**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH**

**KHOA ĐIỆN - ĐIỆN TỬ**


**MÔN HỌC: MẠNG VÔ TUYẾN VÀ DI ĐỘNG**

# EXTENDED COVERAGE GLOBAL SYSTEM FOR MOBILE COMMUNICATION

**(EC-GSM-IoT)**

## GVHD: ThS Trương Ngọc Hà

**Họ và tên SV:**

| | |
|---|---|
| **Trần Thanh Ngọc** | **19119204** |
| **Phan Công Danh** | **19119160** |
| **Võ Minh Hậu** | **19119174** |
| **Phạm Hải Nguyên** | **19119205** |
| **Nguyễn Hà Nhật Linh** | **19119190** |

**Tp. Hồ Chí Minh, tháng 12 năm 2022**

# MỤC LỤC

# DANH MỤC HÌNH

# DANH MỤC BẢNG

# DANH MỤC VIẾT TẮT

| | |
|---|---|
| AKA | Authentication and Key Agreement |
| AoC | Advice of Charge |
| AUC | Authentication Center |
| BIE | Base Station Interface Equipment |
| BSC | Base Station Controller |
| BSS | Base Station Subsystem |
| BTS | Base Transceiver Station |
| CC | Coverage Class |
| CDMA | Code Division Multiple Access |
| CEPT | European Conference of Postal and Telecommunications Administrations |
| CGI | Cell Global Identity |
| CI | Cell Identity |
| CS | Circuit-Switched |
| CSPDN | Circuit Switched Public Data Network |
| DCCH | Dedicated Control Channel) |
| DTMF | Dual-tone multifrequency |
| EC | Extended Coverage |
| EIR | Equipment Identity Register |
| GMSC | Gate Mobile Services Switching Center |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| HLR | Home Location Register |
| IMEI | International Mobile Equipment Identity |

| | |
|---|---|
| IMSI | International Mobile Subscriber Identity |
| IoT | Internet of Things |
| ISDN | Integrated Services Digital Network |
| IWF | Internet Working Fusions |
| LAC | Location Area Code |
| LAI | Location Area Identity |
| LTE | Long Term Evolution |
| MCC | Mobile Country Code |
| ME | Mobile Equipment |
| MNC | Mobile Network Code |
| MS | Mobile Station |
| MSC | Mobile Services Switching Center |
| MSISDN | Mobile Station International Subscriber Directory Number. |
| MSRN | Mobile Station Roaming Number |
| NB | Narrow Band |
| OMC | Operation and Maintenance Center |
| OSS | Operation Subsystem |
| PACCH | Package Associated Control |
| PAGCH | Packet Access Grant Channel |
| PLMN | Public Land Mobile Network |
| PNCH | Packet Notification Channel |
| PPCH | Packet Paging Channel |
| PRACH | Packet Random Access Channel |
| PSPDN | Packet Switched Public Data Network |
| PSTN | Public Switched Telephone Network |

| | |
|---|---|
| PTCCH | Package Timing Control Channel |
| RAND | Random Number |
| SIM | Subscriber Identity Module |
| SS | Switching Subsystem |
| TDMA | Time Division Multiple Access |
| TMSI | Temporary Mobile Subscriber Identity |
| TRAU | Transcoder and Rate Adapter Unit |
| UE | User Equipment |
| UMTS | Universal Mobile Telecommunications System |
| VLR | Visitor Location Register |

# CHƯƠNG 1: TỔNG QUAN

## 1.1 GIỚI THIỆU

Hiện nay trong cuộc sống hàng ngày thông tin liên lạc đóng một vai trò rất quan trọng có ảnh hưởng tích cực đến nhiều mặt hoạt động của xã hội, giúp con người nắm bắt nhanh chóng các giá trị văn hoá, kinh tế, khoa học kỹ thuật rất đa dạng và phong phú.

Bằng những bước phát triển nhanh chóng và mạnh mẽ, các thành tựu công nghệ Điện Tử – Tin Học – Viễn Thông đã làm thay đổi cuộc sống con người rõ rệt, tiềm năng của ngành là rất lớn, trong đó nổi bật là lĩnh vực Thông Tin Di Động. Cùng với nhiều công nghệ khác nhau, Thông Tin Di Động đang không ngừng phát triển và đáp ứng nhu cầu thông tin ngày càng tăng cả về số lượng và chất lượng, tạo nhiều thuận lợi trong miền thời gian cũng như không gian. Chắc chắn trong tương lai, Thông Tin Di Động sẽ được hoàn thiện nhiều hơn nữa để thoả mãn nhu cầu thông tin tự nhiên của con người.

## 1.2 MỤC TIÊU VÀ GIỚI HẠN ĐỀ TÀI

### 1.2.1. Mục tiêu đề tài

Hệ thống lại và nắm rõ về hệ thống GSM bao gồm: Cấu trúc; Vùng mạng; Các đặc tính cũng như dịch vụ thuê bao GSM.

Từ nền tảng của hệ thống GSM, hiểu và phân tích được hoạt động của hệ thống EC-GSM, những lợi ích mà EC-GSM mang lại cho hệ thống GSM cơ bản.

### 1.2.2. Giới hạn đề tài

Tính phổ biến không cao của EC-GSM dẫn tới những khó khăn nhất định trong việc tìm kiếm và tiếp cận những tài liệu liên quan.

## 1.3 PHƯƠNG PHÁP NGHIÊN CỨU

Để thực hiện đề tài này, chúng tôi đã kết hợp các phương pháp nghiên cứu sau:

- Phương pháp phân tích.
- Phương pháp tổng hợp.
- Phương pháp kết luận.

## 1.4 ĐỐI TƯỢNG NGHIÊN CỨU

- Tìm hiểu tổng quan về mạng GSM.
- Tìm hiểu chi tiết về EC-GSM trong lĩnh vực IoT.

# CHƯƠNG 2: GSM

## 2.1 GIỚI THIỆU GSM

### 2.1.1 Định nghĩa

GSM (Global System for Mobile Communication) là hệ thống thông tin di động toàn cầu, một mạng di động kỹ thuật số phổ biến được sử dụng rộng rãi bởi người dùng điện thoại di động ở châu Âu và các nước khác trên khắp thế giới. GSM sử dụng biến thể đa truy nhập phân chia thời gian (TDMA – Time Division Multiple Access) và được sử dụng rộng rãi nhất trong 3 công nghệ điện thoại không dây kỹ thuật số là TDMA, GSM và CDMA [1].

GSM là tiêu chuẩn thế hệ thứ hai (Second Generation) cho các mạng di động. GSM hoạt động trên ba dải tần số sóng khác nhau: băng tần 900MHz được sử dụng cho hệ thống GSM gốc; băng tần 1800MHz được thêm vào để tăng số lượng thuê bao và tần số 1900MHz được sử dụng chủ yếu ở nước Mỹ [1].

### 2.1.2 Lịch sử hình thành

Vào đầu thập niên 1980 tại châu Âu, người ta phát triển một mạng điện thoại di động chỉ sử dụng trong một vài khu vực. Đến năm 1982, nó được chuẩn hoá bởi Hội nghị Quản lý Bưu chính Viễn thông Châu Âu CEPT (European Conference of Postal and Telecommunications Administrations) và tạo ra GSM với mục đích sử dụng chung cho toàn châu Âu. Công nghệ GSM được xây dựng và đưa vào sử dụng đầu tiên ở Phần Lan. Cùng năm đó, dải tần số chuẩn GSM được mở rộng từ 900 MHz lên 1.800 MHz [1].

Vào cuối năm 1993, có hơn 1 triệu thuê bao sử dụng mạng GSM của 70 nhà cung cấp dịch vụ trên 48 quốc gia. Năm 1995, Hệ thống GSM không chỉ được phủ sóng ở các thành phố lớn mà còn được phát triển rộng ra các vùng nông thôn. Năm 2010, GSM chiếm 80% thị trường di động toàn cầu. Tuy nhiên, một số nhà mạng

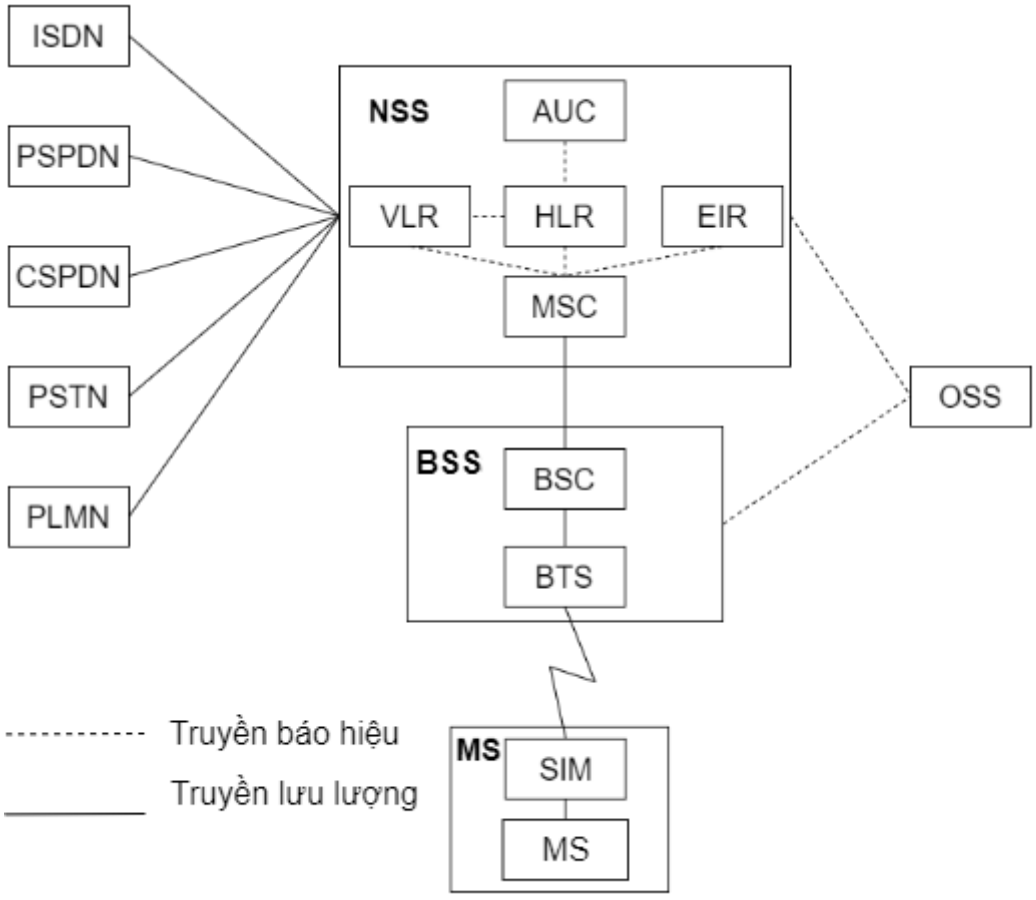
viễn thông đã ngừng hoạt động mạng GSM như ở Úc và Singapore để chuyển sang hệ thống mạng tiên tiến hơn là 3G. 4G, 5G [1].

## 2.2 CẤU TRÚC HỆ THỐNG GSM

Hệ thống GSM có thể được chia thành 4 phần:

- Phân hệ chuyển mạch (SS: Switching Subsystem).
- Phân hệ trạm gốc (BSS: Base Station Subsystem).
- Phân hệ khai thác (OSS: Operation Subsystem).
- Trạm di động (MS: Mobile Station) [1].

Hình 2.1 mô tả cấu trúc của hệ thống GSM [1].




**Hình 2.1**: Cấu trúc hệ thống GSM

### 2.2.1 Phân hệ chuyển mạch

Phân hệ chuyển mạch SS bao gồm các chức năng chuyển mạch chính của GSM cũng như các cơ sở dữ liệu cần thiết cho số liệu thuê bao và quản lý di động của các thuê bao. Phân hệ chuyển mạch có chức năng chính là quản lý thông tin giữa những người sử dụng mạng GSM với nhau và với những mạng khác [1].

Phân hệ chuyển mạch bao gồm các khối chức năng sau:

- Trung tâm chuyển mạch các dịch vụ di động (MSC: Mobile Services Switching Center).
- Bộ ghi định vị tạm trú (VLR: Visitor Location Register).
- Bộ ghi định vị thường trú (HLR: Home Location Register).
- Trung tâm nhận thực (AUC: Authentication Center).
- Bộ nhận dạng thiết bị (EIR: Equipment Identity Register) [1].

#### 2.2.1.1 Trung tâm chuyển mạch các dịch vụ di động MSC

MSC thường là một tổng đài lớn điều khiển và quản lý một số bộ điều khiển trạm gốc (BSC: Base Station Controller) của phân hệ trạm gốc (BSS). Nhiệm vụ chính của MSC là điều phối việc thiết lập cuộc gọi đến của các thuê bao sử dụng mạng GSM. MSC giao tiếp với phân hệ BSS; mặc khác, GSM cũng giao tiếp với các mạng ngoài GSM (gọi là trung tâm chuyển mạch các dịch vụ di động cổng GMSC) [1].

Để kết nối MSC với các mạng khác cần phải thích ứng các đặc điểm truyền dẫn PLMN với các mạng đó. Các thích ứng này gọi là các chức năng tương tác IWF (Internet Working Fusions). IWF là thiết bị thích ứng thủ tục và truyền dẫn. IWF cho phép PLMN kết nối với các mạng PSTN, ISDN, PSPDN, CSPDN. IWF có thể được thực hiện kết hợp trong MSC hay có thể được thực hiện ở thiết bị riêng [1].

Để thiết lập một cuộc gọi đến người sử dụng GSM, trước hết cuộc gọi phải được định tuyến đến một tổng đài cổng GMSC mà không cần biết hiện thời thuê bao đang ở đâu. Các tổng đài cổng có nhiệm vụ lấy thông tin về vị trí của thuê bao và định tuyến cuộc gọi đến tổng đài đang quản lý thuê bao ở thời điểm hiện thời (MSC

tạm trú). Trước hết các tổng đài cổng phải dựa trên số thoại danh bạ của thuê bao để tìm đúng HLR cần thiết và truy vấn HLR này [1].

#### 2.2.1.2 Bộ ghi định vị thường trú HLR

Là cơ sở dữ liệu quan trọng nhất của mạng GSM, lưu trữ các số liệu và địa chỉ nhận dạng cũng như các thông số nhận thực của thuê bao trong mạng. Các thông tin lưu trữ trong HLR gồm: nhận dạng thuê bao IMSI, MSISDN, VLR hiện thời, trạng thái thuê bao, khoá nhận thực và chức năng nhận thực, số lưu động trạm di động MSRN. HLR chứa những cơ sở dữ liệu bậc cao của tất cả các thuê bao trong GSM. Những dữ liệu này được truy nhập từ xa bởi các MSC và VLR của mạng [1].

#### 2.2.1.3 Bộ ghi định vị tạm trú VLR

VLR là cơ sở dữ liệu thứ hai trong mạng GSM, được nối với một hay nhiều MSC và có nhiệm vụ lưu giữ tạm thời số liệu thuê bao của các thuê bao hiện đang nằm trong vùng phục vụ của MSC tương ứng và đồng thời lưu giữ số liệu về vị trí của các thuê bao nói trên ở mức độ chính xác hơn HLR. Các chức năng VLR thường được liên kết với các chức năng MSC [1].

#### 2.2.1.4 Trung tâm nhận thực AUC

AUC quản lý các thông tin nhận thực và mật mã liên quan đến từng cá nhân thuê bao dựa trên một khóa nhận dạng bí mật (Ki) để đảm bảo an toàn số liệu của các thuê bao được phép. Khóa Ki sẽ lưu vĩnh viễn và bí mật trong bộ nhớ có dạng Simcard ở MS (Mobile Station) [1].

Khi người dùng đăng ký thuê bao, khóa Ki sẽ được ghi nhớ vào Simcard của thuê bao cùng với IMSI. Ngoài ra khóa Ki cũng được lưu giữ tại AUC để tạo ra ba thông số (số ngẫu nhiên RAND, mật khẩu SRES, khóa mật mã Kc) để phục vụ cho quá trình nhận thực và mã hóa [1].

#### 2.2.1.5 Bộ đăng ký nhận dạng thiết bị EIR

Quản lý thiết bị di động được thực hiện bởi bộ đăng ký nhận dạng thiết bị EIR. EIR lưu giữ tất cả các dữ liệu liên quan đến phần thiết bị di động ME của trạm di động MS [1].

EIR được nối với MSC thông qua đường báo hiệu để kiểm tra thiết bị có được cho phép hay không bằng cách so sánh tham số nhận dạng thiết bị di động quốc tế IMEI (International Mobile Equipment Identity) của thuê bao gửi tới khi thiết lập thông tin với số IMEI lưu giữ trong EIR phòng trường hợp đây là những thiết bị đầu cuối bị đánh cắp, nếu so sánh không đúng thì thiết bị không thể truy nhập vào mạng được [1].

### 2.2.2 Phân hệ trạm gốc BSS

Phân hệ trạm gốc BSS thực hiện nhiệm vụ giám sát các đường ghép nối vô tuyến, liên kết kênh vô tuyến với máy phát và quản lý cấu hình của các kênh này. Đó là:

- Điều khiển sự thay đổi tần số vô tuyến của đường kết nối và sự thay đổi công suất phát vô tuyến.
- Thực hiện mã hóa kênh và tín hiệu thoại số, phối hợp tốc độ truyền thông tin.
- Quản lý quá trình chuyển giao (Handover).
- Thực hiện bảo mật kênh vô tuyến [1].

Phân hệ BSS gồm hai khối chức năng: Bộ điều khiển trạm gốc (BSC) và các trạm thu phát gốc (BTS: Base Transceiver Station) cung cấp tất cả các chức năng điều khiển và liên kết vật lý giữa MSC và BTS. Nếu khoảng cách giữa BSC và BTS nhỏ hơn 10m thì các kênh thông tin có thể được kết nối trực tiếp (chế độ Combine), ngược lại thì phải qua một giao diện A - bis (chế độ Remote). Một BSC có thể quản lý nhiều BTS theo cấu hình hỗn hợp của hai loại trên [1].

#### 2.2.2.1 Trạm thu phát gốc BTS

Một BTS bao gồm các thiết bị thu phát, anten và xử lý tín hiệu đặc thù cho giao diện vô tuyến. Có thể coi BTS là các Modem vô tuyến phức tạp có thêm một số các chức năng khác. Một bộ phận quan trọng của BTS là TRAU (Transcoder and Rate Adapter Unit: khối chuyển đổi mã và thích ứng tốc độ). TRAU là thiết bị mà ở đó quá trình mã hoá và giải mã tiếng nói đặc thù riêng cho GSM được tiến hành, ở đây cũng thực hiện thích ứng tốc độ trong trường hợp truyền số liệu. TRAU là một

bộ phận của BTS, nhưng cũng có thể đặt cách xa BTS và thậm chí trong nhiều trường hợp được đặt giữa BSC và MSC [1].

BTS có các chức năng sau:

- Quản lý lớp vật lý truyền dẫn vô tuyến.
- Quản lý giao thức cho liên kết số liệu giữa MS và BSC.
- Vận hành và bảo dưỡng trạm BTS.
- Cung cấp các thiết bị truyền dẫn và ghép kênh nổi trên giao tiếp A – bis [1].

#### 2.2.2.2 Bộ điều khiển trạm gốc BSC

Bộ điều khiển trạm gốc BSC có nhiệm vụ quản lý tất cả giao diện vô tuyến qua các lệnh điều khiển từ xa BTS và MS. Các lệnh này chủ yếu là các lệnh ổn định, giải phóng kênh vô tuyến và quản lý chuyển giao (Handover). Một phía BSC được nối với BTS, còn phía kia nối với MSC của SS. Trong thực tế BSC là một tổng đài nhỏ có khả năng tính toán đáng kể. Một BSC có thể quản lý vài chục BTS tuỳ theo lưu lượng các BTS này. Giao diện giữa BSC và MSC là giao diện A, còn giao diện giữa BSC và BTS là giao diện A – bis [1].

BSC có thể thu thập số liệu đo từ BTS và BIE ( Base Station Interface Equipment: Thiết bị giao diện trạm gốc), lưu trữ chúng trong bộ nhớ và cung cấp chúng cho OMC theo yêu cầu [1].

### 2.2.3 Phân hệ khai thác OSS

Phân hệ khai thác OSS thực hiện ba chức năng chính:

Điều khiển quản lý và bảo dưỡng OMC. OMC cho phép các nhà khai thác mạng theo dõi và kiểm tra các hành vi trong mạng như: tải của hệ thống, số lượng chuyển giao giữa các cell,... Nhờ vậy mà họ có thể giám sát được toàn bộ chất lượng dịch vụ mà họ cung cấp cho khách hàng và kịp thời xử lý sự cố. Nó có thể được thay đổi cấu hình để giảm những sự cố xuất hiện, nâng cấp mạng về dung lượng tăng vùng phủ sóng, định vị sửa chữa các sự cố hỏng hóc,… [1].

Quản lý thuê bao bao gồm các hoạt động quản lý đăng ký thuê bao, cũng như xóa thuê bao ra khỏi mạng. Tính cước các cuộc gọi, cước phí phải được tính và gửi đến thuê bao [1].

Quản lý thiết bị di động được bộ EIR thực hiện [1].

### 2.2.4 Trạm di động MS

Trạm di động là thiết bị duy nhất mà người sử dụng có thể thường xuyên nhìn thấy của hệ thống. MS có thể là: máy cầm tay, máy xách tay hay máy đặt trên ô tô. MS chứa các chức năng vô tuyến chung và xử lý cho giao diện vô tuyến, ngoài ra MS còn phải cung cấp các giao diện với người sử dụng (micro, loa, màn hình hiển thị, bàn phím để quản lý cuộc gọi) hoặc giao diện với một số các thiết bị khác (như giao diện với máy tính cá nhân, Fax...) [1].

MS có 3 chức năng chính:

- Thiết bị đầu cuối thực hiện các chức năng không liên quan đến mạng GSM.
- Kết cuối trạm di động thực hiện các chức năng liên quan đến truyền dẫn ở giao diện vô tuyến.
- Bộ thích ứng đầu cuối làm việc như một cửa nối thông thiết bị đầu cuối với kết cuối di động [1].

Trạm di động MS gồm hai phần: Module nhận dạng thuê bao SIM (Subscriber Identity Module) và thiết bị di động ME (Mobile Equipment). Để đăng ký và quản lý thuê bao, mỗi thuê bao phải có một bộ phận gọi là SIM. SIM là một module riêng được tiêu chuẩn hoá trong GSM. Tất cả các bộ phận thu, phát, báo hiệu tạo thành thiết bị ME. ME không chứa các tham số liên quan đến khách hàng, mà tất cả các thông tin này được lưu trữ trong SIM. SIM thường được chế tạo bằng một vi mạch chuyên dụng gắn trên thẻ gọi là Simcard. Simcard có thể rút ra hoặc cắm vào MS [1].

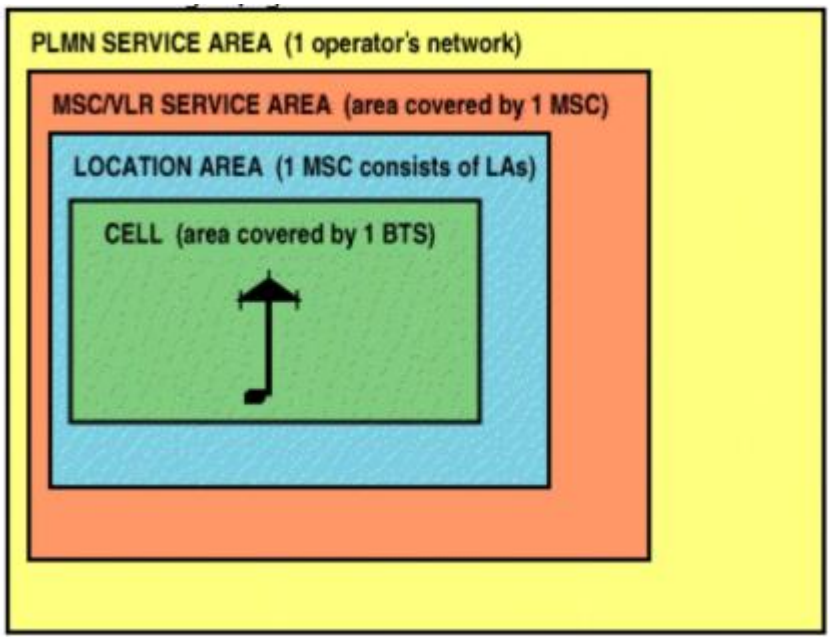
SIM đảm nhiệm các chức năng sau:

- Lưu giữ khoá nhận thực thuê bao Ki cùng với số nhận dụng trên di động quốc tế IMSI nhằm thực hiện các thủ tục nhận thực và mật mã hóa thông tin.

- Khai thác và quản lý số nhận dạng cá nhân PIN (Pers Identity Number) để bảo vệ quyền sử dụng của người sở hữu hợp pháp.
- SIM có phần cứng và phần mềm cần thiết với bộ nhớ nhỏ có thể lưu trữ thông tin. Có hai loại thông tin là Thông tin cố định (Số nhận dạng thuê bao MSISDN, IMSI; Mã khoá cá nhân Ki) và Thông tin thay đổi (Số hiệu nhận dạng vùng định vị LAI; Số nhận dạng thuê bao tạm thời TMSI) [1].

## 2.3 VÙNG MẠNG (NETWORK AREA)

Mạng GSM được tạo thành từ các vùng địa lý. Các vùng này bao gồm các ô (Cell), vùng cục bộ (Location Area), vùng dịch vụ MSC/VLR (MSC/VLR Service Area) và vùng mạng di động mặt đất công cộng (PLMN Service Area). Hình 2.2 mô tả vùng mạng GSM và các thành phần bên trong [2].

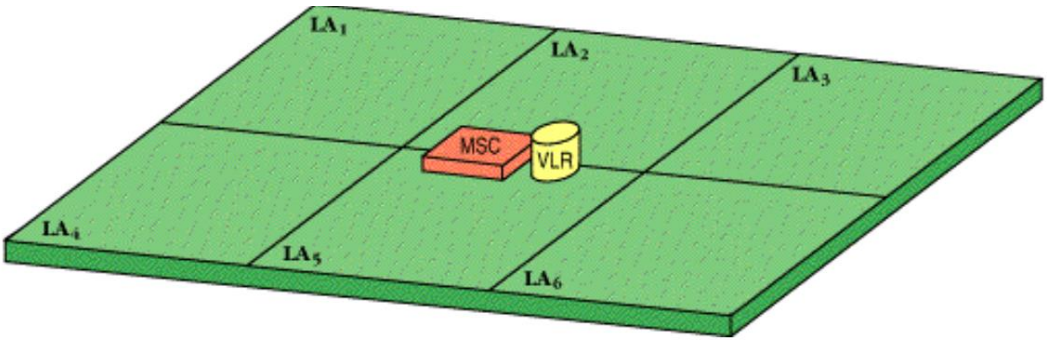



**Hình 2.2**: Vùng mạng GSM

Cell là vùng được phủ sóng bởi một trạm thu phát gốc BTS (Base Transceiver Station). BTS là thiết bị vô tuyến (máy thu phát và anten) cần thiết để phục vụ từng cell trong mạng. Hệ thống mạng GSM nhận diện từng cell thông qua số nhận dạng cell toàn cầu (CGI: Cell Global Identity) được gán cho từng cell bên trong vùng cục bộ. CGI là sự kết hợp của MCC (Mobile Country Code), MNC (Mobile Network

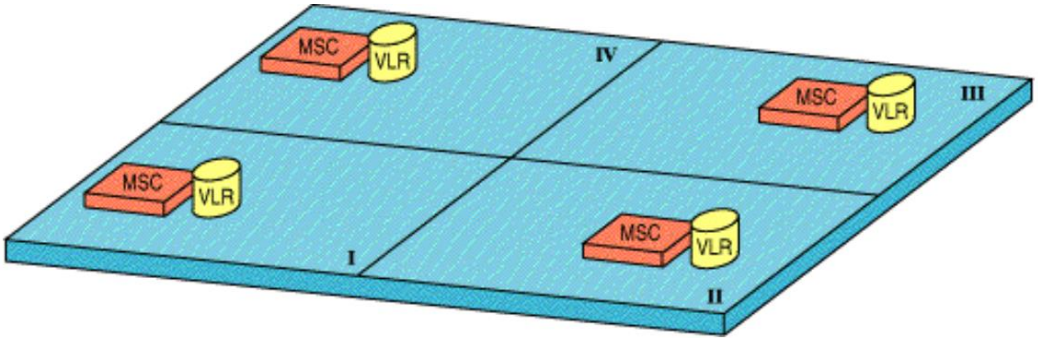
Code), LAC (Location Area Code) và CI (Cell Identity). Từ MCC, chúng ta có thể tìm ra cell nằm ở quốc gia nào. Từ MNC, ta có thể tìm ra nó thuộc về nhà điều hành mạng nào. Từ LAC, ta có thể biết nó thuộc về khu vực cục bộ nào. Cuối cùng, để xác định chính xác một cell sẽ thông qua mã CI [2].

Nhóm tập hợp các cell được gọi là vùng cục bộ LA (Location Area). LA được phục vụ bởi một hoặc nhiều bộ điều khiển trạm gốc BSC (Base Station Controller), nhưng chỉ phục vụ bởi một MSC/VLR duy nhất. Mỗi LA được gán một số nhận dạng vùng cục bộ LAI (Location Area Identity). Location Area Identity bao gồm MCC, MNC và LAC. Hình 2.3 mô tả các vùng cục bộ được phục vụ bởi một MSC/VLR [2].




**Hình 2.3:** Vùng cục bộ

Vùng dịch vụ MSC/VLR đại diện cho một phần của mạng GSM được phủ sóng bởi một MSC duy nhất và có thể truy cập được, nó đã được đăng ký trong VLR của MSC. Hình 2.4 mô tả các vùng dịch vụ MSC/VLR [2].




**Hình 2.4:** Vùng dịch vụ MSC/VLR

Vùng mạng di động mặt đất công cộng PLMN là tập hợp các khu vực dịch vụ MSC/VLR được quản lý bởi một nhà mạng. PLMN là thuật ngữ được sử dụng để mô tả tất cả các mạng không dây di động sử dụng các trạm trên mặt đất thay vì vệ tinh. PLMN được xác định bằng mã PLMN duy nhất trên toàn cầu, bao gồm MCC và MNC. Hình 2.5 mô tả các vùng mạng PLMN [2].


**Hình 2.5:** Vùng mạng di động mặt đất công cộng PLMN

## 2.4 CÁC ĐẶC TÍNH CỦA GSM

Tần số làm việc đặc trưng của GSM nằm trong khoảng từ 1850 tới 1990MHz [3].

Tần số truyền song công: là độ lớn tần số nằm giữa các kết nối uplink và downlink, có giá trị là 80MHz. Ngoài ra kênh truyền cũng có 2 tần số có giá trị tương tự nhau là 80MHz [3].

Tách kênh: Khoảng cách của các kênh truyền cho biết khoảng cách của các sóng mang liền kề. Trong GSM, khoảng cách này là 200KHz [3].

Điều chế: Điều chế là quá trình chuyển đổi dữ liệu đầu vào thành một định dạng phù hợp cho phương tiện truyền dẫn. Dữ liệu được truyền đi được giải điều

chế trở lại dạng ban đầu ở đầu nhận. GSM sử dụng phương pháp điều chế Gaussian Minimum Shift Keying (GMSK) [3].

Tốc độ truyền: Tổng tốc độ symbol cho GSM ở mức 1 bit cho mỗi symbol trong GMSK tạo ra 270,833 symbol/s. Tổng tốc độ truyền của khung thời gian là 22,8 Kbps. Nói chung GSM là một hệ thống kỹ thuật số có tốc độ bit qua mạng là 270 kbps [3].

Phương pháp truy cập: Phổ vô tuyến là một nguồn tài nguyên hạn chế được tiêu thụ và phân chia cho tất cả người dùng, GSM đã nghĩ ra sự kết hợp của TDMA / FDMA như một phương pháp để phân chia băng thông cho người dùng. Trong quá trình này, phần FDMA chia tần số của tổng băng thông 25MHz thành 124 tần số sóng mang có băng thông 200 kHz [3].

Mã hóa: Để mã hóa hoặc xử lý giọng nói, GSM sử dụng Mã hóa dự đoán tuyến tính (LPC). Công cụ này nén tốc độ bit và đưa ra ước tính về các tham số giọng nói. Khi tín hiệu âm thanh đi qua bộ lọc, nó sẽ bắt chước đường thanh âm. Ở đây, giọng nói được mã hóa ở tốc độ 13 kbps [3].

## 2.5 DỊCH VỤ THUÊ BAO GSM

Có hai loại dịch vụ cơ bản được cung cấp thông qua GSM: Telephony (dịch vụ viễn thông) và Data (dịch vụ mạng):

- Dịch vụ viễn thông chủ yếu là dịch vụ thoại cung cấp cho thuê bao khả năng liên lạc với các thuê bao khác.
- Dịch vụ mạng cung cấp dung lượng cần thiết để truyền tín hiệu dữ liệu thích hợp giữa hai điểm truy cập tạo giao diện với mạng [2].

Ngoài điện thoại thông thường, các dịch vụ thuê bao sau được hỗ trợ bởi GSM:

- Dual-tone multifrequency (DTMF): âm kép đa tần là âm thanh do điện thoại tạo ra khi nhấn các phím số. Các âm này được truyền cùng với kênh thoại. DTMF được sử dụng để điều khiển thiết bị tự động và báo hiệu ý định của người dùng, chẳng hạn như số họ muốn quay. Mỗi phím có hai âm ở tần số cụ

thể, một âm được tạo từ một nhóm âm tần số cao, trong khi âm còn lại thuộc nhóm tần số thấp.

- Facsimile group III: Ngoài chuẩn group 1 và 2, thì group 3 được sử dụng phổ biến nhất vì các máy fax tiêu chuẩn được thiết kế để kết nối với điện thoại bằng tín hiệu tương tự, nên một bộ chuyển đổi fax đặc biệt kết nối với tổng đài được sử dụng trong hệ thống GSM. Điều này cho phép fax được kết nối GSM giao tiếp với bất kỳ fax nào trong mạng.
- Short message service: Một tin nhắn bao gồm tối đa 160 ký tự chữ và số có thể được gửi đến từ một trạm di động. Nếu thiết bị di động của thuê bao bị tắt nguồn hoặc đã rời khỏi vùng phủ sóng, tin nhắn sẽ được lưu trữ và cung cấp lại cho thuê bao khi thiết bị di động được bật nguồn hoặc đã vào lại vùng phủ sóng của mạng, đảm bảo rằng tin nhắn sẽ được nhận.
- Cell broadcast (quảng bá di động): Một biến thể của dịch vụ tin nhắn ngắn. Một tin nhắn dài tối đa 93 ký tự có thể được quảng bá đến tất cả các thuê bao di động trong một khu vực địa lý nhất định. Các ứng dụng điển hình bao gồm cảnh báo tắc nghẽn giao thông và báo cáo về tai nạn.
- Voice mail: Dịch vụ này thực sự là một máy trả lời tự động trong mạng do thuê bao kiểm soát. Các cuộc gọi có thể được chuyển tiếp đến hộp thư thoại của thuê bao và thuê bao kiểm tra tin nhắn thông qua mã bảo mật cá nhân.
- Fax mail: Với dịch vụ này, thuê bao có thể nhận tin nhắn fax tại bất kỳ máy fax nào. Các tin nhắn được lưu trữ trong một trung tâm dịch vụ mà từ đó thuê bao có thể truy xuất chúng thông qua mã bảo mật cá nhân đến số fax mong muốn [2].

GSM hỗ trợ một tập hợp toàn diện các dịch vụ bổ sung có thể bổ sung và hỗ trợ cả dịch vụ điện thoại và dữ liệu. Sau đây là danh sách một phần các dịch vụ bổ sung:

- Call forward: Dịch vụ này cung cấp cho thuê bao khả năng chuyển tiếp các cuộc gọi đến tới một số khác nếu thiết bị di động được gọi không liên lạc được hoặc máy bận không trả lời.
- Barring of outgoing calls: Dịch vụ này giúp thuê bao di động có thể chặn tất cả các cuộc gọi đi.
- Barring of incoming calls: Chức năng này cho phép thuê bao chặn cuộc gọi đến.
- Advice of Charge (AoC): Dịch vụ AoC cung cấp cho thuê bao di động ước tính cước phí các dịch vụ mà thuê bao đang sử dụng.
- Call hold: Dịch vụ này cho phép thuê bao tạm thời ngắt cuộc gọi đang diễn ra và sau đó tiếp tục lại cuộc gọi.
- Call waiting: Dịch vụ này cho phép thuê bao di động được thông báo về cuộc gọi đến trong khi đang diễn ra một cuộc gọi khác. Thuê bao có thể trả lời, từ chối hoặc bỏ qua cuộc gọi đến.
- Multiparty service: Cho phép thuê bao di động thiết lập cuộc gọi nhiều bên, nghĩa là đồng thời giữa ba và sáu thuê bao [2].

# CHƯƠNG 3: EXTENDED COVERAGE GSM

## 3.1 GIỚI THIỆU

EC-GSM-IoT là sự phát triển của EGPRS, giảm độ phức tạp của trạm di động (Mobile Station) đồng thời tiết kiệm năng lượng cộng với phạm vi phủ sóng mở rộng so với GPRS/EGPRS. EC-GSM-IoT cũng yêu cầu cả mạng và trạm di động sử dụng framework được cải thiện về bảo mật [4].

EC-GSM-IoT sử dụng BSIC (The base station identity code - Mã nhận dạng trạm gốc, là một mã được sử dụng trong GSM để nhận dạng duy nhất một trạm gốc. Mã này là cần thiết vì có thể các trạm di động nhận kênh quảng bá của nhiều hơn một trạm gốc trên cùng một tần số. Điều này là do việc sử dụng lại tần số trong mạng di động) 9bit trong đó BSIC 6bit được bổ sung 3bit mã màu tần số vô tuyến với mục đích giúp phân biệt giữa các ô trong mạng tái sử dụng tần số [4].

Không hỗ trợ truyền gói tin uplink downlink đồng thời. Uplink là để chỉ đường lên tín hiệu từ thiết bị đầu cuối di động tới trạm gốc BTS. Còn Downlink là đường xuống tín hiệu từ BTS tới thiết bị đầu cuối [4].

Trạm di động EC-GSM-IoT không cần tuân thủ các yêu cầu của GPRS, nhưng phải tuân thủ các yêu cầu của EGPRS trừ khi có quy định khác [4].

Trạm di động EC-GSM-IoT chỉ cần hỗ trợ hoạt động của Extended Coverage. Trạm di động cũng có thể tùy chọn hỗ trợ các dịch vụ PS (Packet Switching) khác, chẳng hạn như GPRS, EGPRS và/hoặc EGPRS2 hoặc các dịch vụ liên quan đến CS (Circuit-Switched) [4].

EC-GSM-IoT MS có thể hoạt động trong vùng phủ sóng mở rộng ở cả đường lên và đường xuống, điều này cải thiện độ nhạy và hiệu suất nhiễu của MS và BTS [4].

Một số các blind physical layer transmissions (lớp truyền vật lý ẩn) của kênh logic được được sử dụng để hỗ trợ khả năng phủ sóng mở rộng. Số lượng blind physical layer transmissions có thể khác nhau tùy thuộc vào phần mở rộng vùng phủ sóng được yêu cầu. Bốn loại phủ sóng khác nhau được xác định là CC1, CC1, CC3, CC4. Các kênh logic hỗ trợ hoạt động trong vùng phủ sóng mở rộng được gọi là các kênh EC. Bảng 3.1 liệt kê mức độ bao phủ mở rộng so với GPRS/EGPRS [5].

**Bảng 3.1:** Mức độ bao phủ mở rộng so với GPRS/EGPRS

| **Lớp mở rộng** | **Mức độ bao phủ mở rộng so với GPRS / EGPRS [dB]** |
|---|---|
| CC1 | 0-6 |
| CC2 | 6-12 |
| CC3 | 12-15 |
| CC4 | 15-20 |
| **Chú ý:** Các giá trị áp dụng cho cùng một công suất đầu ra tối đa (33dBm) của EC-GSM-IoT MS và GPRS / EGPRS MS. | |

Blind physical layer transmissions trên các kênh EC-PDTCH và EC-PACCH được ánh xạ tới 2 tài nguyên PDCH liên tiếp hoặc 4 tài nguyên PDCH liên tiếp theo thông tin quảng bá trong EC SI. Việc sử dụng 2 tài nguyên PDCH được dự trù cho các tình huống hạn chế về tài nguyên [5].

Kênh truy nhập điều khiển gói (PRACH: Packet Random Access Channel) MS sử dụng kênh này để khởi xướng truyền số liệu hoặc báo hiệu gói [5].

Kênh tìm gọi gói (PPCH: Packet Paging Channel) chỉ sử dụng ở đường xuống. Mạng sử dụng kênh này để tìm gọi MS trước khi tải gói xuống [5].

Kênh cấp phép truy nhập gói (PAGCH: Packet Access Grant Channel) chỉ sử dụng ở đường xuống. Mạng sử dụng kênh này để chỉ định tài nguyên cho MS trước khi truyền gói [5].

Kênh thông báo gói (PNCH: Packet Notification Channel): kênh này được sử dụng để thông báo truyền hoàn tất hoặc thất bại [5].

PCCH có thể được đặt vào các tài nguyên vô tuyến khác nhau (các khe thời gian khác nhau) của kênh CCCH. Tuy nhiên việc sử dụng kênh PCCH là tùy chọn. Nếu kênh này không được sử dụng thì các chức năng liên quan đến GPRS được thực hiện ở kênh CCCH [5].

GSM hỗ trợ một số kênh điều khiển riêng DCCH (Dedicated Control Channel) trong đó có các kênh điều khiển liên kết nhanh PACCH (package associated control) và kênh điều khiển định thời PTCCH (package Timing Control Channel). PTCCH được sử dụng để định thời trước cho các MS. PACCH là một kênh 2 chiều dùng để chuyển giao tiếp các thông tin khác giữa MS và mạng trong khi truyền các gói. Kênh này được liên kết với một kênh lưu lượng số liệu PDTCH (packet data traffic channel). PACCH không được ấn định tài nguyên cố định. Khi cần gửi thông tin ở kênh PACCH, một phần số liệu gói của người sử dụng sẽ dừng truyền [5].

Các kênh lưu lượng số liệu gói (PDTCH: Packet Data Traffic Channel). PDTCH là kênh được sử dụng để truyền số liệu thực sự của người sử dụng trên giao diện vô tuyến [5].

## 3.2 LỢI ÍCH

EC-GSM là công nghệ phổ biến thứ 2 thế giới, vào năm 2017 công nghệ này gần như đã bao phủ 90% dân số thế giới. Công nghệ EC GSM đã mang đến cho con người rất nhiều lợi ích thiết thực trong đó:

- Tăng cường phạm vi phủ sóng.
- Giảm tiêu thụ năng lượng.
- Có cấu trúc tái sử dụng các cơ sở hạ tầng hiện có.

- Ứng dụng mạnh mẽ cho lĩnh vực IoT.
- Tăng cường bảo mật [4].

### 3.2.1 Tăng cường phạm vi phủ sóng

Với yêu cầu được đặt ra là các thiết bị nằm trong những môi trường khắc nghiệt hoặc bị ảnh hưởng bởi nhiều yếu tố ngoại vi phải được kết nối ổn định, để thực hiện được yêu cầu khó khăn này thì chúng ta sử dụng mô hình phủ sóng của EC GSM [5].

Với kết cấu gồm nhiều lớp tăng cường đặt chồng lên nhau, lớp tăng cường đầu tiên CC1 hỗ trợ tốc độ truyền dữ liệu từ 8.8KBit đến 59,2KBbit. Các lớp phủ sóng thứ 2 3 4 sẽ được đặt chồng lên nhằm tăng phạm vi phủ sóng, không chỉ về khoảng cách theo phương ngang cả những môi trường trên cao hoặc sâu dưới lòng đất vẫn có thể hoạt động tốt [5].

EC-GSM-IoT MS có thể hoạt động trong vùng phủ sóng mở rộng ở cả đường lên và đường xuống, điều này được định nghĩa là độ nhạy và hiệu suất nhiễu của MS và BTS được cải thiện. Tính năng này đã được thiết kế để cải thiện vùng phủ sóng thêm 20 dB và mức nhiễu cũng tăng 20 dB so với GPRS/EGPRS [5].

Một số lượng truyền lớp vật lý ẩn cụ thể của kênh logic được xác định trước được sử dụng để hỗ trợ một mức độ phủ sóng mở rộng nhất định. Đối với một số kênh logic, số lần truyền lớp vật lý mù có thể khác nhau tùy thuộc vào phần mở rộng vùng phủ sóng được yêu cầu. Bốn loại phủ sóng khác nhau được xác định, mỗi loại xấp xỉ với mức độ phủ sóng mở rộng so với GPRS/EGPRS, được ký hiệu lần lượt là CC1, CC2, CC3 và CC4 [5].

Trong trường hợp mở rộng phạm vi phủ sóng đáng kể, một số lần truyền lớp vật lý ẩn cố định được xác định trước sẽ được áp dụng cho mỗi kênh logic. Số lần truyền thông qua lớp vật lý ẩn này, được sử dụng bởi CC2, CC3 và CC4, có thể khác nhau giữa các kênh logic cho cùng một Lớp phủ sóng. Các lớp phủ sóng khác nhau có thể được sử dụng trên đường lên và đường xuống. Các kênh logic hỗ trợ hoạt động trong vùng phủ sóng mở rộng được gọi là các kênh EC. Ngoài ra, kênh FCCH có thể hoạt

động trong phạm vi phủ sóng mở rộng mà EC-GSM-IoT hướng tới và do đó được sử dụng cho mục đích đồng bộ hóa [5].

### 3.2.2 Giảm tiêu thụ năng lượng

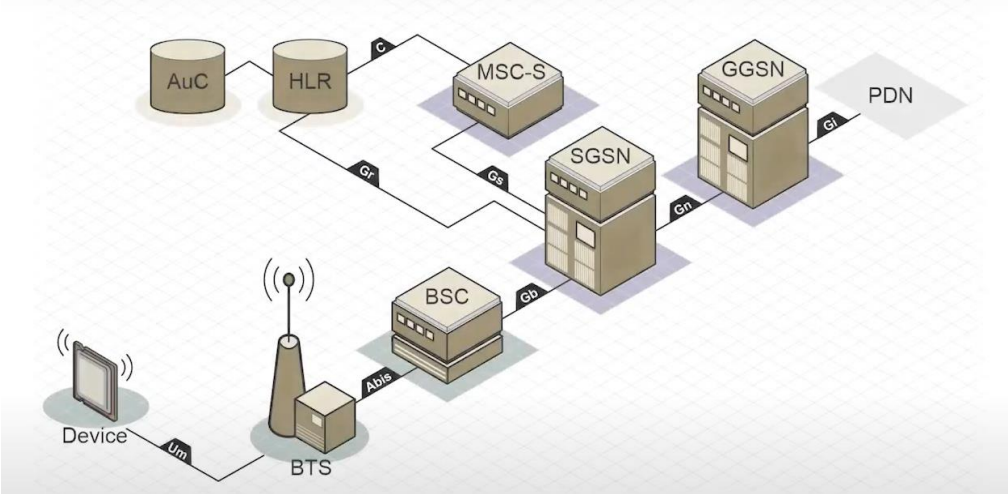
Ngày nay, các thiết bị cũng như cảm biến không được kết nối tới nguồn cấp chính và chúng hoạt động thông qua pin. Chúng ta cần tiếp cận những phương pháp mới để giảm mức tiêu thụ của pin và tránh việc thêm những cục pin lớn hơn để sử dụng [5].

Đối với EC-GSM trong IoT, chúng ta sẽ có những cách tiếp cận như sau:

- Tùy chỉnh linh hoạt: giảm yêu cầu thực hiện các phép đo định kỳ, đọc thông báo thông tin hệ thống và thực hiện các quy trình di động khi ở chế độ truyền gói.
- Cho phép thiết bị vào chế độ tiết kiệm năng lượng: thiết bị có thể đi ngủ trong 1 khoảng chu kì thời gian (có thể lên đến 413 ngày), tuy nhiên nó vẫn giữ kết nối đến mạng. Vì vậy nên khi thiết bị kết nối lại và thoát khỏi chế độ ngủ, nó có thể bắt đầu truyền nhận dữ liệu.
- Sử dụng 1 tiến trình gọi là extended DRX (tiếp nhận ko liên tục): cho phép thiết bị đi ngủ trong 1 khoảng chu kì thời gian (cao nhất là 52 phút) và tiết kiệm pin. Phương pháp này cũng có 1 ưu điểm giống như phương pháp trên là khi thiết bị được đánh thức, nó ko cần kết nối lại với mạng [5].

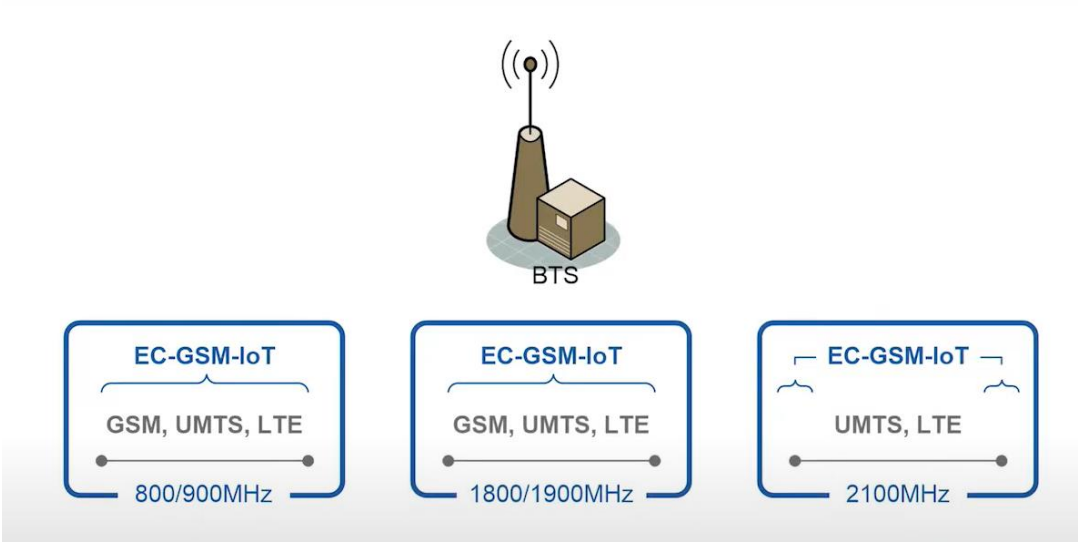
### 3.2.3 Có cấu trúc tái sử dụng các cơ sở hạ tầng hiện có

Hầu hết các nhà cung cấp đang hỗ trợ EC-GSM IoT chỉ nâng cấp phần mềm tại trạm cơ sở (Base Station) và thành phần điều khiển trạm cơ sở (Base Station Controller). Hình 3.1 mô tả cơ sở hạ tầng trong mạng [4].




**Hình 3.1:** Cơ sở hạ tầng trong mạng

Nhắc đến phương pháp tái sử dụng cơ sở hạ tầng đang tồn tại, cần nhắc đến phổ tần số vô tuyến - một thứ rất có giá trị đối với các nhà cung cấp dịch vụ. Điều đó dẫn đến việc chúng cần được sử dụng một cách thật hiệu quả. Hình 3.2 mô tả dải tần số hoạt động của EC-GSM [4].



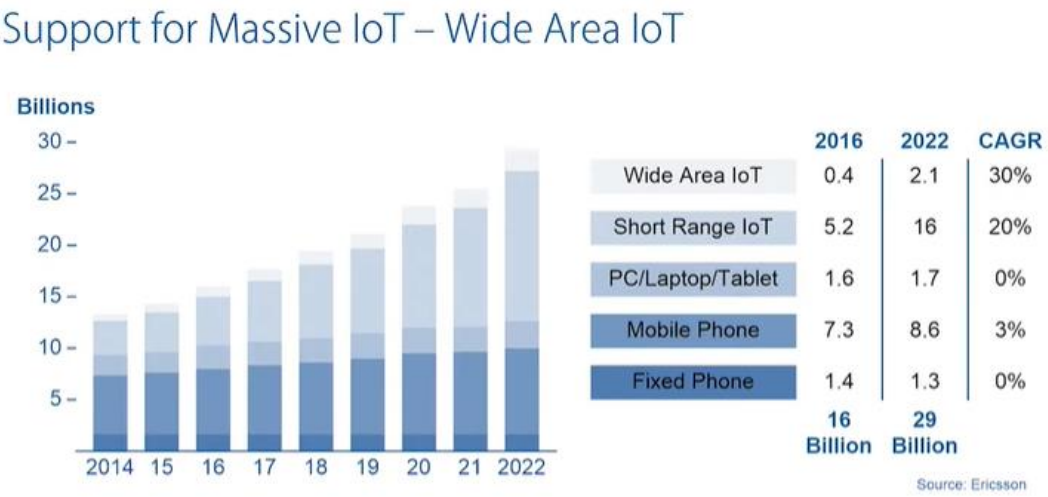

**Hình 3.2:** Dải tần số hoạt động của EC-GSM

EC-GSM có thể hoạt động trong băng tần đang tồn tại của GSM và GPRS (800, 900, 1800, 1900 MHz), cũng có thể lên đến 2100 MHz khi nó được sử dụng bởi mạng UMTS và LTE. EC-GSM có thể cung cấp độ phủ sóng với chỉ 600 kHz của phổ tần sử dụng 3 tần số [4].

Ngoài ra, cần phải cân nhắc dữ liệu mà những cảm biến sẽ gửi đi, chúng rất nhỏ khi so với những chiếc smartphone – 1 thiết bị dễ dàng giám sát các thống số ví dụ như mực nước trong ứng dụng cảnh báo lũ lụt mà chỉ cần gửi 1 lượng nhỏ dữ liệu và dữ liệu này có thể được gửi với tần số hàng ngày hàng tuần. Thậm chí khi sử dụng tần số hẹp, nó vẫn có thể hỗ trợ hàng ngàn thiết bị và điều này phụ thuộc vào lượng dữ liệu mà thiết bị muốn gửi [4].

### 3.2.4 Ứng dụng mạnh mẽ cho lĩnh vực IoT

Ở thế kỉ hiện đại, tiềm năng để các kiến trúc IoT phát triển là rất lớn, với sự phát triển không ngừng của nền công nghiệp, hàng nghìn các thiết bị di động/công nghệ mà con người sử dụng được dự đoán sẽ là sự hỗ trợ đắc lực cho việc phát triển các kiến trúc IoT sau này. Hình 3.3 mô tả tốc độ tăng trưởng của các thiết bị IoT từ năm 2016 đến năm 2022 [4].




**Hình 3.3:** Biểu đồ tốc độ tăng trưởng của các thiết bị IoT 2016-2022

Với tệp thiết bị đầu tiên, ta có Fixed Phone (thiết bị liên lạc cố định), tỷ lệ tăng trưởng hàng năm giảm từ 1,4 tỷ còn 1,3 tỷ, việc sử dụng cáp đồng để kết nối liên lạc khiến điều này là khá hợp lý và không có gì bất ngờ vì đây là những thiết bị lạc hậu ở thập kỷ này [4].

Không còn xa lạ với thiết bị điện thoại di động, tỉ lệ tăng trưởng của loại thiết bị này tăng 3% (từ 7,3 tỷ lên 8,6 tỷ thiết bị), tỉ lệ dù không cao nhưng đây vẫn là con

số khá đáng kể, thể hiện được lượng tăng phổ biến của thiết bị điện thoại trên toàn cầu [4].

Pc/Laptop/Tablet tăng nhẹ và cực kì ít, chỉ 100 triệu thiết bị trong vòng 6 năm [4].

Short Range Iot có tốc độ tăng trưởng nằm ở mức 1/5. Các thiết bị sử dụng mô hình IoT này không dựa trên kiến trúc EC-GSM**,** ví dụ như các chuẩn giao tiếp cá nhân ở hình 3.4 [4].


**Hình 3.4:** Các chuẩn giao tiếp IoT phạm vi nhỏ phổ biến

Các thiết bị sử dụng chuẩn giao tiếp trên thường có phạm vi kết nối rất ngắn, thường chỉ tới 100m là tối đa. Các thiết bị sử dụng Short Ranged IoT thường không được cấp phép bởi FCC (Ủy ban truyền thông liên bang), điều này có nghĩa là thiết bị cũng sẽ thông qua các dải tần không được cấp phép (dải tần mở và miễn phí), đó là 900Mhz, 2,4ghz và 5.9ghz [4].

Wide Range Iot có tỷ lệ tăng trưởng lên đến 30%, thể hiện tiềm năng to lớn cho sự phát triển của Wide Range IoT trong tương lai, các thiết bị kết nối qua công nghệ này thường sử dụng kết nối di động hoặc mạng diện rộng công suất thấp. Phạm vi kết nối rất rộng, được tính theo đơn vị km. Hình 3.5 mô tả các chuẩn giao tiếp IoT phạm vi lớn phổ biến [4].


**Hình 3.5:** Các chuẩn giao tiếp IoT phạm vi lớn phổ biến

Ngoài ra, Wide Range Iot còn xuất hiện trong dự án 3GPP (3GPP còn là thành quả đầu tiên và là dấu mốc quan trọng), đây là dự án hợp tác nhằm phát triển kỹ thuật hướng tới sự chấp nhận trên toàn cầu cho thế hệ thứ ba (3G) trong hệ thống di động. 3GPP đã nghiên cứu, phát triển 3 tiêu chuẩn MIoT gồm: LTE-M (LTE for Machines)

hay còn gọi là LTE Cat-M1; NB-IoT (NarrowBand IoT) và EC-GSM-IoT (Extended Coverage-GSM-IoT). Các tiêu chuẩn này đã được công bố vào tháng 6 năm 2016 tại Release 13 của 3GPP. Không những chỉ có 3GPP phát triển công nghệ này mà còn có sự tham gia của các hệ thống độc quyền như Sigfox và LORA [6].

### 3.2.5 Tăng cường bảo mật

Công nghệ GSM/GPRS đã được phát minh vào cuối những năm 1980, trong khoảng thời đó thì vấn đề bảo mật cũng như các mối đe dọa tới vấn đề bảo mật cũng đã thay đổi rất nhiều. Do đó, công nghệ này cần được cải tiến để nó có thể hoạt động tốt trong thời điểm hiện tại [4].

Đã có nhiều ví dụ về các thiết bị IoT với khả năng bảo mật cực kì kém đã bị tấn công [4].

Công nghệ EC-GSM hỗ trợ mã hóa và bảo vệ một cách toàn vẹn. Công nghệ bảo mật được dựa trên UMTS Authentication and Key Agreement [4].

Bản chất của AKA là việc xác thực người dùng với mạng và ngược lại. AKA là một cơ chế trong đó thiết bị di động và nhà khai thác mạng di động Xác thực và Phân phối các key. Trong quy trình AKA, các thông báo có tham số được xác nhận bởi User Equipment/Thiết bị người dùng (UE), được gửi từ AuC. Các tham số như vậy được kết hợp với nhau trong một Authentication Vector/Vectơ xác thực (AV). AV được phân phối tới Mạng lõi, mạng này phân phối các phần của AV này thông qua mạng truy cập tới UE. Sau đó, UE phải thực hiện một số tính toán để phù hợp với thử thách này. Kết quả của UE được gửi trở lại và được kiểm tra đối với AV nơi nó bắt nguồn. Nếu kết quả trùng khớp thì xác thực thành công. Nếu kết quả không thành công, một số quy trình khác sẽ được kích hoạt để khắc phục sự cố [4].

## 3.3 SO SÁNH EC-GSM VỚI MỘT SỐ CÔNG NGHỆ KHÁC

Để thể hiện kĩ hơn về cấu trúc IoT trong dự án 3GPP, tiến hành so sánh EC GSM với LTE - CAT M1 và NarrowBand – IoT [4].

LTE-M cho phép các thiết bị IoT chạy bằng pin kết nối trực tiếp tới mạng 4G mà không cần cổng kết nối. Về phía nhà mạng 4G, họ không cần thay đổi ăng ten thu phát mà chủ yếu là nâng cấp phần mềm để hỗ trợ LTE-M [4].

NB-IoT tập trung vào việc phủ sóng nội bộ, hạ giá thành thiết bị, tăng tuổi thọ pin và cho phép một lượng lớn các thiết bị có thể kết nối tới mạng. NB-IoT có thể triển khai băng tần nội dành cho LTE bằng cách sử dụng một sóng mang LTE thông thường hoặc sử dụng phổ tần ở băng bảo vệ của LTE hoặc triển khai trên băng tần độc lập. Băng tần GSM refarming là một trong những băng tần rất phù hợp cho triển khai NB-IoT [4].

EC-GSM-IoT là phiên bản nâng cấp mạng GSM để hỗ trợ IoT, chính vì vậy nó có thể triển khai trên nền mạng GSM hiện có của các nhà mạng. Tuy nhiên công nghệ này hiện chưa nhận được nhiều sự quan tâm và để ý của các hãng công nghệ và các nhà mạng như LTE-M và NB-IoT [4].

Bảng 3.2 so sánh EC-GSM với các chuẩn giao tiếp khác.

**Bảng 3.2:** So sánh EC-GSM với các chuẩn giao tiếp khác

| | **LTE Cat M1 (LTE-M)** | **LTE Cat NB1 (NB-IoT)** | **EC-GSM-IoT** |
|---|---|---|---|
| **3GPP Release** | Release 13 | Release 13 | Release 13 |
| **Downlink Peak Rate** | 1 Mbit/s | 250 kbit/s | 474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B) |

| | | | |
|---|---|---|---|
| **Uplink Peak Rate** | 1 Mbit/s | 250 kbit/s (multi-tone) 20 kbit/s (single-tone) | 474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B) |
| **Latency** | 10ms-15ms | 1.6s-10s | 700ms-2s |
| **Number of Antennas** | 1 | 1 | 1-2 |
| **Duplex Mode** | Full or Half Duplex | Half Duplex | Half Duplex |
| **Device Receive Bandwidth** | 1.08 MHz | 180 kHz | 200 kHz |
| **Receiver Chains** | 1 (SISO) | 1 (SISO) | 1-2 |
| **Device Transmit Power** | 20 / 23 dBm | 20 / 23 dBm | 23 / 33 dBm |

# TÀI LIỆU THAM KHẢO

[1] Phạm Công Hùng, Nguyễn Hoàng Hải, Tạ Vũ Hằng, Vũ Thị Minh Tú, Đỗ Trọng Tuấn, Vũ Đức Thọ, Nguyễn Văn Đức, "Giáo trình Thông tin di động", 2007.

[2] The International Engineering Consortium, "Global System for Mobile Communication (GSM)", 2.11.2022, https://www.uky.edu/~jclark/mas355/GSM.PDF

[3] Tutorials Point, "GSM Tutorial", 17.1.2018, https://www.tutorialspoint.com/gsm/gsm_specification.htm

[4] Mpirical, "EC-GSM IoT - Extended Coverage GSM - Cellular IoT Air Interface Course", 2.11.2022, https://www.youtube.com/watch?v=ooS3HdLK1F8

[5] 3GPP, "Digital cellular telecommunications system (Phase 2+) (GSM) 3GPP TS 43.064 version 14.3.0 Release 14".

[6] Phạm Vĩnh Hòa, "Các Nguyên Tắc Sử Dụng Mạng Vô Tuyến Trong Mạng GSM/GPRS", 2.2.2018.