази даних для зберігання інформації;
- реалізовано алгоритми захищеного обміну повідомленнями та процес авторизаціїї в мережі.

Дана розробка є результатом дослідження та аналізу принципів побудови безпроводових мереж, алгоритмів захисту інформації та аутентифікації користувачів, а також дозволяє проаналізувати та дослідити їх ефективність та способи реалізації.

Ключові слова:

безпроводова мережа, авторизація, шифрування, цілісність інформації, технологія LTE-A, Visual Studio, SQL, C#, .NET.

SUMMARY

The qualifying work includes an explanatory note (55 p., 28 figures, 4 annexes).

The object of the development - an analysis of the peculiarities of the construction of LTE-A wireless computer networks and the development on this basis of a wireless network structure that allows secure messaging.

The developed wireless network allows:

- register and authorize with login and password;
- send messages to other users of the network;
- View messages received from other users.

The design provides mechanisms for protecting the integrity of information, as well as its encryption. In the development process, the C # programming language was used using the .NET framework and the VisualStudio development environment. To work with the database, SQL was used.

During the course of the diploma project:

- analysis of existing solutions for the development of wireless networks;
- the architecture of the network is developed;
- the structure of the database for storing information is developed;
- implemented secure messaging algorithms and authorization process on the network.

This development is the result of research and analysis of the principles of building wireless networks, information security algorithms and user authentication, as well as analyzing and exploring their effectiveness and implementation methods.

Keywords:

wireless network, authorization, encryption, integrity of information, LTE-A technology, Visual Studio, SQL, C #, .NET.

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
			Документація загальна			
			Новорозроблена			
	А4	ІАЛЦ. 467100.002 ТЗ	Комп’ютерна мережа	4		
			технології LTE-A.			
			Технічне завдання			
	А4	ІАЛЦ. 467100.003 ТП	Комп’ютерна мережа	2		
			технології LTE-A.			
			Відомість технічного			
			проекту			
	А4	ІАЛЦ. 467100.004 ПЗ	Комп’ютерна мережа	55		
			технології LTE-A.			
			Пояснювальна записка			
	А4	ІАЛЦ. 467100.005 Д1	Комп’ютерна мережа	1		
			технології LTE-A.			
			Схема мережі.			
			Схема структурна			
	А4	ІАЛЦ. 467100.006 Д2	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм шифрування.			
			Схема алгоритму			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ. 467100.001 ОА		
Розробив		Курій К.А.			Комп’ютерна мережа технології LTE-A. Опис альбому	Літ.	Аркуш 1 / Аркушів 2
Перевірив		Орлова М.М.					
Н. контроль		Клятченко Я.М.				КПІ ім. Сікорського, ФПМ, КВ-51	
Затвердив		Тарасенко В.П.					

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
	А4	ІАЛЦ. 467100.007 Д3	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм цілісності.			
			Схема алгоритму			
	А4	ІАЛЦ. 467100.008 Д4	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм роботи			
			програми.			
			Схема структурна			
		Диск CD-ROM	Вміст пояснювальної	1		
			записки.			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ. 467100.001 ОА	Арк. 2

Зміст

					ІАЛЦ.467100.002 ТЗ		
Зм.	Арк.	№ докум.	Підп.	Дата			
Розроб.		Курій К.А.			Комп’ютерна мережа технології LTE-A Технічне завдання	Літ.	Аркуш 1 / Аркушів 4
Перевір.		Орлова М.М.					
Н. контр.		Клятченко Я.М.				КПІ ім. Ігоря Сікорського, ФПМ, КВ-51	
Затв.		Тарасенко В.П.					

1. НАЙМЕНУВАННЯ І ОБЛАСТЬ ЗАСТОСУВАННЯ

Найменування роботи – «Комп’ютерна мережа технології LTE-A».

Область застосування: інформаційні технології, телекомунікаційні технології, передача інформації.

2. ПІДСТАВА ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання першого (бакалаврського) рівня вищої освіти, затверджене кафедрою системного програмування і спеціалізованих комп’ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

3. ЦІЛЬ І ПРИЗНАЧЕННЯ РОБОТИ

Метою даного проекту є розробка структури безпроводової мережі, яка забезпечує цілісну передачу повідомлень та їх шифрування на основі алгоритмів технології LTE-A.

4. ДЖЕРЕЛА РОБОТИ

Джерелами інформації для розроблення є технічна література, публікації у періодичних виданнях та Інтернет ресурси з питань розробки безпроводових мереж технології LTE-A.

5. ТЕХНІЧНІ ВИМОГИ

5.1. Вимоги до програмного продукту, що розробляється**:**

- підтримка авторизації за допомогою логіну та паролю;
- можливість реєстрації в мережі;
- можливість пошуку інших користувачів за їх номером;
- відправка повідомлення іншим користувачам;
- отримання повідомлень від інших користувачів мережі;
- отримання сповіщень про помилки.

5.2. Вимоги до апаратного забезпечення

- Процесор: 2 - 4-ядерний, MediaTek, Snapdragon, Kirin, Intel Atom;
- Оперативна пам’ять: 2 Гб.

5.3. Вимоги до мінімального програмного забезпечення

- Операційна система Windows, Linux;
- SQL сервер;
- Visual Studio.

6. ЕТАПИ РОЗРОБКИ

№ з/п	Назва етапів виконання дипломного проекту	Термін виконання етапів
1.	Вивчення літератури за тематикою проекту	15.11.2018
2.	Розроблення та узгодження технічного завдання	30.11.2018
3.	Аналіз існуючих рішень	05.02.2019
4.	Підготовка матеріалів першого розділу дипломного проекту	05.05.2019
5.	Підготовка матеріалів другого розділу дипломного проекту	07.05.2019

6.	Підготовка матеріалів третього розділу дипломного проекту	10.05.2019
7.	Підготовка матеріалів четвертого розділу дипломного проекту	14.05.2019
8.	Підготовка графічної частини дипломного проекту	20.05.2019
9.	Оформлення документації дипломного проекту	23.05.2019
10.	Попередній огляд матеріалів диплому на кафедрі	27.05.2019

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
	А4	ІАЛЦ. 467100.004 ПЗ	Комп’ютерна мережа	55		
			технології LTE-A.			
			Пояснювальна записка			
	А4	ІАЛЦ. 467100.005 Д1	Комп’ютерна мережа	1		
			технології LTE-A.			
			Схема мережі.			
			Схема структурна			
	А4	ІАЛЦ. 467100.006 Д1	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм шифрування.			
			Схема алгоритму			
	А4	ІАЛЦ. 467100.007 Д1	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм цілісності.			
			Схема алгоритму			
	А4	ІАЛЦ. 467100.008 Д1	Комп’ютерна мережа	1		
			технології LTE-A.			
			Алгоритм роботи			
			програми.			
			Схема структурна			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ. 467100.003 ВП		
Розробив		Курій К.А.			Комп’ютерна мережа технології LTE-A. Опис альбому	Літ.	Аркуш 1 / Аркушів 2
Перевірив		Орлова М.М.					
Н. контроль		Клятченко Я.М.				КПІ ім. Сікорського, ФПМ, КВ-51	
Затвердив		Тарасенко В.П.					

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
		Диск CD-ROM	Вміст пояснювальної	1		
			записки.			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ. 467100.003 ОА	Арк. 2

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

Авторизація	-	керування рівнями та засобами доступу до певного захищеного ресурсу.
БС	-	базова станція.
Безпроводова мережа	-	тип комп'ютерної мережі, яка використовує бездротове з'єднання для передачі даних й підключення до мережевих вузлів.
ПВП	-	псевдовипадкова послідовність.
AMF	-	Authentification Managemeent Field, аутентифікація керуючого поля.
CDMA	-	Code Division Multiple Access, кодовий роздільний доступ.
CSFB	-	Circuit-switched fallback, резервне перемикання ланцюга.
E-UTRAN	-	Evolved Universal Terrestrial Radio Access Network, універсальна мережа наземного радіодоступу.
ETSI	-	Universal Mobil Telecommunications Standards Institute, Інститут стандартів універсальних мобільних телекомунікацій.
FDD	-	Frequency Division Duplex, дуплексний розподіл частот.
FDMA	-	Frequency Division Multiple Access, частотний розподіл множинного доступу.
G	-	Generation, покоління.
GPRS	-	General Packet Radio Service, загальна послуга пакетної радіозв'язку.
GSM	-	Global System for Mobile communications, глобальна

система мобільного зв'язку.

3GPP	-	3rd Generation Partnership Project, партнерська асоціація груп телекомунікаційних компаній.
HSCSD	-	High Speed Circuit Switched Data, дані високошвидкісного комутації.
HSPA	-	High Speed Packet Access, високошвидкісний пакетний доступ.
HSS	-	Home Subscriber Server, сервер абонентських даних мережі мобільного зв'язку стандарту LTE.
IMT-Advanced	-	International Mobile Telecommunications Advanced, міжнародний мобільний зв'язок.
LTE	-	Long-Term Evolution, назва мобільного протоколу передавання даних.
LTE-A	-	LTE Advanced, стандарт мобільного зв'язку.
MIMO	-	Multiple Input/Multiple Output, множинний ввів/ множинний вивід.
MME	-	Mobility Management Entity, суб'єкт управління мобільності.
OFDM	-	Orthogonal Frequency-Division Multiplexing, мультиплексування з ортогональним частотним поділом.
PCell	-	Primery Cell, первинна сота.
PCRF	-	Policy and Charging Rules Function, функція політики та правил оплати.
PGW	-	Packet Gateway, пакетний шлюз.
RE	-	Resource Element, ресурсний елемент.
SAE	-	обслуговуючий шлюз мережі LTE.
SCells	-	Secondary Cells, вторинна сота.

SC-FDMA	-	Single Carrier Frequency-Division Multiplexing, мультиплексування з одночастотним розподілом частот.
SGW	-	Serving Gateway, шлюз обслуговування.
UE	-	User Equipment, абонентський термінал.
UMTS	-	Universal Mobile Telecommunications System, універсальна система мобільного зв'язку.
TDMA	-	Time Division Multiple Access, множинний доступ з часовим розподілом.
TDD	-	Time Division Duplex, дуплексний розподіл часу.
VoLTE	-	Voice over LTE, технологія передачі голосу по мережі LTE.
WiMAX	-	Worldwide Interoperability for Microwave Access, всесвітня взаємодія для мікрохвильового доступу.

ВСТУП

Сьогодні людство живе в часи інформаційних технологій, де телекомунікації є життєво необхідними. Об’єми інформації, що передаються через інформаційно-телекомунікаційні інфраструктури, з кожним роком значно зростають. Завдяки розвитку безпроводових технологій сучасні користувачі мобільних пристроїв не пов'язані проводами. Людям не потрібно носити з собою купу кабелів, щоб зайти в мережу Інтернет, зателефонувати знайомому чи передати якийсь файл на інший пристрій. Технології безпроводових мереж набули значного поширення і їх масове використання стимулює їх потужний і невпинний розвиток.

В даній роботі розглянуто та проаналізовано існуючі рішення технологій безпроводових мереж, їх основні характеристики, переваги та недоліки, структури цих мереж, досліджено процес передачі повідомлень. В результаті розроблено структуру безпроводової комп’ютерної мережі, яка дозволяє авторизуватись користувачеві в мережі та обмінюватись повідомленнями з іншими користувачами мережі, а також забезпечує цілісність та шифрування повідомлень.

1. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБГРУНТУВАННЯ ТЕМИ БАКАЛАВРСЬКОГО ПРОЕКТУ

1.1. Покоління мобільного зв’язку

За весь період свого існування мобільні мережі зазнали значних змін і розвитку. Для того, щоб зафіксувати ці видозміни було введено поняття «покоління».

Покоління мобільного зв’язку - це функціональний набір можливостей роботи мережі в рамках певних стандартів, що включають в себе реєстрацію абонента, встановлення сеансу зв’язку, передача інформації між абонентським терміналом UE (User Equipment) та базовою станцією (БС) по радіоканалу, шифрування, роумінг в інших мережах, а також набір послуг, що надається користувачеві [1].

На сьогоднішній день еволюція систем мобільного зв’язку нараховує декілька поколінь: 1G, 2G, 3G, 4G, а також вже і 5G, де «G» - Generation (покоління). Мережі першого покоління були аналоговими і використовувались лише для голосових викликів. Їхніми недоліками були: відносно низька ємкість, відсутність шифрування, відсутність ефективної боротьби з завмиранням сигналу, а також велика вага і висока вартість абонентських терміналів та проблема здійснення процедури роумінгу. Для одночасної передачі використовувався метод множинного доступу з частотним розподілом каналів FDMA (Frequency Division Multiple Access). Нераціональне використання виділених частот призводило до низької ємкості. В кожній європейській країні була своя власна, несумісна з іншими, аналогова система зв’язку [1].

Мережа другого покоління була створена як нова загальноєвропейська система мобільного зв’язку GSM (Global System for Mobile communications). Її основними перевагами були: відносно висока ємкість мережі, шифрування інформації, що передається, можливість надання послуги передачі даних,

висока завадостійкість, можливість реалізації роумінгу, а також невелика вага і відносно не висока вартість абонентських терміналів. Для одночасної передачі декількох каналів разом з FDMA почали використовувати технологію множинного доступу з часовим розподілом каналів TDMA (Time Division Multiple Access). Кожному абоненту на час сеансу зв'язку надавалась не лише частина частотного спектру, але й певний часовий інтервал передачі. Таким чином на одній частині спектру розміщувалось 8 часових інтервалів [2].

Поява мережі Інтернет та стрімкий ріст її користувачів стали поштовхом до пошуку рішень для збільшення швидкості передачі даних в радіоканалі. Одним з перших рішень була технологія високошвидкісної передачі даних з комутацією каналів HSCSD (High Speed Circuit Switched Data), де одному абоненту виділяється, при наявності вільних каналів, не один, а декілька часових інтервалів. Канал звільняється лише після фактичного закінчення сеансу. В результаті наявності пауз при передачі голосу та даних канал використовується не раціонально [1].

Наступним етапом розвитку GSM стала технологія пакетного радіозв'язку спільного користування GPRS (General Packet Radio Service), використання якої дозволило найбільш ефективно використовувати канальний ресурс і досягти теоретично максимальної швидкості передачі даних. Наступний етап розвитку передбачав введення нової схеми модуляції, в результаті чого стала доступною швидкість передачі даних 473,6 Кбіт/с [1].

Потреба в третьому поколінні мобільного зв'язку постала з появою нових послуг пов'язаних з передачею даних, які вимагали більшої швидкості передачі даних та забезпечення високих якісних характеристик. Принциповою зміною в цьому поколінні стало широке застосування кодового розподілу каналів CDMA (Code Division Multiple Access). Абоненти отримують всю смугу частот для передачі, а їх канали розподіляють за допомогою кодів (кодова модуляція) [1].

Для задоволення вимог до мереж третього покоління була розроблена універсальна мобільна телекомунікаційна система ETSI (Universal Mobil Telecommunications Standards Institute). Подальшим розвитком цієї мережі стала технологія високошвидкісного пакетного доступу HSPA (High Speed Packet Access). Передача ведеться короткими кадрами завдовжки 20 мс з управлінням форматом передачі в реальному часі. Що дозволяє відслідковувати завмирання сигналу та підвищує надійність каналу зв'язку. Для підвищення швидкості передачі даних використовується багатокодовий режим передачі трафіка. При повторній передачі неприйнятих кадрів використовується гібридного автоматичного запиту повторної передачі, в якій друга передача може проводитись іншою MCS [1].

Мережа четвертого покоління, яка отримала назву International Mobile Telecommunications Advanced (IMT-Advanced), повинна забезпечувати швидкість передачі даних для мобільних абонентів з високою швидкістю переміщення до 100 Мбіт/с, а для абонентів з низькою швидкістю переміщення – до 1Гбіт/с. Для задоволення цих вимог були розроблені стандарти WiMAX (Worldwide Interoperability for Microwave Access) та LTE (Long Term Evolution), з яких перемога залишилась за LTE. Базовим принципом мереж четвертого покоління є технологія мультиплексування з ортогональним розподілом каналів OFDM (Orthogonal Frequency-Division Multiplexing), також для підвищення ефективності використання частотного ресурсу застосовується технологія одночасної передачі даних з допомогою N антен і їх одночасний прийом з допомогою M антен MIMO (Multiple Input/Multiple Output) [1].

Вимогами до мереж п'ятого покоління будуть: зріст швидкості передачі даних в 10-100 разів, зростання трафіку використовуваного абонентами, можливість обслуговування більшої кількості підключених до мережі абонентів, зменшення використання енергії абонентськими

терміналами, скорочення затримок в мережі, а також зниження загальної вартості експлуатації мереж п’ятого покоління [1].

1.2. Стандарт LTE

LTE – це унікальна технологія побудови мережі мобільного зв’язку, яка належить до четвертого покоління зв’язку. Технологія побудована на базі IP-технологій, що означає, що вона має підвищену швидкість передачі інформації. Цей стандарт був розроблений і затверджений міжнародним об’єднанням 3GPP (3rd Generation Partnership Project). LTE – це не просто покращення третього покоління, а це більш глибока і значна його зміна. Це перехід від системи стандарту CDMA до систем OFDM, а також від систем, які використовують комутацію каналів, до систем, які використовують комутацію пакетів [2].

В першу чергу стандарт зв'язку LTE був розроблений для досягнення наступних цілей [2]:

- зниження вартості передачі інформації по безпроводовій мережі;
- істотне підвищення швидкості передачі даних;
- розширення спектру послуг, що надаються і зниження їх вартості;
- збільшення гнучкості застосування вже наявних систем мобільного зв'язку.

Головною метою розробки стандарту LTE є збільшення швидкості передачі даних по безпроводових мережах. Всі інші цілі автоматично будуть досягнуті при досягненні першої. Інтеграція технології LTE надає можливість створення високошвидкісних систем мобільного зв'язку, які будуть оптимізовані саме для пакетної передачі динних. При цьому швидкість в каналі прийому (download), теоретично, становить 326 Мбіт/с, а в каналі віддачі (upload) - 75 Мбіт/с [2].

Технологія LTE підтримує гнучкі варіанти смуги пропускання з частотою 1,4-20 МГц. Крім цього дана технологія підтримує дуплексну

передачу даних з можливістю поділу сигналів по частоті FDD (Frequency Division Duplex), а також за часом TDD (Time Division Duplex).

Технологія LTE має значно меншу затримку при передачі даних для протоколів на рівні користувача. Це відкриває багато можливостей, наприклад, у абонентів з'являється можливість грати в онлайн-ігри розраховані на велику кількість користувачів [2].

Радіус дії базової станції LTE залежить від потужності випромінювання і теоретично не обмежений, а максимальна швидкість передачі даних залежить від радіочастоти і віддаленості від базової станції. Теоретична межа для швидкості в 1 Мбіт/с - від 3,2 км (2600 МГц) до 19,7 км (450 МГц). Базові станції діапазону 800 МГц здатні забезпечити таку швидкість на відстані до 13,4 км. Діапазон 1800 МГц - найбільш використовуваний в світі, він поєднує в собі високу ємність і щодо великий радіус дії (6,8 км) [2].

Велика частина роботи спрямована на спрощення архітектури системи: вона переходить з існуючих UMTS (Universal Mobile Telecommunications System) та комутації пакетів об'єднаної мережі до єдиної IP-інфраструктури (all-IP). E-UTRA (Evolved Universal Terrestrial Radio Access) є безпроводовим інтерфейсом LTE. Його основні особливості [3]:

- максимальна швидкість завантаження з мережі до 299,6 Мбіт/с і максимальна швидкість завантаження в мережу від абонента до 75,4 Мбіт/с в залежності від категорії обладнання користувача (антена 4 × 4 з використанням спектра 20 МГц);
- низька затримка при передачі даних (5 мс затримка для маленьких IP пакетів в оптимальних умовах), більш низька затримка під час активного з'єднання;
- покращена підтримка мобільності, як приклад термінал, який рухається зі швидкістю 350 км/год або 500 км/год залежно від діапазону частот.
- OFDMA для низхідній лінії зв'язку, SC-FDMA для висхідній лінії зв'язку з метою економії енергії;

- підтримка і FDD і TDD систем зв'язку, а також напівдуплексниєєєй FDD з однієї і тієї ж технологією радіодоступу;
- підвищення гнучкості - спектр: 1,4 МГц, 3 МГц, 5 МГц, 10 МГц, 15 МГц і 20 МГц для ширини стільники стандартизовані;
- підтримка розмірів соти від декількох десятків метрів (фемто і пікосоти) до 100 км; в нижніх частотних діапазонах, які будуть використовуватися в сільських районах, 5 км є оптимальним розміром соти;
- підтримка як мінімум 200 активних клієнтів у кожній соті 5 МГц;
- підтримка співіснування зі старими стандартами (наприклад, GSM/EDGE, UMTS і CDMA2000), користувачі можуть почати виклик або передачу даних в області з наявністю LTE і, покинувши область покриття, продовжити роботу без будь-яких спеціальних дій з його боку в мережах GSM/GPRS;
- радіоінтерфейс комутації пакетів.

Стандарт LTE підтримує тільки комутацію пакетів зі своєю мережею all-IP. Здійснювати дзвінки в GSM, UMTS і CDMA2000 є комутацією каналів, тому з переходом на LTE оператори повинні реорганізувати свою мережу голосових викликів [4]. Існують наступні три способи [3]:

VoLTE (Voice over LTE) - технологія передачі голосу по мережі LTE, заснована на IP Multimedia Subsystem (IMS). Дозволяє надавати голосові послуги і доставляти їх як потік даних по LTE. VoLTE має в три рази більшу голосову ємність і ємність даних, ніж мережі 3G UMTS і до шести разів більшу, ніж мережі 2G GSM. Крім того, вона вивільняє пропускну спроможність, оскільки заголовки пакетів менше, ніж у неоптимізованої VoIP/LTE.

Circuit-switched fallback (CSFB) - при такому підході LTE забезпечує тільки послуги передачі даних, тому, коли потрібно прийняти або зробити голосовий виклик, термінал просто повертається до мережі з комутацією каналів (наприклад, GSM або UMTS). При використанні цього рішення

операторам просто потрібно оновити MSC, замість розгортання IMS, тому можна швидко почати надавати послуги. Однак недоліком є більш тривала затримка при установці виклику. Даний спосіб організації виклику в даний час використовують всі російські стільникові оператори, що надають LTE.

Одночасна передача голосу і LTE (SVLTE) - при такому підході термінал працює одночасно в LTE і з комутацією каналів, в режимі LTE надаються послуги передачі даних і в режимі з комутацією каналів забезпечуються голосові послуги. Це рішення засноване виключно на вимогах до мобільного телефону і не має спеціальних вимог до мережі. Недоліком такого рішення є те, що такий телефон може стати дорогим і мати високе енергоспоживання [3].

Для розширення спектру абонентських мобільних пристроїв планується оснащувати модулями LTE не тільки мобільні телефони (смартфони) і планшетні ПК, але і ноутбуки, відеокамери, ігрові приставки, а також інші побутові та портативні прилади [2].

1.3. Стандарт LTE-A

LTE-Advanced - це назва специфікації 3GPP 10 версії, яким Міжнародний союз електрозв'язку (МСЕ) присвоїв сертифікат «IMT-Advanced».

Можливість агрегування спектра є, мабуть, найголовнішою характерною особливістю LTE-Advanced і забезпечує додаткову гнучкість використання спектра, закладену в системі LTE в формі набору каналів з масштабованою шириною [1].

Розглянемо ряд аспектів, пов'язаних з цим важливим питанням. По-перше, для досягнення заявленої в вимогах МСЕ і стандартах 3GPP швидкості передачі даних 1 Гбіт/с в LTE-Advanced необхідно істотно розширити смугу каналу. Таке рішення є найбільш ймовірним і можливим, тому що на сьогоднішній день мала ймовірність збільшення пропускної

здатності системи за рахунок помітного поліпшення показників спектральної ефективності, існуючих в LTE. У зв'язку з цим в LTE-Advanced встановлено верхню межу ширини каналу 100 МГц, тобто обрана досить широка смуга [5].

По-друге, через відсутність вільних смуг спектра зазначеної ширини практично в усьому світі в стандартах 3GPP закладена можливість агрегації (об'єднання) декількох смуг частот, яка також отримала назву агрегації несучих частот.

До LTE-A застосовуються більш жорсткі вимоги, у порівнянні з попередніми технологіями [5].

Вимоги до LTE-Advanced [1]:

високий ступінь функціональності для надання широкого діапазону високошвидкісних послуг в масштабах світового ринку з істотною економічною ефективністю і якістю;

можливість взаємодії з іншими системами радіодоступу, включаючи повну сумісність з LTE (Rel'8);

гармонізація та сумісність абонентських пристроїв в міжнародному масштабі;

реалізація роумінгу по всьому світу;

підтримання ширини каналу до 40 МГц включно;

можливість організації більш широкої смуги каналу (до 100 МГц), яка потенційно може забезпечити пікову швидкість передачі даних 3 Гбіт/с в Downlink і 1,5 Гбіт/с в Uplink;

забезпечення спектральної ефективності в каналах Downlink до 15 біт/с/Гц при 4x4 MIMO і до 6,75 біт/с/Гц - при 2x4 MIMO в каналах Uplink.

використання 8 передавальних антен MIMO в каналах Downlink [5].

LTE-Advanced допускає агрегацію максимум п'яти роздільних несучих зі смугою до 20 МГц для отримання загальної смуги передачі до 100 МГц. Оскільки жоден з операторів зв'язку не має безперервної смуги 100 МГц,

передбачені три різних режиму агрегації несучих (рисунок 1.1): внутрішньо-смугова агрегація суміжних несучих, внутрішньо-смугова агрегація несуміжних несучих і поза-смугова агрегація несучих. Робоча група RAN 4 (RAN4), що відповідає в 3GPP за визначення вимог до характеристик, спочатку обмежила агрегацію лише двома компонентними несучими [5].

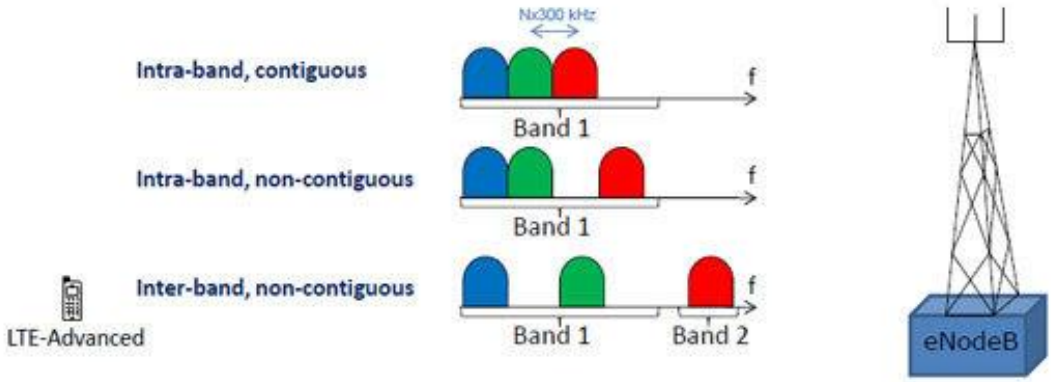


Рисунок 1.1 - Режими агрегації несучих

Також розглядається можливість агрегації між технологіями. Передбачається, що ця технологія дозволить підвищити пропускну спроможність мереж мобільного зв'язку.

В специфікаціях LTE при агрегації смуг використовують такі поняття:

- первинна сота PCell (Primery Cell), яку виділяють кожному UE;
- вторинна сота SCells (Secondary Cells), всі інші соти, які підключені до первинної [1].

В первинній соті здійснюється передача всієї системної інформації: сигнали синхронізації, канали FBCH, SIB, пейджинг, відповіді на запити для доступу в мережу, дані, що обслуговуються. UE, які використовують агрегацію смуг, отримують в первинній соті індивідуальні повідомлення каналів управління, в цій смузі виконуються запити на доступ до мережі і виконується вимір зв'язку з хендовером. Процедура хендовера також направлена на роботу з первинними сотами. Після закінчення хеновера

забезпечується виділення вторинних сот. Сконфігуровані SCells проходять процедуру активації/деактивації на протокольному рівні MAC [1].

Основною процедурою при реалізації технології агрегації є процедура управління сотами, за рахунок якої мережа додає/відключає/переключає SCeels чи переключає PCeel UE [1].

Сигналізація для агрегації несучих в напрямку пристрою кінцевого користувача впливає не на весь стек протоколів, а тільки на певні рівні. Наприклад, пристрій постійно підключено через первинну компонентну несучу (PCC) до первинної обслуговуючої соти (PCell). Функції рівня без доступу (NAS), такі як обмін захищеними ключами і інформація про мобільність абонентського обладнання, надаються PCell. Всі вторинні компонентні несучі вважаються додатковими ресурсами передачі. Для протоколу управління передачею пакетних даних (PDCP) і рівня управління каналом радіозв'язку (RLC) сигналізація агрегації несучих є прозорою. Налаштування терміналу для роботи з вторинними компонентними несучими здійснюється на рівні управління радіоресурсами (RRC). Крім того, на рівні RRC налаштовуються параметри вторинних сот (SCell). Рівень управління доступом до середовища передачі (MAC) виконує функції мультиплексування об'єкта для агрегованих компонентних несучих, оскільки вони активуються або деактивуються елементами управління MAC. Якщо ввімкнути функцію в підкадрів n ресурсів будуть доступні для пристрою через 8 підкадрів (8 мс), і воно зможе перевірити заплановані призначення. Хоча MAC діє в якості мультиплексора, слід зазначити, що кожна компонентна несуча має свій власний об'єкт фізичного рівня (PHY), що забезпечує кодування каналу, HARQ, модуляцію даних і зіставлення ресурсів [5].

Підтримка агрегації несучих є ключовим фактором, завдяки якому технологія LTE-Advanced виконує вимоги стандарту IMT-Advanced за піковими швидкостями передачі даних. Це дуже важлива опція з точки зору

оператора мережі, оскільки вона також забезпечує агрегацію різних фрагментів спектра. Однак основні проблеми з точки зору розробки відносяться до сторони терміналу. Підтримка більш високої пропускної здатності і агрегації несучих в різних частотних діапазонах ускладнює ланцюг приймача і його компоненти, такі як широкосмугові підсилювачі потужності, високоефективні комутатори і елементи антен, що підлягають налаштуванням [1].

Крім того, необхідно ретельно тестувати додаткові функції фізичного рівня (PHY) і рівня MAC, а також адаптацію до рівня RRC. Rohde & Schwarz пропонує безліч рішень для тестування рішень на основі LTE-Advanced з агрегацією несучих. Широкий асортимент пропозицій включає в себе генератори і аналізатори сигналів для проведення тестів фізичного рівня на базових станціях, мобільних пристроях або компонентах, а також емулятори базових станцій для тестування фізичного рівня і протоколів для будь-яких видів безпроводових пристроїв і наборів мікросхем [1].

LTE Rel’8 підтримує кілька схем антен введення/виведення як в низхідному, так і в висхідному напрямку. У напрямку низхідної лінії зв'язку може використовуватися до чотирьох передавальних антен, тоді як максимальна кількість кодових слів дорівнює двом незалежно від кількості антен. Підтримуються мультиплексування з просторовим розділенням (SDM) декількох потоків символів модуляції як на один UE, що використовує один і той же частотно-часовий ресурс, так званий однокористувацький MIMO (SU-MIMO), так і на різні UE, що використовують один і той же частотно-часової ресурс, так званий MU-MIMO. У напрямку висхідної лінії зв'язку використовується тільки MU-MIMO, тобто існує тільки один потік модульованих символів на UE, який повинен бути прийнятий eNodeB, тоді як безліч UE можуть передавати на одному частотно-часовому ресурсі. З огляду на певні класи можливостей UE, можна очікувати, що дві операції антени в

низхідній лінії зв'язку і одна операція антени в висхідній лінії зв'язку будуть стандартним випадком для початкового розгортання LTE [6].

В LTE-Advanced розширюються можливості MIMO, що підтримувались в LTE Rel'8 і тепер підтримуються вісім антен низхідній лінії зв'язку і чотири антени висхідній лінії. У напрямку висхідній лінії зв'язку LTE-Advanced застосовуються ті ж принципи, які визначені в низхідній лінії зв'язку LTE версії 8, тоді як в напрямку низхідній лінії зв'язку LTE-Advanced існуюча схема LTE версії 8 просто розширюється. Як і схеми передачі MIMO, рознесення передачі можливе як в низхідній лінії зв'язку, так і в напрямку висхідної лінії зв'язку [6].

В розділі було проаналізовано існуючі методи створення різних поколінь безпроводових мобільних мереж, проаналізовано їх переваги та недоліки, а також детально розглянуто технологію LTE, яка і є темою дипломного проекту.

2. РОЗРОБКА СТРУКТУРИ БЕЗПРОВОДОВОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Спрощена структура LTE

Мережа LTE складається з мережі радіодоступу E-UTRAN (Evolved Universal Terrestrial Radio Access Network) та вдосконаленого пакетного ядра EPC (Evolved Packet Core), як представлено на рисунку 2.1 [7].

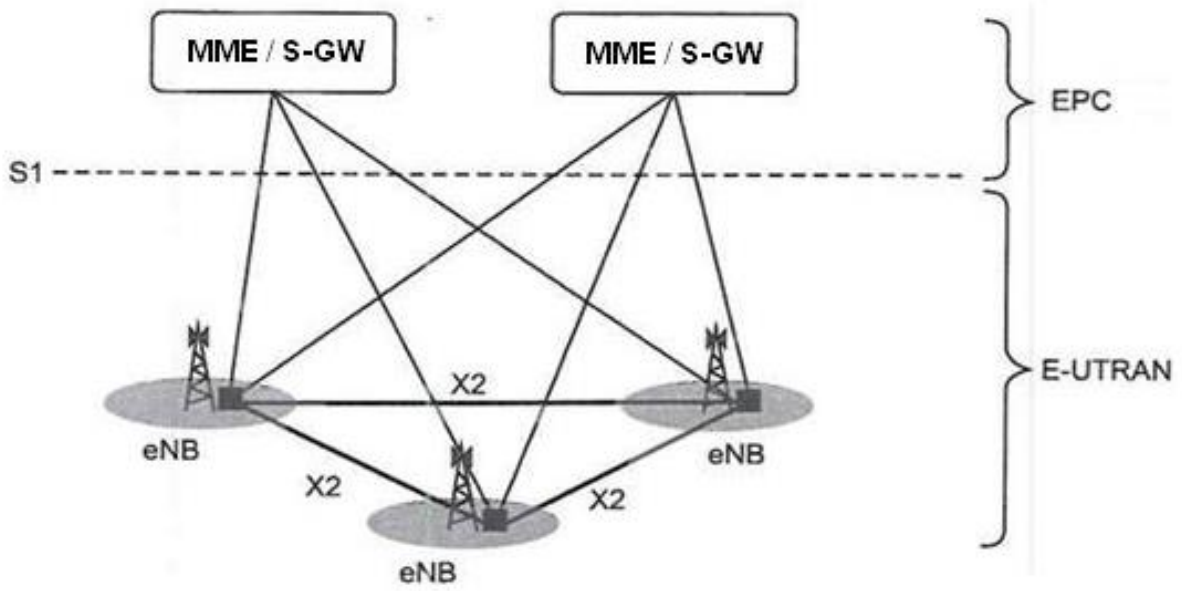


Рисунок 2.1 - Спрощена архітектура мережі LTE

Мережа LTE представлена сукупністю базових станцій eNodeB (Evolved NodeB чи eNodeB), які з'єднані між собою інтерфейсом X2. eNodeB під'єднуються до EPC за допомогою інтерфейсу S1. Також на рисунку 2.1 представлено взаємодію нових елементів мережі: SGW (Serving Gateway), що обслуговують шлюзи по утриманню програмного забезпечення управління по протоколу MM (MME – Mobility Management Entity) [7].

В мережі радіодоступу створено радіоінтерфейс між UE і eNodeB на основі технології ортогонального частотного рознесення OFDMA (Orthogonal Frequency Division Multiplexing).

EPC працює на основі технології IP. Таку структуру відносять до мереж All-IP Network (AIPN) [7].

2.2 Детальна структура мереж LTE/LTE-A

Архітектура мережі LTE розроблялась таким чином, щоб забезпечити об’єднання пакетного IP-трафіка з так званою «безшовною» мобільністю, мінімальними затримками передачі пакетів та високими показниками якості обслуговування. Основною метою розробників було максимально спростити структуру мережі (рисунок 2.2).

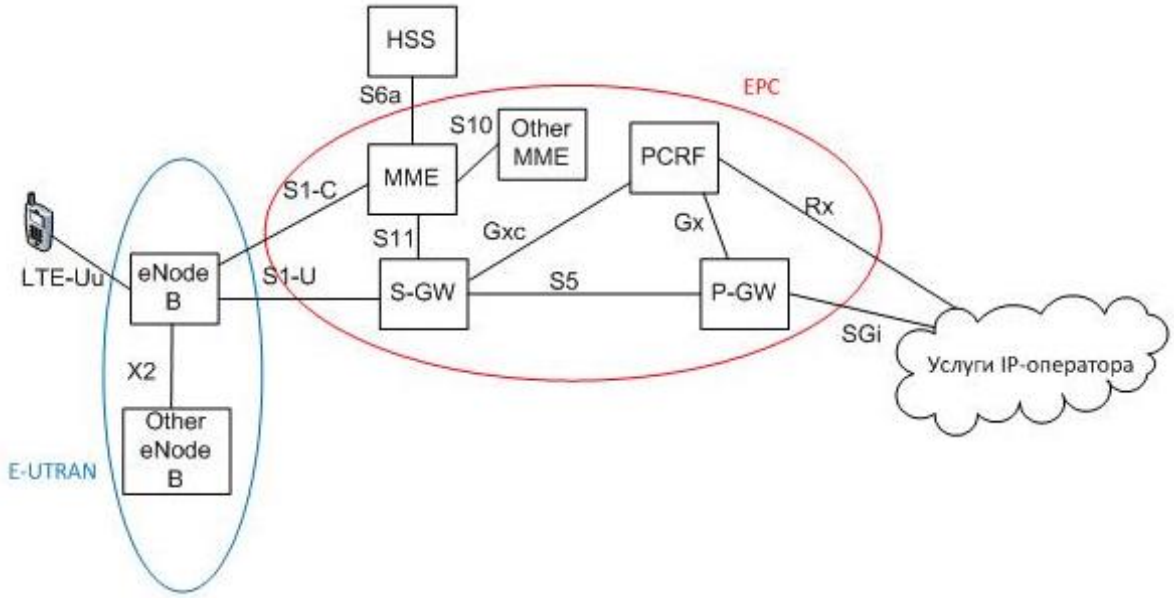


Рисунок 2.2 - Структура мережі LTE

На фізичному рівні мережа LTE складається з двох частин: мережі радіо-доступу E-UTRAN і базовою мережею SAE, яку також називають покращеним пакетним ядром EPC [1].

Мережа радіо-доступу E-UTRAN [1]:

- вузли базових станцій (eNodeB).

Базова мережа SAE (покращене пакетне ядро EPC) [1]:

- обслуговуючий шлюз SGW;
- шлюз виходу на пакетні мережі PGW;
- структура управління мобільністю MME;
- сервер абонентських даних HSS;
- білінгова функція PCRF;

eNodeB – виконує функції базових станцій і контролерів мережі третього покоління [1]:

- організовує передачу трафіка і сигналізацію по радіоканалу;
- керує розподілом радіо-ресурсів;
- організовує наскрізний канал трафіку до SGW;
- попереджує сигналізацію передач і контролює рівень завад в соті;
- забезпечує шифрування і цілісність передачі в радіоканалі;
- виконує вибір MME і виконує сигнальний обмін з ними;
- виконує стиснення заголовку IP-пакетів.

X2 – інтерефейс між eNodeB – eNodeB, основною задачею якого є організація хендовера між сусідніми eNodeB, в тому числі і при балансування навантаження між ними.

S1 – інтерфейс між E-UTRAN I SAE (EPC), який забезпечує передачу даних eNodeB – SGW (S1-U) і сигналізації eNodeB - MME(S1-C).

SAE – обслуговуючий шлюз мережі LTE, основна мета якого полягає в обробці і маршрутизації пакетних даних, які надходять з/в E-UTRAN. SGW має пряме з'єднання з мережами другого і третього покоління того ж оператора, що спрощує передачу з'єднання. Кожен працюючий абонентський термінал UE обслуговує певний SGW. Теоретично UE може бути пов'язаний з декількома пакетними мережами, тоді його будуть обслуговувати декілька SGW [1].

Основними функціями SGW є [1]:

- маршрутизація пакетних даних, що передаються;
- буферизація пакетів для UE, що перебувають в режимі очікування;
- надання облікових даних в PCRF для тарифікації і оплати наданих послуг.

PGW – шлюз призначений для маршрутизації трафіка мережі LTE до інших мереж передачі даних. При наявності у користувача статичної IP-

адреси, PGW її активує. У випадку, якщо абонент повинен отримати на час сеансу зв’язку динамічну IP-адресу, PGW робить запит на сервер протокола динамічної конфігурації вузла DHCP або сам виконує необхідні функції DHCP, після чого виконує доставку IP-адреси абоненту. В склад PGW входить пристрій з прийняття рішень по виділенню ресурсів та тарифікації PCEF, який забезпечує якісні характеристики послуг на зовнішньому з’єднанні через інтерфейс SGi та фільтрацію пакетних даних. При знаходженні абонента в роумінгу PGW зазвичай знаходиться в домашній мережі абонента, а SGW, MME і eNodeB, відповідно у гостьовій. Якщо абонента обслуговує домашня мережа, то PGW і SGW пов’язані інтерфейсом S5. Якщо SGW знаходиться у гостьовій мережі, а PWG – в домашній, то між ними інтерфейс S8, що являє собою міжмережевий варіант S5 [1].

MME – вузол управління мобільністю мережі мобільного зв’язку LTE. Призначений для обробки сигналізації, переважно пов’язаний з необхідністю перемаршрутизації трафіка в мережі з переміщеннями UE в мережі. Підтримує виконання процедур протоколу управління мобільністю, забезпечує безпеку роботи в мережі при підключенні UE і вибір SGW, PGW.

S6a – інтерфейс між MME і HSS своєї мережі.

S10 – інтерфейс, що з’єднує різні MME, дозволяє обслуговувати UE при переміщеннях абонента, а також при його находженні в роумінгу.

HSS – сервер абонентських даних в мережі мобільного зв’язку стандарту LTE. Представляє собою базу даних абонентів і їх трафіків, послуг і т.п. Крім цього, HSS генерує дані, необхідні для реалізації процедур безпеки. В мережі LTE може знаходитись один або декілька HSS. Кількість HSS обумовлена структурою мережі або кількістю абонентів [1].

PCRF – елемент мережі мобільного зв’язку стандарту LTE, в функції якого входить [1]:

- встановлення параметрів для організації та модернізації наскрізних каналів;

- встановлення тарифів для організованих послуг;
- підготовка даних для генерації облікових записів CDR.

Іншими словами, PCRF – це керуючий сервер, що забезпечує централізоване управління ресурсами мережі [1].

2.3 Архітектура суміщених мереж зв'язку

У зв'язку з необхідністю інтеграції мереж LTE/LTE-A до існуючих мереж 2G і 3G, була розроблена структура комплексної мережі мобільного зв'язку (рисунок 2.3), причини створення якої обумовлені [1]:

- значною кількістю пристроїв минулих поколінь, які не виробляють ресурси і які не можна або не вигідно замінити;
- в місцях, які радіо-покриті менш якісно в період запуску LTE – необхідно підхоплювати з них абонентів в мережах попередніх поколінь [1].

Коли відбувається інтеграція LTE в комплексну мережу між MME і SGSN, SGW і SGSN використовуються інтерфейси взаємодії S3 і S4. Через інтерфейс S3 - SGSN виконує обмін сигнальною інформацією з MME при передачі обслуговування UE між GERAN чи UTRAN/E-UTRAN. Ця процедура зветься хендовером, аналогічно до передачі обслуговування від БС до БС всередині самих мереж радіодоступу [1].

Для оптимізації схеми доступу абонента до мережі Інтернет виконується через PGW. Якщо абонент обслуговується GERAN (2G), то його трафік передається на SGW з SGSN через інтерфейс S4, а потім по інтерфейсу S5/S8 на PGW і далі в IP мережу. Якщо ж абонент працює в мережі 3G (UTRAN), то його трафік також може проходити по інтерфейсам lu/S4 через SGSN в SGW і далі в IP мережу через PGW. Таким чином, SGW представляє собою точку прив'язки трафіку до місця знаходження абонента [1].

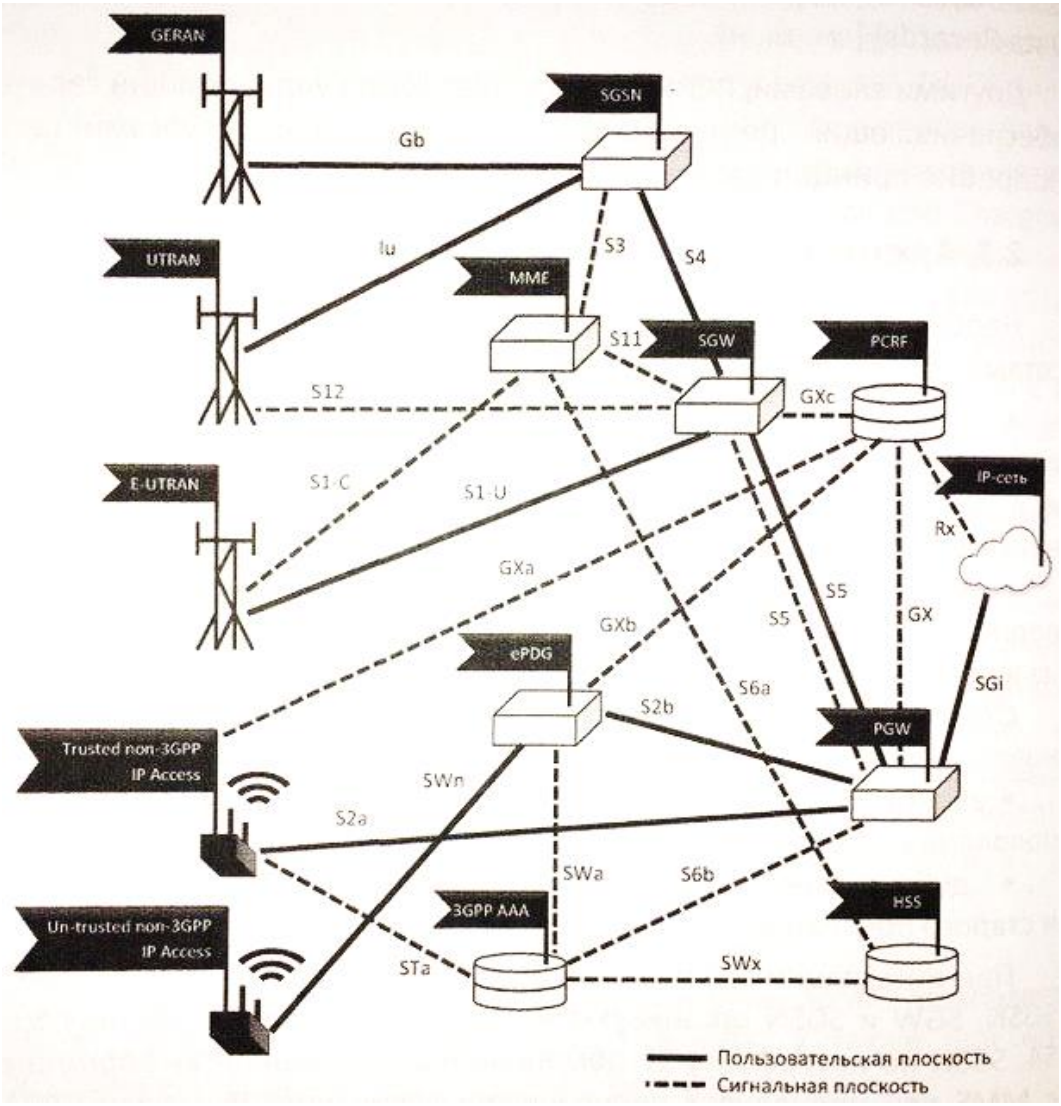


Рисунок 2.3 – Структура комплексної мережі мобільного зв’язку

2.4 Абонентський термінал UE в E-UTRAN

Під час роботи в мережі E-UTRAN абонентський термінал може перебувати в одному із трьох станів (рисунок 2.4) [1]:

- LTE_DETACHED - абонент не в мережі;
- LTE_CONNECTED – абонент в активному стані;
- LTE_IDLE – в очікуванні.

Після того як UE ввімкнули він переходить в режим LTE_DETACHED, при тому в цьому стані він ще не зареєстрований і не має авторизованої IP-адреси.

Після отримання реєстрації UE переходить в режим LTE_CONNECTED і в цьому стані відбувається обмін повідомленнями через радіоінтерфейс [1]. Уже в режимі LTE_CONNECTED UE, маючи активовану адресу і прив'язку до конкретної eNodeB, він також отримує тимчасовий ідентифікатор C-RNTI (Cell Radio Network Temporary Identifier) для обслуговування на радіоінтерфейсі [1].

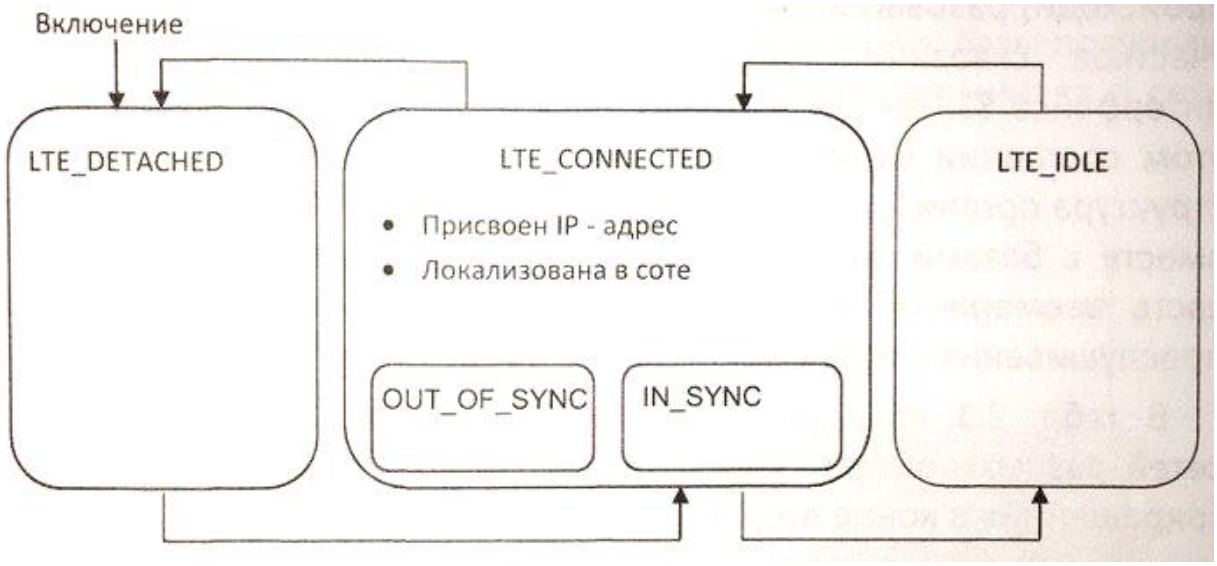


Рисунок 2.4 - Стани абонентського терміналу

Режим LTE_CONNECTED має два стани: OUT_OF_SYNC та INC_SYNC (рисунок 2.4), в залежності від того чи синхронізована чи ні передача вверх з eNodeB [1].

В стані INC_SYNC eNodeB вимірює затримку при надходженні OFDM-символів на свій приймач, а також виконує корегування часу попередження на UE. Якщо протягом деякого часу передача вверх була відсутньою, то корекція часу попередження стає неможливою і користувацький термінал переходить в стан OUT_OF_SYNC. Для того, щоб відновити синхронізацію на лінії вверх, UE необхідно ще раз виконати процедуру доступу до мережі [1].

UE може переходити в режим LTE_IDLE під час пауз в сеансі , при цьому відбувається розірвання сигнального з'єднання UE – MME та розрив

ділянок наскрізних каналів трафіку на радіоінтерфейсі та інтерфейсі S1. Базова станція очищує базу даних відповідного UE, проте останній в свою чергу зберігає IP адресу , залишається незмінною структура організованих наскрізних каналів в ядрі мережі разом з базами даних абонентів MME, SGW і PGW. Переважно більшу частину часу UE перебуває в неактивному стані, лише час від часу вмикає приймач для прослуховування сигналів системного управління [1].

В розділі було розглянено та досліджено структуру безпроводової мережі LTE, її компоненти та їх характеристики.

3. АЛГОРИТМИ ЗАХИСТУ ТА ПЕРЕДАЧІ ІНФОРМАЦІЇ

3.1 Передача даних на фізичному рівні

Стандарт LTE на фізичному рівні по лінії вверх використовує технологію Orthogonal Freuency Division Multiplexing (OFDM). Ця технологія дозволяє уникнути міжсимвольну інтерференцію, яка виникає при високошвидкісній передачі даних при багатопроменевому поширенню сигналу (рисунок 3.1).

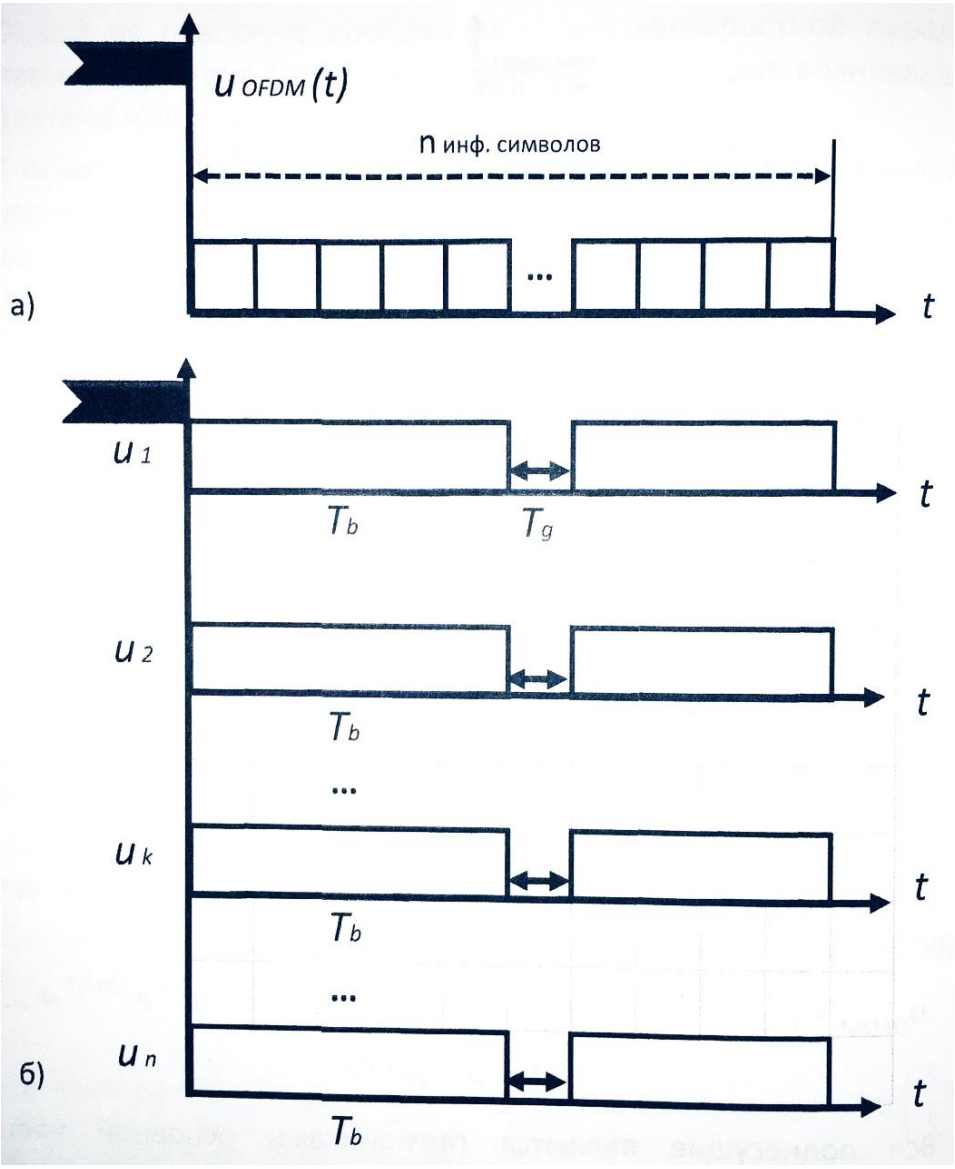


Рисунок 3.1 – Принцип технології OFDM

Дана технології полягає в тому, що замість того, щоб передавати n інформаційних символів інформаційного цифрового сигналу на одній несучій частоті (рисунок 3.1, а) - здійснюється одночасна передача n інформаційних символів цифрового сигналу на n піднесучих частотах, що розміщені в смузі радіоканалу (рисунок 3.1, б). Кількість піднесучих частот в робочій смузі 29 МГц дорівнює 1200. Між символами додаються циклічні префікси довжиною Tq, для того, щоб символи, які прийдуть з запізненням не накладались один на один [1].

При використанні OFDM передача даних здійснюється на безлічі частотних піднесучих (subcarrier). При відстані між піднесучими ΔF = 15 кГц тривалість OFDM символу становить 1/ΔF = 66.7 мкс. У кожному слоті (0.5 мс) передають 6 або 7 OFDM символів в залежності від тривалості циклічного префікса CP (Cyclic Prefix). Тривалість циклічного префікса дорівнює TCP = 160xTS = 5.2 мкс перед першим символом і TCP = 144xTS = 4.7 мкс перед іншими символами. Також є можливість використання розширеного циклічного префікса тривалістю TCP = 512xTS = 16.7 мкс. В цьому випадку в одному слоті передаються 6 OFDM символів.

Наявність нормального циклічного префікса надає можливість боротись з затримками відбитих сигналів, що пройшли на 1,4 км більше, ніж прямий сигнал. Передача інформаційних символів в каналі представляє собою передачу комплексних чисел.

При формуванні OFDM-сигналу застосовується обернене швидке перетворення Фурьє. Схема формування OFDM-сигналу в передавачі базової станції мережі LTE представлено на рисунку 3.2.

Основною проблемою при використанні цієї технології є забезпечення високого співвідношення сигнал/шум в приймачі. Спектри сигналів на розташованих поряд піднесучих накладаються один на один. Саме через це приймання сигналів відбувається з використанням прямого перетворення

Фурьє. Тому паралельно працюють n приймачів, кожен з яких обробляє сигнал однієї піднесучої [1].

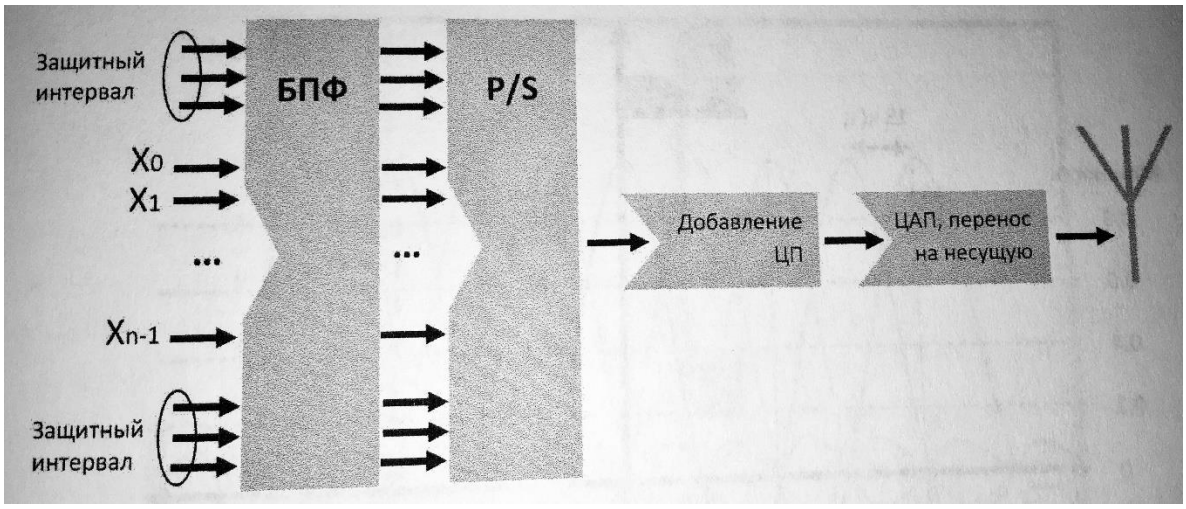


Рисунок 3.2 – Структурна схема формування OFDM сигналів

Весь канальний ресурс розбивається на ресурсні блоки RB (Resource Block). Один блок складається з 12 розташованих поруч піднесучих, що займають смугу 180 кГц, і одного часового слота (6 або 7 OFDM символів загальною тривалістю 0.5 мс). Кожен OFDM символ на кожній з піднесучих утворює ресурсний елемент RE (Resource Element), який характеризується парою значень {k, l}, де k - номер піднесучої, l - номер символу в ресурсному блоці. При стандартній конфігурації (зі стандартною тривалістю циклічного префікса і, отже, з 7 OFDM символами в одному слоті) в низхідному каналі кожен ресурсний блок включає в себе 12x7 = 84 ресурсних елементи.

Частина з ресурсних елементів використовується для передачі пілотного (reference) сигналу, який використовується для синхронізації і оцінки стану радіоканалу. Ці сигнали передаються в першому і п'ятому OFDM символі кожного слота при стандартній довжині циклічного префікса і в першому і четвертому - при розширеній довжині циклічного префікса. При цьому, в частотній області ці сигнали розносяться на фіксовану величину.

Для передачі по лінії вверх в стандарті LTE використовується технологія SC-FDMA (Single Carrier FDMA) з метою підвищення ефективності роботи підсилювачів передаючого тракта. Замість самих символів інформаційного блоку на піднесучих розміщують спектральні характеристики цього блоку. Для цього над блоком, що передається виконують пряме перетворення Фурьє. Так на кожній піднесучій формується відповідний сигнал відліку спектра. Сума всіх сигналів піднесучих повертає вихідних інформаційний сигнал. В результаті через радіоінтерфейс передається дискретний аналоговий сигнал, що підвищує вимоги до сигнал/шум на приймачі eNodeB.

В приймачі eNodeB за допомогою прямого перетворення Фурьє отримують відрахунки спектра блоку, що передавався, а потім за допомогою оберненого перетворення Фурьє відновлюють початковий вихідний цифровий сигнал (рисунок 3.3) [1].

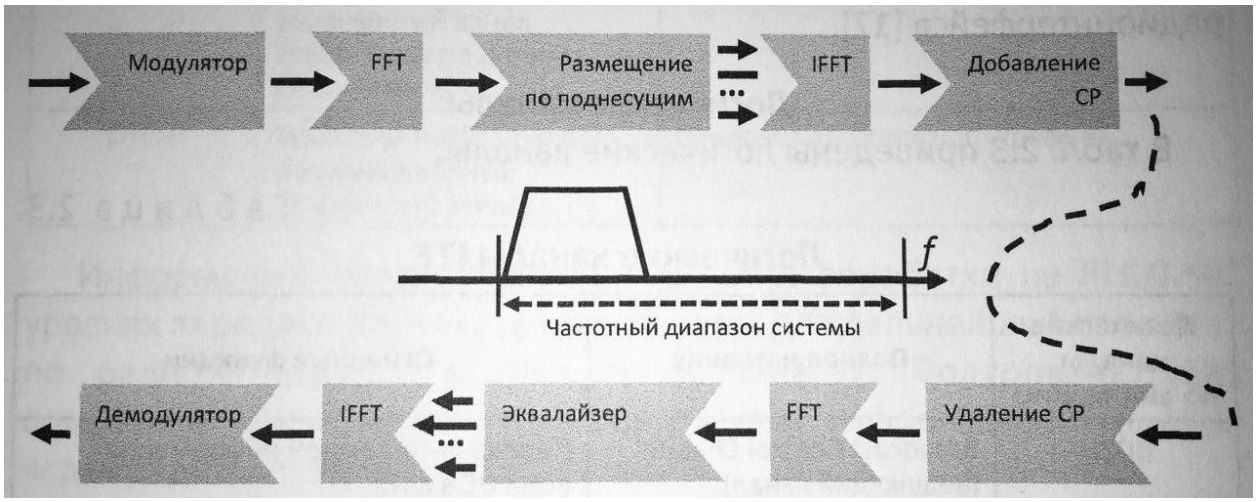


Рисунок 3.3 – Передача даних з використанням технології SC-FDMA

Аналогічно до OFDMA в SC-FDMA кожен фізичний ресурсний блок , що відповідає певному слоту, займає 12 піднесучих з кроком 15 кГц в частотній області і 0,5 мс – в часовій. Ресурсний блок – це 12 піднесучих в частотній області і один тайм-слот або 7 OFDM-символів в часовій області. Для захисту використовуються піднесучі на краях спектрів [1].

3.2 Алгоритми захисту інформації про абонента

Захист інформації в мережах LTE поділяється на такі області:

- аутентифікація абонента в мережі;
- захист абонентів;
- захист і шифрування переданих повідомлень.

Захист абонента в мережі полягає в наданні йому тимчасового ідентифікатора під час його перебування в мережі.

Для приховування даних в мережах LTE/LTE-A використовується потокове шифрування за допомогою накладення псевдовипадкової послідовності (ПВП) на відкриту інформацію за допомогою оператора XOR. Для забезпечення безпеки в таких мережах використовують принцип тунелювання з’єднань.

Під час підключення абонента до мережі чи його активації в мережі запускається процедура аутентифікації і угоди про ключі AKA (Authentication and Key Agreement). Це дозволяє створити проміжний ключ KA-SME для взаємної аутентифікації абонента і мережі. Час роботи механізму AKA займає досить кориткий проміжок часу, який необхідний для створення ключа в додатку USIM і для підтримання зв'язку з Центром реєстрації (HSS). Таким чином, щоб досягти більш швидкої передачі даних в мережі необхідно додати функцію оновлення інформації про ключі без ініціалізації процедури AKA. Для цього в мережах LTE-A використовується ієрархічна ключова структура, де додаток USIM та Центр аутентифікації (AC) здійснює попередній розподіл ключів.

Коли, для здійснення двосторонньої аутентифікації користувача і мережі, здійснюється ініціалізація механізму AKA, генеруються ключ шифрування CK і ключ загального захисту, які потім передаються з USIM в Мобільне обладнання (ME) і з Центру аутентифікації в Центр реєстрації (HSS). В свою чергу ME і HSS, використовуючи ключі CK і IK та ID мережі, що використовується - утворює ключ KA-SME. Встановивши залежність

ключа від ID мережі, Центр реєстрації гарантує можливість використання ключа лише в межах цієї мережі.

Потім утворений KA-SME передається з HSS в MME поточної мережі, де він використовується в якості майстер-ключа. За допомогою KA-SME утворюється ключ KNAS-ENC, що використовується для шифрування даних протоколу NAS між мобільним пристроєм (UE) і MME, і KNAS-INT, необхідний для захисту цілісності. Під час під'єднання UE до мережі, MME генерує ключ KEYNodeB і передає його на eNodeB. Потім з ключа KEYNodeB виробляється ключ KUP-ENC, який використовується для шифрування даних користувача протоколу U-Plane, ключ KRRC-ENC для протоколу RRC (Radio Resource Control) і ключ KRRC-INT, призначений для захисту цілісності (рисунок 3.4).

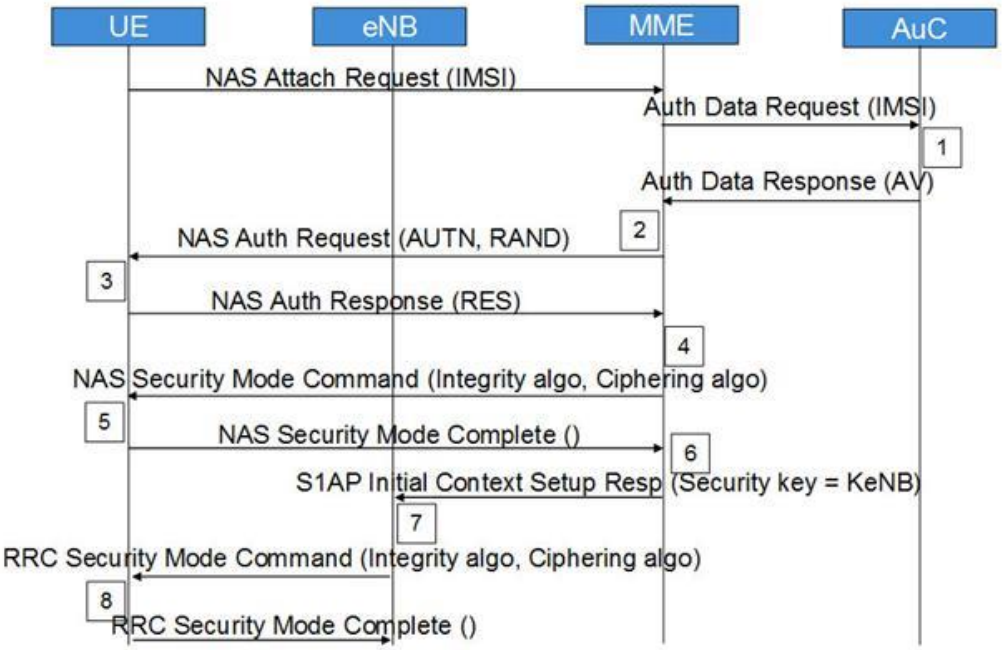


Рисунок 3.4 – Схема алгоритму аутентифікації та генерації ключа

Алгоритм аутентифікації та генерації ключа полягає в такій послідовності кроків.

Крок 1. Запит від мобільної станції (UE) про підключення до мережі. MME запитує аутентифікаційні дані, які відповідають конкретному IMSI, відправляючи Authentication Data Request. AuC/HSS обирає PSK, що відповідає конкретній IMSI і визначає дані для аутентифікації за допомогою PSK. AuC/HSS відправляє назад AV з Authentication Data Response.

Крок 2. MME отримує IK, CK, XRES, RAND і AUTH з AV. MME відправляє до UE за допомогою Authentication Request AUTH і RAND.

Крок 3. UE аутентифікує NW, перевіряючи отриманий AUTH. Потім визначає IK, CK, RES, XMAC зі свого ключа захисту, AMF, (OP), AUTH і RAND. Вона відправляє RES з Authentication response.

Крок 4. Після отримання RES, MME порівнює його з XRES і якщо вони співпадають, то аутентифікація пройшла успішно, в іншому випадку, MME відправляє збій аутентифікації (Authentication failure) до UE. MME скидає лічильник DL NAS. Розраховує KA-SME, KEYNodeB, KNAS-INT, KNAS-ENC. Відправляє NAS команду режиму безпеки (алгоритм цілісності, алгоритм шифрування, NAS набір ключів ID, функцію безпеки UE) з цілісністю, використовуючи KNAC-INC.

Крок 5. Після отримання NAS команди режиму безпеки, UE обраховує KA-SME, KEYNodeB, KNAS-INT, KNAS-ENC. UE відправляє NAS режим безпеки виконаний з цілісністю, захищених і зашифрованих даних.

Крок 6. Після отримання NAS команди режиму безпеки від UE, MME відправляє KEYNodeB в eNodeB з S1AP первісне встановлення початкового контексту (ключ захисту).

Крок 7. Після отримання KEYNodeB, eNodeB обчислює KRRC-INT, KRRC-ENC, KUP-ENC. Потім воно відправляє RRC ключ захисту команди з AS цілісністю алгоритму і AS шифрує алгоритм.

Крок 8. Після отримання RRC команди ключа захисту UE обчислює KRRC-INT, KRRC-ENC, KUP-ENC. UE відправляє RRC виконаний ключ шифрування на eNodeB.

Після виконання всіх цих кроків, всі NAS і AS повідомлення будуть надійно захищені і зашифровані, на відміну від призначених для користувача даних, які будуть тільки шифруватися [9].

Механізм забезпечення безпеки LTE забезпечує системою безпеки і рівень NAS і рівень AS (рисунок 3.5).

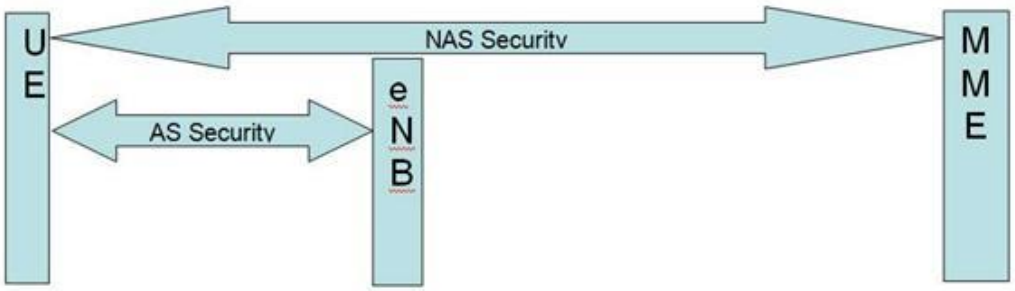


Рисунок 3.5 – Рівні безпеки в мережі LTE

Безпека NAS (рівень без доступу) створена для NAS повідомлень і належить області UE і MME. У цьому випадку необхідна при передачі повідомлень NAS між UE і MME - цілісність, захищена і зашифрована з додатковим заголовком безпеки NAS.

Безпека AS (рівень з доступом) створена для RRC і областей призначених для даних користувача, що належать UE і eNodeB. Рівень PDCP на сторонах UE і eNodeB відповідає за шифрування і захист цілісності.

RRC повідомлення захищені цілісністю і зашифровані, а дані U-Plane лише зашифровані.

Для генерування векторів аутентифікації використовується криптографічний алгоритм з допомогою однонаправлених функцій - прямий результат отримується шляхом простих обчислень, а зворотний результат не може бути отриманий зворотним шляхом. Таким чином не існує ефективного алгоритму отримання зворотного результату. Для цього використовується випадкове 128 бітове число RAND, майстер-ключ K абонента, 128 біт і

порядковий номер процедури SQN (Sequence Number). Лічильник SQN змінюється при кожній генерації вектора аутентифікації. Схожий лічильник SQN працює і в USIM. Такий метод дозволяє генерувати кожен раз новий вектор аутентифікації, не повторюючи попередній вектор аутентифікації, що вже був у використанні.

Крім трьох вихідних величин: SQN, RAND і K в алгоритмі f1 використовується поле управління аутентифікацією Authentication Management Field (AMF), а в алгоритмах f2 - f5 вихідні параметри - RAND і K. На виходах відповідних функцій отримують Message Authentication Code (MAC) - 64 біта; XRES - eXpected Response, результат роботи алгоритму аутентифікації (32 - 128 біт); ключ шифрування CK, що генерується з використанням вхідних (K, RAND) -> f3-> CK; ключ цілісності IK, згенерований з використанням входить (K, RAND) -> f4-> IK; і проміжний ключ Anonymity Key (AK), що генерується за допомогою (K, RAND) -> f5-> AK - 64 біта.

Під час обслуговування абонента мережею E-UTRAN ключі CK і IK не передаються в ядро мережі у відкритому вигляді. В такому випадку HSS генерує KASME за допомогою алгоритму KDF (Key Derivation Function), для якого вихідними параметрами є CK і IK, а також ідентифікатор, який обслуговує мережі і SQNÅAK. Вектор аутентифікації містить в собі RAND, XRES, AUTN і KASME на основі якого відбувається генерація ключів шифрування і цілісності, які використовуються у відповідномих алгоритмах.
Коли мобільна станція отримує з ядра мережі три параметра (RAND, AUTN і KSIASME, де KSI - Key Set Identifier, ідентифікатор утвореного ключа, однозначно пов'язаний з KASME в мобільній станції).

Потім, використовуючи RAND і AUTN, USIM за допомогою алгоритмів безпеки, що зберігаються в HSS, відбувається визначення XMAC, RES, CK і IK.

Після цього у відповіді RES UE передає в MME обчислене RES, яке має співпадати з XRES, отриманим з HSS. Таким чином мережа аутентифікує абонента. Визначивши XMAC, UE порівнює його з MAC, отриманим нею в AUTN. При успішній аутентифікації мережі (MAC = XMAC) UE повідомляє про це у відповіді RES. Якщо аутентифікація мережі не вдалася (MAC ≠ XMAC), то UE направляє в MME відповідь CAUSE, де вказує причину помилки при аутентифікації.

Якщо попередній етап закінчився успішно MME, eNB і UE виконують генерацію ключів, що використовуються для шифрування і перевірки цілісності одержуваних повідомлень. E-UTRAN має ієрархію ключів (рисунок 3.6).

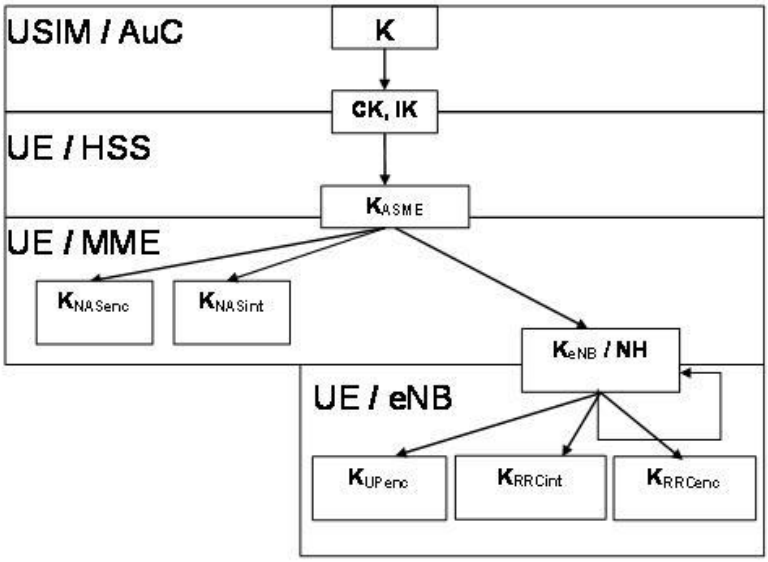


Рисунок 3.6 – Ієрархія ключів E-UTRAN

Вектори аутентифікації:

- ключі IK і CK, що генеруються в центрі аутентифікації і в USIM;
- ключ AK, що генерується тільки в центрі аутентифікації;
- відповідь XRES, яка генерується тільки в центрі аутентифікації, а RES генерується в USIM;

- код MAC, який генерується тільки в центрі аутентифікації, а відповідний йому параметр XMAC генерується в USIM;
- маркер AUTH, що генерується тільки в центрі аутентифікації.

Вихідним ключем з цього всього є KASME (256 біт). При передачі в радіоканалі захист забезпечують для сигнального трафіку (Control Plane) і для призначених для користувача пакетів (User Plane). При цьому всі повідомлення сигналізації поділяють на наскрізні сигнальні повідомлення між UE і MME протоколів MM і SM (NAS - Non Access Stratum) і сигнальні повідомлення між eNodeB протоколу RRC (AS - Access Stratum). Для шифрування і захисту цілісності можна використовувати різні базові алгоритми:

- UEA2 (UMTS Encryption Algorithm 2) і UIA2 (UMTS Integrity Algorithm 2);
- розроблені для стандартів 3G, AES (Advanced Encryption Standard).

Сигнальні повідомлення протоколу RRC (AS) також шифрують і забезпечують їх цілісність. Пакети трафіку тільки шифрують. Ці операції проводять в обслуговуючій eNodeB і UE. Схема отримання ключів шифрування і цілісності (рисунок 3.7) для AS і UP трафіку відрізняється від попереднього випадку тим, що вихідним параметром тут служить вторинний проміжний ключ KEYNodeB (256 біт).

Цей ключ генерують, також за допомогою KDF, де вхідними параметрами є: KA-SME, лічильник сигнальних повідомлень NAS вгору, попереднє значення KEYNodeB, ідентифікатор соти і номер частотного каналу в напрямку вгору. Отже, при будь-якій періодичної локалізації UE відбувається зміна KEYNodeB.

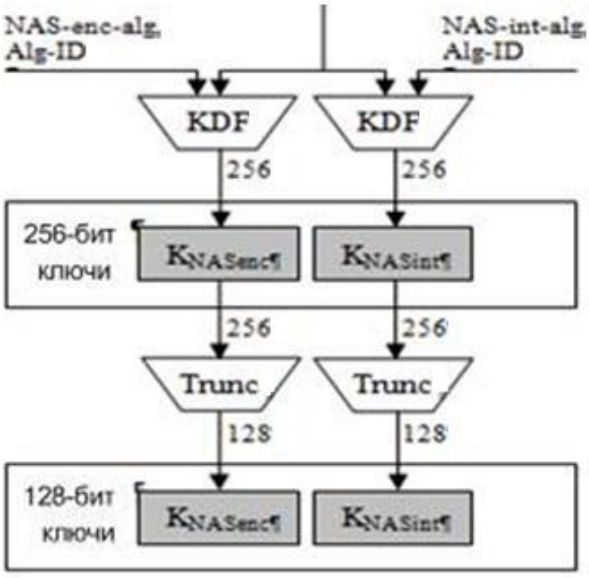


Рисунок 3.7 - Генерація ключів шифрування і цілісності для NAS сигналізації

Також KEYNodeB змінюється і при хендовері (процес переходу абонента від однієї базової станції до іншої), при цьому в алгоритмі генерації нового KEYNodeB використовується додатковий параметр NH (Next Hop), що є лічильником кількості базових станцій, які обслуговують абонента (рисунок 3.8).

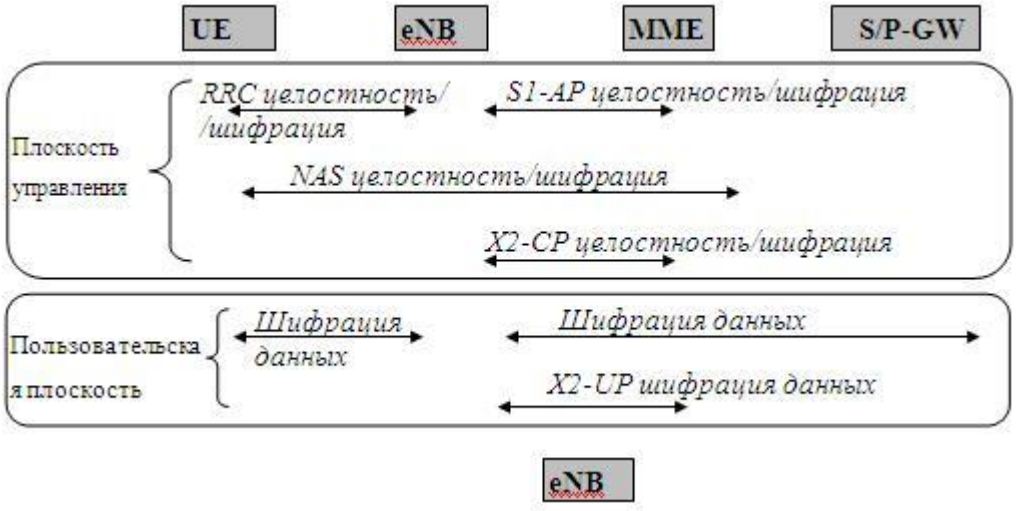


Рисунок 3.8 - Процедури безпеки в мережі E-UTRAN

3.3 Алгоритми шифрування повідомлень в LTE-A

В стандарті LTE-A для шифрування та дешифрування повідомлень використовується алгоритм представлений на рисунку 3.9.

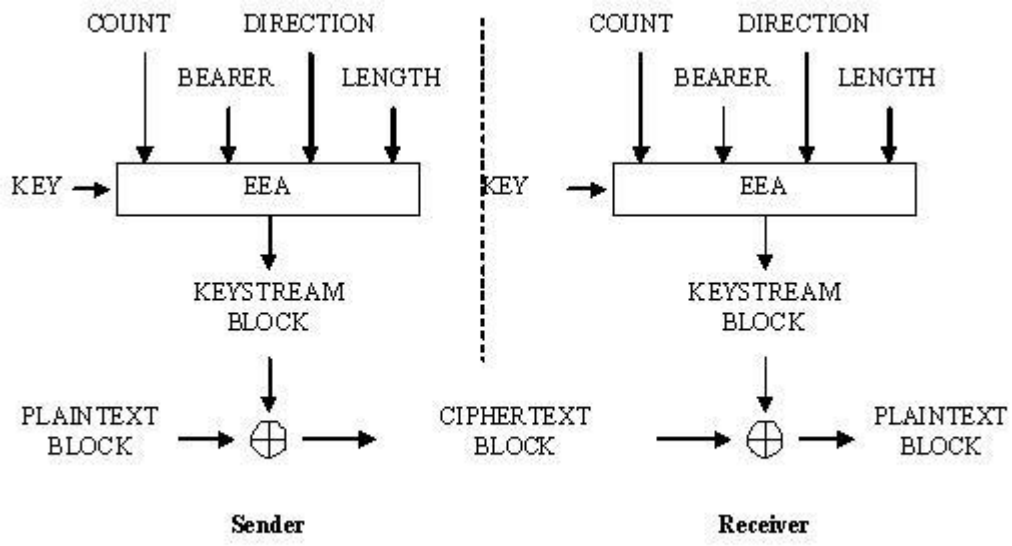


Рисунок 3.9 – Алгоритм шифрування в LTE

Вихідними параметрами для цього алгоритму є ключ шифрування KEY (128 біт), лічильник пакетів (блоків) COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і довжина шифрувального ключа LENGTH. Відповідно до обраного алгоритму шифрування EEA (EPS Encryption Algorithm) виробляється шифрувальне число KEYSTREAM BLOCK, яке при передачі складають по модулю два з зашифрованих вихідним текстом блоку PLAINTEXT BLOCK [8].

При дешифрування на приймальному кінці повторно роблять цю ж операцію.

Процедура захисту цілісності повідомлення складається в генерації заголовку MAC (Message Authentication Code) (32 біта), що додається до пакету, що передається. Алгоритм генерації MAC і перевірки цілісності отриманого

пакета шляхом порівняння XMAC з MAC (вони повинні співпадати) відображено на рисунку 3.10 [8].

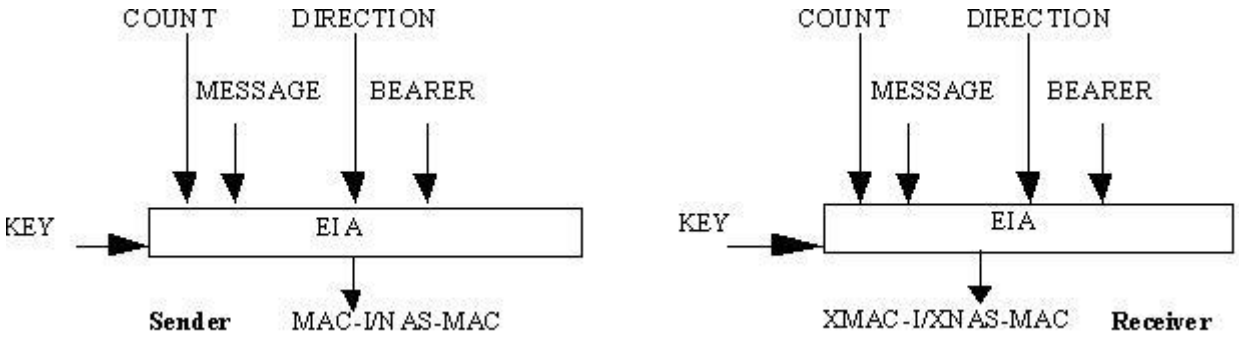


Рисунок 3.10 – Алгоритм перевірки цілісності

В алгоритмі EIA (EPS Integrity Algorithm) використаний ключ цілісності KEY (128 біт), лічильник повідомлень COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і саме повідомлення MESSAGE.

3.4 Алгоритм конфіденційності EEA2 в LTE-A

Послідовність блоків 128-бітових лічильників, необхідних для режиму CTR T1, T2, ..., Ti, ... будується наступним чином. Найбільш значущі 64 біти T1 складаються з COUNT [0] .. COUNT [31] | | BEARER [0] .. BEARER [4] || НАПРЯМКИ || 026 (тобто 26 нульових біт). Ці вхідні значення записуються з найбільш значущого біта ліворуч до найменшого значущого біта праворуч, так, наприклад, COUNT [0] є найбільш значущим бітом T1. Найменш значущими 64 бітами T1 є всі 0 [8].

Потім наступні блоки лічильників отримують шляхом застосування стандартної цілочисельної функції mod 264 до найменш значущих 64 бітів попереднього блоку лічильників.

Для шифрування корисного навантаження за допомогою AES-CTR, шифрування розділяє відкритий текст PT на 128-бітові блоки. Останній блок не повинен обов’язково бути 128 біт, він може бути й меншим [10].

PT = PT [1] PT [2] ... PT [n]

Для кожного блоку PT виконується XOR з блоком потоку ключів для генерації шифрованого тексту, CT. Шифрування AES кожного блоку лічильників призводить до отримання 128 бітів потоку ключів. Найбільш значущі 64 біти блоку T лічильника ініціалізуються, після чого йдуть 64 біти, які є 0. Ця частина лічильника T є значенням, яке збільшується на один mod 264 для створення наступних блоків лічильників кожен з яких отримав ще 128 біт потоку. Шифрування n блоків відкритого тексту можна представити так [8]:

T := COUNT || BEARER || DIRECTION || 026 ||

T0(T0 - 64 біта, які дорівнюють 0. Він представляє частину блоку лічильника T, який буде збільшувати mod 264).

FOR i := 1 to n-1 DO

CT[i] := PT[i] XOR AES(T)

T0 := T0 + 1

END

CT[n] := PT[n] XOR TRUNC(AES(T))

Функція AES() виконує шифрування AES під керуванням ключа конфіденційності. Функція TRUNC() обрізає останній результат операції AES шифрування до тієї ж довжини, що й остаточний блок відкритого тексту, повертаючи найбільш значущі біти [10].

Операція дешифрування схожа на шифрування і важливо відзначити, що AES-CTR використовує лише операцію шифрування AES (як для шифрування, так і для розшифрування), що робить реалізацію AES-CTR меншою, ніж реалізація багатьох інших режимів AES.

В даному розділі було проаналізовано та досліджено алгоритми захисту в мереж LTE а саме способи та алгоритми захисту аутентифікації, захисту інформації абонента, а також найголовніше – алгоритми захисту інформації, яка передається в мережі.

4. ОПИС РОЗРОБЛЕНОГО ПРОГРАМНОГО ПРОДУКТУ

4.1 Призначення та опис програмного продукту

Даний програмний продукт призначений для емуляції функціонування безпроводової мережі технології LTE-A на прикладі аутентифікації користувача в мережі та обміну повідомленнями з іншими користувачами у захищеному режимі. В програмі були використані алгоритми шифрування та цілісності інформації подібні до тих алгоритмів захисту, які використовуються в технології LTE-A.

Розроблена програма реалізує такі функції:

- авторизація абонента в мережі за допомогою логіна та пароля;
- реєстрація в мережі за номером абонента;
- перегляд вхідних та вихідних повідомлень;
- відправлення повідомлень іншим користувачам мережі;
- захист персональних даних користувача;
- шифрування повідомлень, що передаються в мережі.

Відповідно до проаналізованої структури безпроводової мережі LTE-A та її функціонування - розроблений програмний продукт представляє собою емулятор безпроводової мережі, яка складається з абонентських терміналів – тобто сам інтерфейс користувача програми, який доступний для будь-якого користувача, а також з бази даних, де зберігаються всі дані про користувача та зашифровані повідомлення, а також з сервера, який обробляє запити та виконує обслуговування користувачів в мережі.

Інтерфейс користувача написаний мовою програмування C# з використанням фреймворку .NET (рисунок 4.1).

Робота серверної частини забезпечується SQL сервером і відповідно використовуються SQL для управління базою даних(рисунок 4.2).

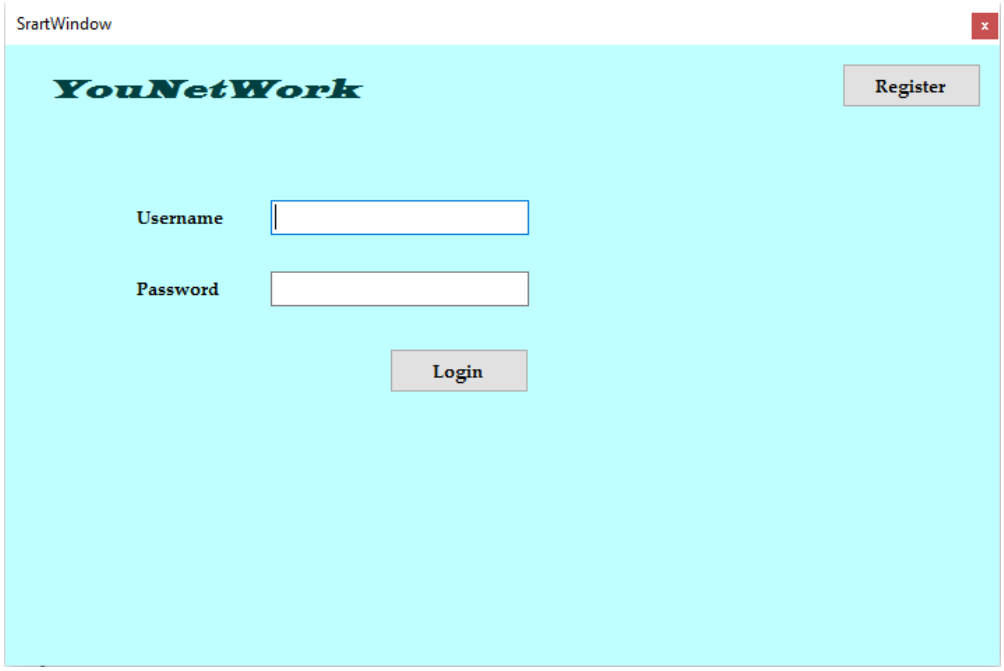


Рисунок 4.1 – Початкова сторінка інтерфейсу користувача

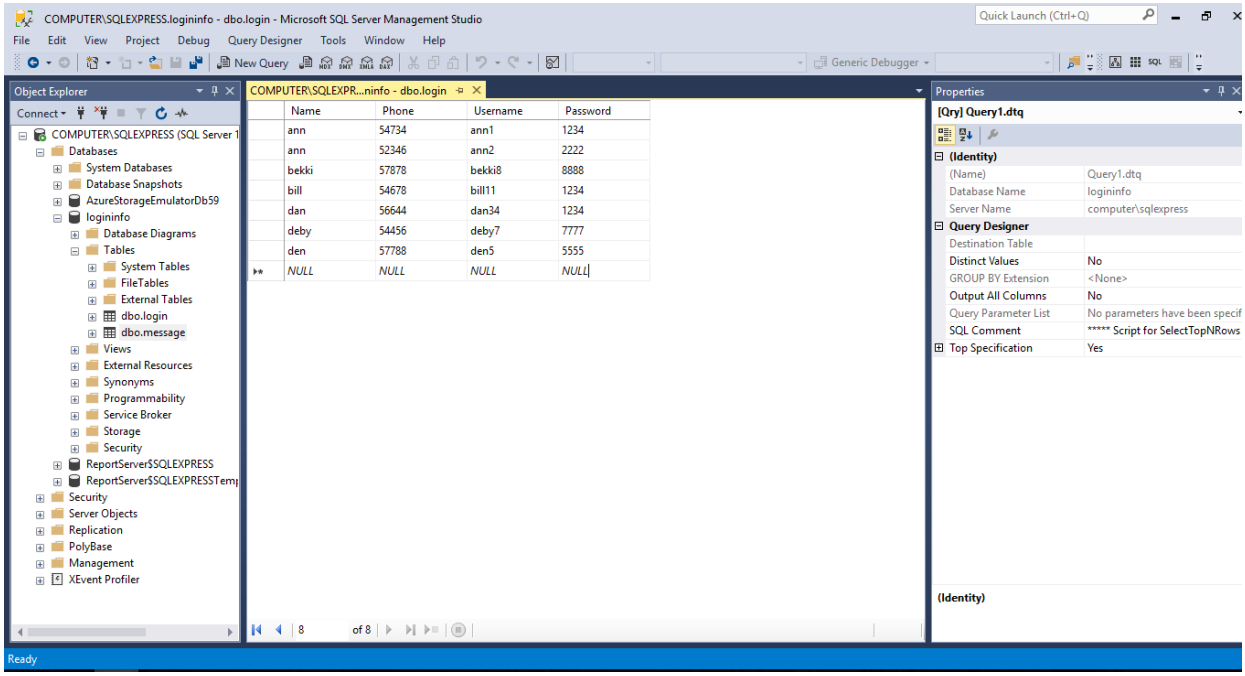


Рисунок 4.2 – База даних користувачів мережі

4.2 Опис методів, що реалізовані в програмі

Розроблена програма складається з 5 програмних модулів:

- Program;
- StartWindow;
- Register;

- MessageBox;
- WriteMessage.

Program – основна програма, яка запускає графічний інтерфейс мережі, об’єднуючи всі модулі та базу даних.

StartWindow – модуль початкового вікна, який відображає графічний інтерфейс вхідного вікна, а також містить функції зчитування та обробки введених користувачем логіну та пароля, виконує виведення повідомлення про помилку, при некоректних даних, забезпечує перехід на інтерфейс реєстрації.

Метод *Button_LogIn* зчитує інформацію з полів логіну та паролю і відправляє запит на сервер чи є введені дані в базі даних, якщо дані співпадають – авторизація пройшла успішно. Якщо ж дані не співпадають, то виводиться повідомлення про помилку.

Метод *Button_Register* обробляє натискання на кнопку Register та завантажує вікно реєстрації.

Register – модуль, що відображає графічний інтерфейс вікна реєстрації, а також перевіряє коректність введених даних для реєстрації та в разі помилки виводить відповідне повідомлення.

Метод *Button_Save* обробляє введену інформацію для реєстрації та відправляє її на сервер в базу даних, якщо все коректно, в іншому випадку формується повідомлення про помилку.

Метод *Button_BackToForm1* виконує повернення на початкову сторінку авторизації.

MessageBox – модуль вікна власного кабінету абонента в мережі. Реалізує виведення на екран вхідних та вихідних повідомлень користувача, а також надає можливість перейти до написання повідомлення. Виведенню повідомлень на екран передує зчитування відповідної інформації з бази даних та дешифрування повідомлень.

Метод *Button_Input* виконує виведення вхідних повідомлень. Для цього на сервер в базу даних відправляється відповідний запит. Зчитані дані з бази даних дешифруються і виводяться на екран.

Метод *Button_Output* виконує виведення надісланих повідомлень і аналогічно до попереднього методу виконує запит в базу даних, а потім дешифрацію.

Метод *Button_WriteMessage* викликає вікно для відправлення повідомлень.

Метод *Button_BackToForm1* виконує вихід абонента з мережі та повернення на вікно авторизації.

Метод *Decryption* – реалізує алгоритм шифрування повідомлення.

WriteMessage – модуль, що здійснює надсилання повідомлення. Він забезпечує перевірку адресної інформації і в разі помилки виводить відповідне повідомлення, якщо ж все добре – повідомлення шифрується і відправляється на сервер.

Метод Button_Send виконує перевірку введених даних про адресанта і якщо дані коректні – шифрує та надсилає повідомлення на сервер.

Метод Button_Back – виконує повернення до власного кабінету абонента.

Метод Encryption – реалізує алгоритм дешифрування повідомлення.

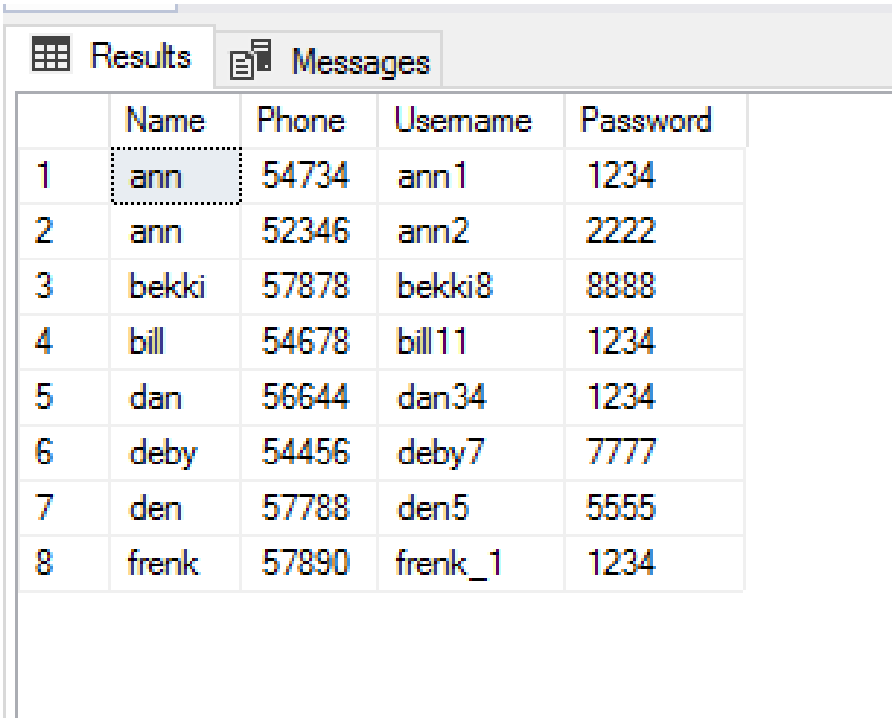
4.3 Опис бази даних, що використовується в програмі

В даній розробці для роботи з базою даних використовується SQL, для підключення бази даних до програми використовується SQL сервер, який власне і оброблює всі запити, які надсилаються з програми.

Для коректної роботи всієї програми було створено базу даних loginfo, яка складається двох таблиць: login і message.

Інформація про всіх абонентів, які зареєстровані в мережі зберігається в таблиці login бази даних loginfo. Таблиця містить 4 поля: Name, Phone,

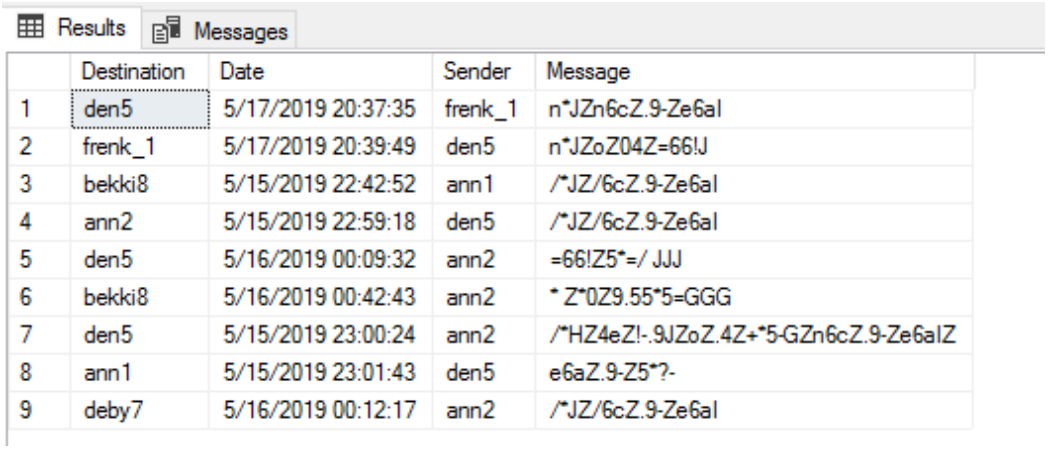
Username, Password, в кожному з яких відповідно зберігається ім'я користувача, номер абонента, його користувацьке ім'я (логін) та пароль. Структура інформації про зареєстрованих користувачів представлена на рисунку 4.3.


Results Messages

	Name	Phone	Username	Password
1	ann	54734	ann1	1234
2	ann	52346	ann2	2222
3	bekki	57878	bekki8	8888
4	bill	54678	bill11	1234
5	dan	56644	dan34	1234
6	deby	54456	deby7	7777
7	den	57788	den5	5555
8	frenk	57890	frenk_1	1234

Рисунок 4.3 – Структура інформації про зареєстрованих абонентів

Таблиця бази даних message також має 4 поля: Destination, Date, Sender, Message, де відповідно зберігається інформація про те кому, коли, ким і яке повідомлення було надіслане (рисунок 4.4). Проте повідомлення у базі даних зберігаються у зашифрованому вигляді.


Results Messages

	Destination	Date	Sender	Message
1	den5	5/17/2019 20:37:35	frenk_1	n*JZn6cZ.9-Ze6aI
2	frenk_1	5/17/2019 20:39:49	den5	n*JZoZ04Z=66!J
3	bekki8	5/15/2019 22:42:52	ann1	/*JZ/6cZ.9-Ze6aI
4	ann2	5/15/2019 22:59:18	den5	/*JZ/6cZ.9-Ze6aI
5	den5	5/16/2019 00:09:32	ann2	=66!Z5*=/ JJJ
6	bekki8	5/16/2019 00:42:43	ann2	* Z*0Z9.55*5=GGG
7	den5	5/15/2019 23:00:24	ann2	/*HZ4eZ!-.9JZoZ.4Z+*5-GZn6cZ.9-Ze6aIZ
8	ann1	5/15/2019 23:01:43	den5	e6aZ.9-Z5*?-
9	deby7	5/16/2019 00:12:17	ann2	/*JZ/6cZ.9-Ze6aI

Рисунок 4.4 – Структура інформації про переслані повідомлення

4.4 Опис інтерфейсу користувача

В розробленій програмі найпершою завантажується сторінка авторизації (рисунок 4.5), яка містить в собі назву мережі, поля для введення логіну та паролю, а також кнопки входу та реєстрації.

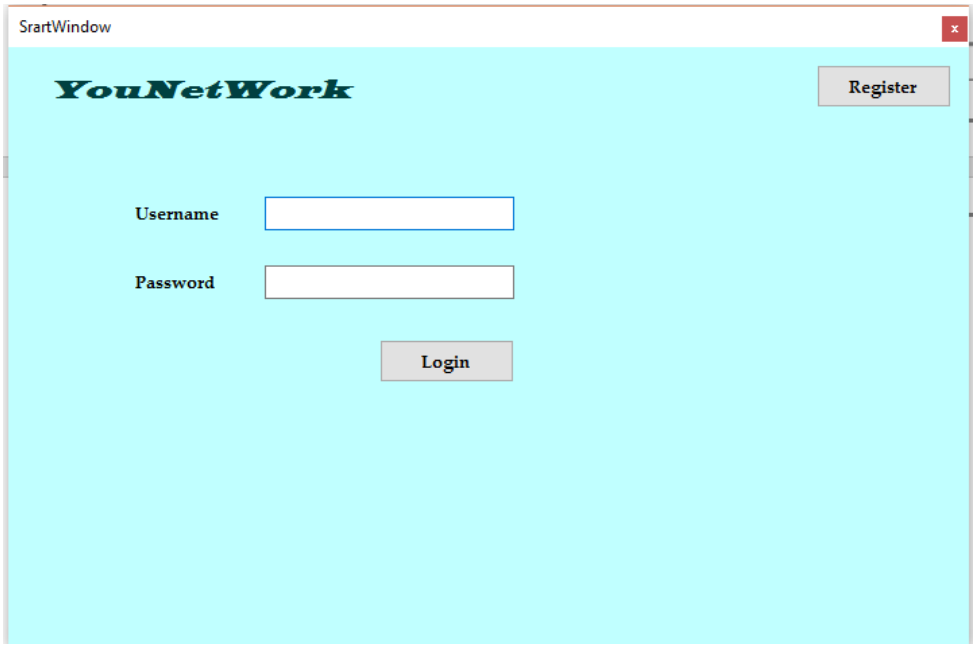


Рисунок 4.5 – Вікно авторизації

Якщо натиснути на кнопку реєстрації – користувач перейде на сторінку для реєстрації (рисунок 4.6), де йому потрібно заповнити 4 поля: ім’я, абонентський номер, користувацьке ім’я та пароль. Після натискання кнопки зберегти – введена інформація обробляється і в разі коректності – зберігається. Якщо ж були введені некоректні дані для реєстрації, то виводиться відповідне повідомлення про помилку. Ім’я має бути введене з великої букви, абонентський номер та ім’я користувача в мережі мають бути унікальними, якщо такі дані вже є в мережі, то відповідно буде виведене повідомлення про помилку, пароль має складатись з 4 символів, введення яких відбувається у прихованому режимі. Кнопка повернення назад дозволяє перейти на початкову сторінку і ввести дані для входу до персонального кабінету (рисунок 4.7).

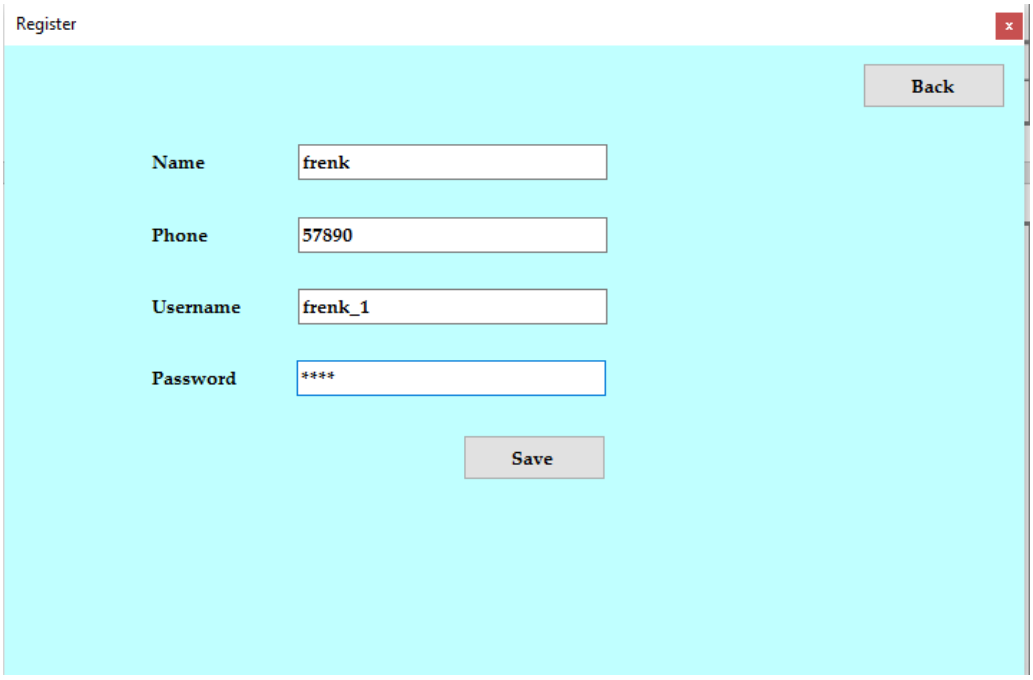


Рисунок 4.6 – Вікно реєстрації абонента

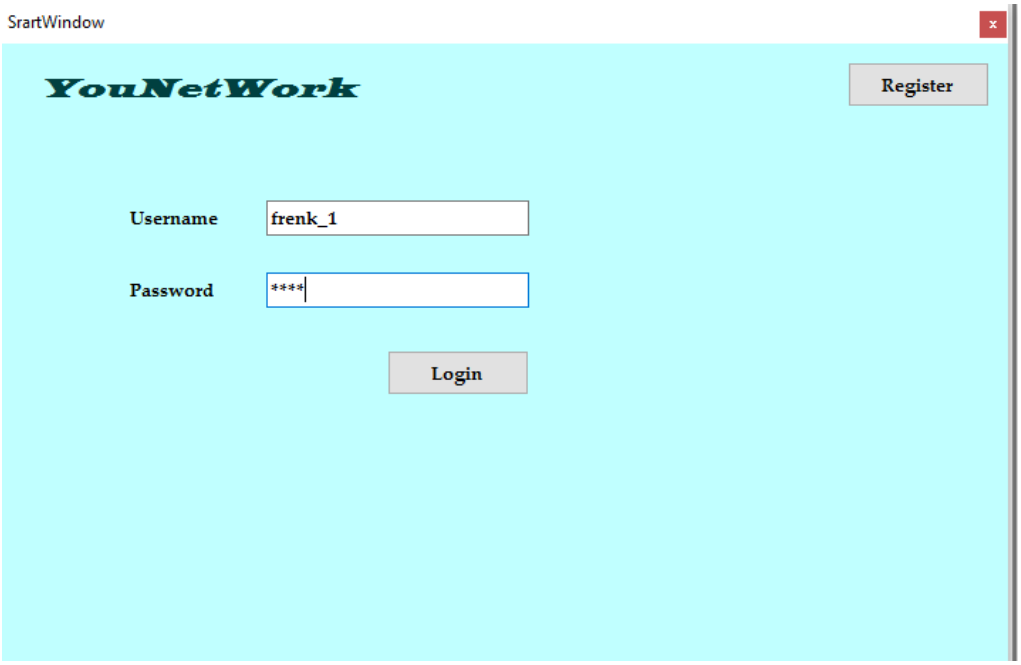


Рисунок 4.7 – Введення вхідних даних

В персональному кабінеті (рисунок 4.8) в лівому верхньому кутку висвічується користувацьке ім’я абонента, також є панель управління, що містить в собі 4 кнопки: вхідні повідомлення, вихідні повідомлення, відправка повідомлення та вихід.

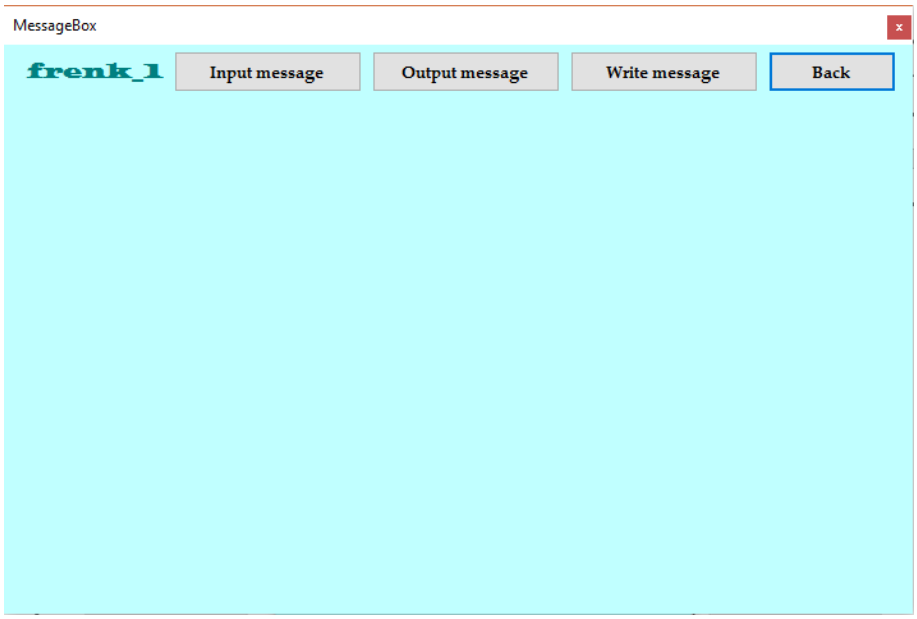


Рисунок 4.8 – Персональний кабінет абонента

Натиснувши кнопку написати повідомлення користувач переходить у вікно відправки повідомлення, де має ввести кому і що він хоче надіслати та натиснути відповідну кнопку. Для повернення у попереднє вікно можна натиснути кнопку у правому верхньому кутку (рисунок 4.9).

Рисунок 4.9 – Вікно відправки повідомлення

Після того, як користувач ввів коректні дані адресанта і відправив повідомлення, відкривши вихідні повідомлення, буде відображено відповідне надіслане повідомлення (рисунок 4.10).

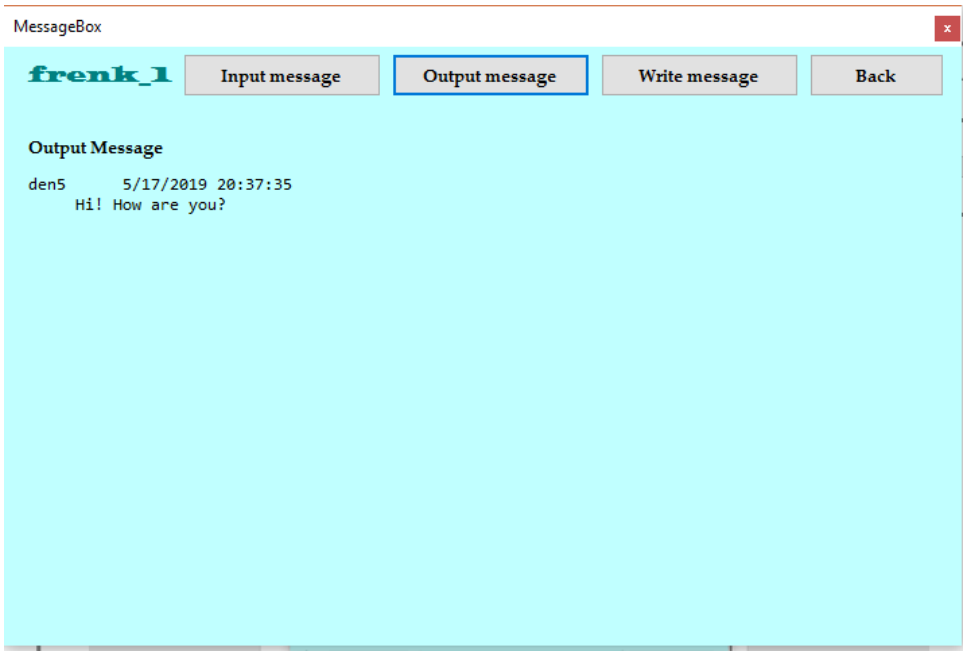


Рисунок 4.10 – Відображення надісланого повідомлення

Зайшовши на сторінку адресата та відкривши вхідні повідомлення можна поюачити, що повідомлення успішно доставлене (рисунок 4.11).

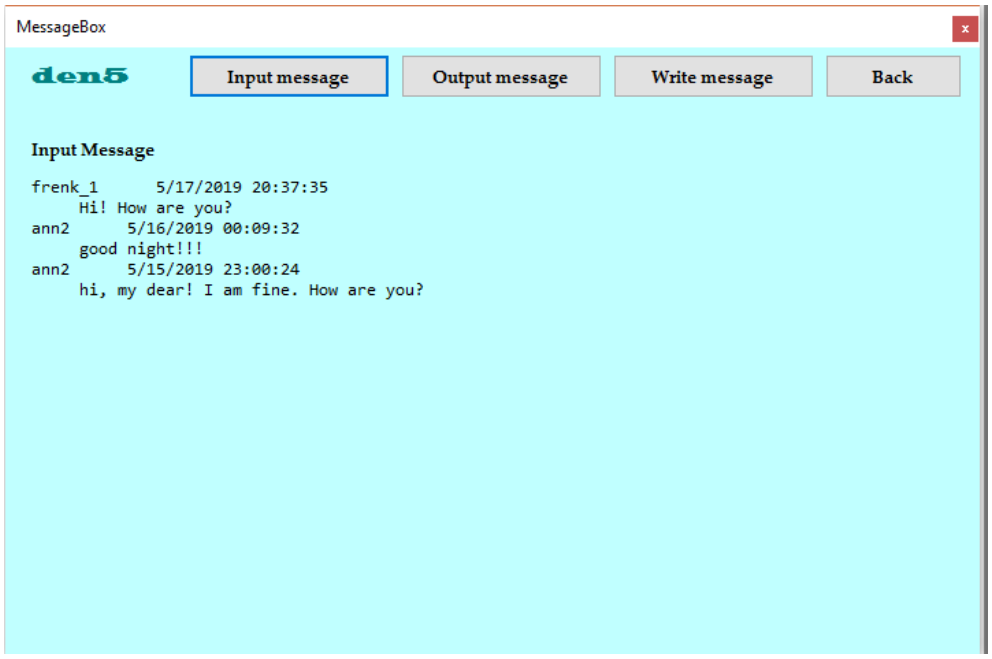


Рисунок 4.11 – Відображення вхідних повідомлень

При неправильно введених даних: неправильне ім’я користувача чи пароль чи введення неіснуючого користувача – буде виводитись відповідне повідомлення про помилку (рисунок 4.12, рисунок 4.13).

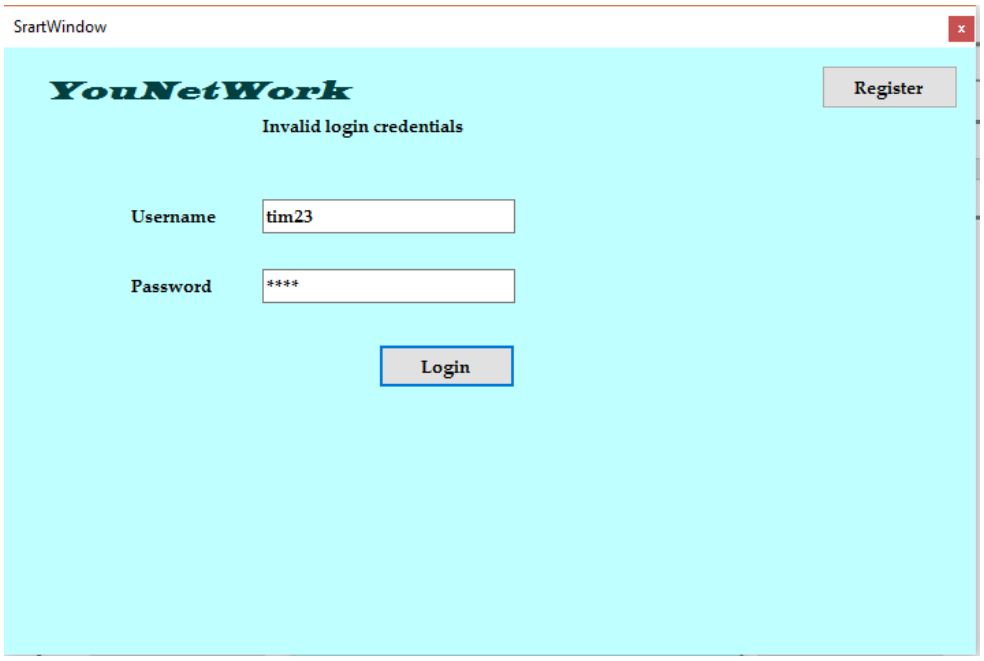


Рисунок 4.12 – Повідомлення про неправильні дані для авторизації

Рисунок 4.13 – Повідомлення про неправильно введеного адресата

В розділі було представлено та проаналізовано розроблений програмний продукт для дослідження роботи та захисту інформації в безпроводовій мережі мобільного зв'язку. Було представлено інтерфейс користувача та описано як ним користуватись.

Розроблена програма дозволяє користувачу зареєструватися в мережі та авторизуватись, також абонент мережі може надсилати повідомлення іншим абонентам мережі, а також переглядати свої повідомлення (вхідні та надіслані). Також програма застосовує алгоритм шифрування для повідомлень, які передаються в мережі. Перед тим як відправити дані в базу даних вони шифруються, а коли користувач їх відкриває, то вони проходять процедуру розшифрування і вже відображаються адресату в тому вигляді, в якому вони були відправлені адресантом.

Таким чином забезпечується надійний захист інформації, яка передається у відкритому каналі безпроводової мережі.

ВИСНОВКИ

В дипломному проекті досліджено та проаналізовано безпроводову комп`ютерну мережу технології LTE-A, розроблено структуру даної мережі та алгоритми захисту даних користувача та інформації, які передаються в мережі. На основі досліджень та аналізу розроблено програму, яка емулює процес авторизації абонента в мережі, а також пересилання ним повідомлень в захищеному режимі.

Розроблена програма дозволяє зберігати дані користувачів при їх реєстрації в мережі, потім через ці дані користувачу надається доступ до ресурсів мережі. Також дана програма дозволяє виконували обмін повідомленнями між авторизованими користувачами мережі в захищеному режимі, що забезпечується застосуванням алгоритмів цілісності та шифрування повідомлень, які пересилаються в мережі. Використання цих алгоритмів дозволяє підвищити надійність та захист обміну повідомленнями в мережі, запобігає викраденню чи нелегальному використанню даних про користувачів, що підвищує довіру користувачів до мережі та збільшує попит на неї.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Степутин А. Н. Мобильная связь на пути к 6G. В 2 Т. Том1 / А. Н. Степутин, А Д. Николаев. – 2-е изд. – Москва-Вологда: Инфра-Инженерия, 2018 – 384 с. : ил
2. LTE – что это такое и зачем оно нужно – [Електроннийресурс]. - Режимдоступу: http://www.techno-guide.ru/informatsionnye-tekhnologii/mobilnaya-svyaz/lte-chto-eto-takoe-i-zachem-ono-nuzhno.html
3. LTE – [Електроннийресурс]. –Режимдоступу: https://ru.wikipedia.org/wiki/LTE#cite_ref-4
4. «Voice and SMS in LTE Technology White Paper, Rohde & Schwarz, 2011»
5. Общие сведения о технологии LTE-Advanced – [Електроннийресурс]. – Режимдоступу: http://1234g.ru/4g/lte-advanced/obshchie-svedeniya-o-tekhnologii-lte-advanced
6. LTE-Advanced – [Електроннийресурс]. –Режимдоступу: https://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced
7. Принципы построения и функционирования сетей LTE – [Електроннийресурс]. –Режимдоступу: http://1234g.ru/4g/lte/printsip-raboty-seti-lte/printsipy-postroeniya-i-funktsionirovaniya-setej-lte
8. Безопасность в сетях LTE – [Електроннийресурс]. –Режимдоступу: http://1234g.ru/4g/lte/printsip-raboty-seti-lte/bezopasnost-v-setyakh-lte
9. New Network Security Challenges in LTE – [Електроннийресурс]. – Режимдоступу: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.symantec.com/content/en/us/enterprise/white_papers/heavy-reading-authentication-as-a-service_WP.en-us.pdf
10. EPS Confidentiality and Integrity mechanisms Algorithmic Approach – [Електроннийресурс]. –Режимдоступу: chrome-

extension://oemmndcbldboiebfnladdacbdfmadadm/https://pdfs.semanticscholar.org/e3f7/3cc95afb5e7deb11de253cc80c6275283be7.pdf