Харківський національний економічний університет
імені Семена Кузнеця

ЗВІТ
З ВИКОНАННЯ Лабораторної роботи №6

за дисципліною: *"Безпека та аудит бездротових та рухомих мереж"*

На тему: «Структура логічних каналів управління і алгоритми функціонування систем GSM»

Варіант № 4

Виконав: студент факультету Інформаційних технологій

3 курсу, спец. Кібербезпека,

групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:

Лимаренко В'ячеслав Володимирович

ХНЕУ ім. С. Кузнеця
2024

Мета: Вивчити структуру логічних каналів управління і алгоритми функціонування систем GSM по встановленню вихідного і вхідного з’єднань.

Завдання:

1. Вивчити структуру логічних каналів управління.
2. Вивчити алгоритм встановлення вихідного з’єднання (MS=>BTS, МС=>БС).
3. Вивчити алгоритм встановлення вхідного з’єднання (BTS=>MS, БС=>МС).
4. Вивчити механізми безпеки.
5. Скласти звіт.

Характеристика логічних каналів управління

В стандарті GSM використовується 4 типи ЛКУ:

- КПСУ (BCCH) - канал передачі сигналів управління, використовується для синхронізації та передачі загальної інформації про стільник.
- ЗКУ (CCCH) - загальний канал управління, використовується для виклику абонента, запиту на виділення ІКУ, дозволу доступу до каналу зв'язку.
- ІКУ (SDCCH) - індивідуальний канал управління, використовується для дуплексного зв'язку між МС та БС.
- СКУ (ACCH) - суміщений канал управління, використовується для передачі команд управління та інформації про статус МС.

Контрольні запитання та відповіді на них:

1. Види логічних каналів управління в стандарті GSM та їхня характеристика.
   В GSM використовується 4 типи ЛКУ, як описано в розділі 2.
2. Поясніть структуру 51-кадрового мультикадру.
   51-кадровий мультикадр використовується для передачі сигналів ЛКУ та даних.
   Він складається з 5 груп по 10 кадрів, де один кадр залишається незайнятим.
   Кожна група починається з кадрів КПЧ, за якими йдуть кадри КУС.
   Інші 8 кадрів в кожній групі утворюють два блоки з чотирьох кадрів.
3. Поясніть алгоритм встановлення вихідного з'єднання (МС -> БС).
   3.1. МС сканує всі доступні частоти.
   3.2. МС обирає БС з найкращим сигналом.
   3.3. МС передає сигнал КПД для визначення виду обслуговування.
   3.4. БС передає МС свій код BSIC.
   3.5. МС передає IMSI та Ki для аутентифікації.
   3.6. ЦКРЗ аутентифікує абонента.
   3.7. Встановлюється з'єднання між МС та БС.
4. Поясніть алгоритм встановлення вхідного з'єднання (БС -> МС).
   4.1. ЦКРЗ передає БС сигнал виклику абонента.
   4.2. БС передає виклик в мультикадрі КПСУ/ЗКУ.
   4.3. МС підтверджує отримання виклику.
   4.4. ЦКРЗ передає МС тимчасове опереження (ТА).
   4.5. МС вимірює ТА та передає його в ЦКРЗ.
   4.6. ЦКРЗ може переключити МС на іншу БС.
   4.7. Після аутентифікації абонента відбувається комутація речевого тракту.

5. Поясніть механізм секретності передачі даних.
   Для шифрування даних використовуються алгоритми A5 та A8. Ключ шифрування (Kc) генерується на основі Ki та випадкового числа RAND.
6. Поясніть механізм забезпечення секретності абонента.
   Для забезпечення секретності абонента використовується TMSI – тимчасовий міжнародний ідентифікаційний номер користувача. TMSI дійсний лише в межах зони розташування.
7. Характеристика процедури коригування місця знаходження
   Ця процедура гарантує, що МС буде зареєстрована в новому місцезнаходженні та зможе здійснювати та приймати дзвінки. Вона складається з кількох етапів:
   7.1. Виявлення зміни зони розташування (LAA): БС визначає, що МС знаходиться на межі зони або вже перемістився в іншу зону.
   7.2. Встановлення зв'язку з новою БС: МС отримує інформацію про сусідні БС та встановлює з'єднання з тією, що має найкращий сигнал.
   7.3. Аутентифікація та оновлення TMSI: МС проходить процес аутентифікації за допомогою IMSI та Ki, після чого отримує новий TMSI від нової зони розташування.
8. Яка інформація вважається секретною?
   В стандарті GSM наступна інформація вважається секретною:
   8.1. Ідентифікаційна інформація абонента: IMSI, TMSI, номер телефону.
   8.2. Дані аутентифікації: Ki.
   8.3. Зміст розмови: Шифрується алгоритмами A5 та A8.
   8.4. Місцезнаходження абонента: Забезпечується TMSI та процедурою коригування місця знаходження.

Висновок:
Стандарт GSM використовує логічні канали управління та різні алгоритми для забезпечення ефективної роботи мережі мобільного зв'язку. ЛКУ відповідають за передачу сигналів управління, а алгоритми встановлення з'єднання дозволяють здійснювати та приймати дзвінки. При виконанні лабораторної роботи я дізнався про застосування механізмів безпеки, таких як шифрування даних та забезпечення секретності абонента, є важливим для захисту інформації юзерів.