Chương 3: Mạng không dây tế bào (Các hệ thống điện thoại di động)

Các hệ thống điện thoại di động

* 3.1 Các hệ thống điện thoại di động thế hệ thứ nhất
  * 3.1.1 Hệ thống điện thoại di động kỹ thuật tương tự
  * 3.1.2 Advanced Mobile Phone System (AMPS)
* 3.2 Các hệ thống điện thoại di động thế hệ thứ hai
  * 3.2.1 Giới thiệu
  * 3.2.2 Global System for Mobile Communication (GSM)

Các hệ thống điện thoại di động thế hệ thứ nhất

* Hệ thống điện thoại di động kỹ thuật tương tự
  * Hệ thống điện thoại di động đầu tiên Mobile Telephone System (MTS)
    * Sự đột phát về công nghệ thời bấy giờ
    * Có rất nhiều giới hạn: máy thu phát rất lớn, sử dụng phổ không hiệu quả, chuyển mạch cuộc gọi thủ công
  * Thời kỳ của điện thoại di động bắt đầu từ điện thoại di động thế hệ thứ nhất (1G)
    * Áp dụng khái niệm tế bào
    * Phát triển quá sự tưởng tượng của người tìm ra hệ thống

Hệ thống điện thoại di động kỹ thuật tương tự

* Vẫn được sử dụng ở một số nơi như Bắc Mỹ
* Các hệ thống thế hệ một khá thô sơ do sử dụng tín hiệu tương tự
  * Không có mật mã hoá
  * Chất lượng cuộc gọi kém
  * Sử dụng phổ không hiệu quả: một sóng mang RF tận hiến cho một người sử dụng

Hệ thống điện thoại kỹ thuật tương tự

* US
  * Advanced Mobile Phone System (AMPS)
    * Không có truyền dữ liệu
    * Các kênh cách nhau 30KHz
    * Kênh tiếng nói dùng Frequency Modulation (FM)
    * Kênh điều khiển dùng Binary Frequency Shift Keying (BFSK), 10 kbps
    * Lược đồ sử dụng tần số: cụm 12 nhóm hoặc cụm 7 nhóm
    * Hai nhà cung cấp dịch vụ có thể cùng hoạt động: mỗi bên dùng 25 MHz phổ

Hệ thống điện thoại di động kỹ thuật tương tự

* Châu Âu
  * Rất nhiều hệ thống được triển khai
    * Total Access Communication System (TACS): Anh, Ý, Tây ban nha, Áo
    * Nordic Mobile Telephone (NMT)
    * C-450: Đức, Bồ đào nha
    * Radiocom 2000: Pháp
    * Radio Telephone Mobile System (RTMS): Ý
  * Tất cả đều sử dụng FM kênh thoại và Frequency Shift Keying (FSK) cho kênh điều khiển
  * Quyết định chuyển giao dựa trên mức độ điện năng của thiết bị di động nhận được tại BS, trừ C-450 dựa trên thời gian trễ RTT

Hệ thống điện thoại kỹ thuật tương tự

* Nhật
  * Nippon Telephone and Telegraph (NTT)
  * IDO: sử dụng một biến thể của TACS tại châu Âu, NTACS
  * DDI Cellular Group: biến thể của TACS, JTACS/NTACS

Advanced Mobile Phone System (AMPS)

* Các kênh của AMPS
* AMPS là một đại diện tiêu biểu cho các hệ thống thế hệ thứ nhất
* Phát triển bởi Bell Labs
* Cấp phát tần số của AMPS: băng thông cấp phát nằm trong phần 800 MHz của phổ
* Các kênh của AMPS
  * Băng tần hoạt động của AMPS là $2 \times 25 = 50$ MHz, 824-849 MHz và 869-894 MHz
  * Hai nhà cung cấp dịch vụ có thể cùng hoạt động, sở hữu 25 MHz, gọi là băng tần A và B
  * Hai tập kênh A, B, gồm các kênh đánh số từ 1-333 và 334-666
  * Các kênh điều khiển: 313-333 và 334-354, 312 kênh thoại và 21 kênh điều khiển cho mỗi nhà cung cấp dịch vụ
  * 16 kênh thoại được điều khiển bởi 1 kênh điều khiển

Advanced Mobile Phone System (AMPS)

* Các kênh của AMPS
  * Các kênh thoại chính là Forward Voice Channel (FVC) (từ BS đến MS) và Reverse Voice Channel (RVC) (từ MS đến BS) được cấp cho MS khi thiết lập cuộc gọi
  * Mỗi MS khi đang ở trạng thái nhàn rỗi chốt vào một kênh điều khiển mạnh nhất để nhận thông tin trạng thái
    * Forward Control Channel (FOCC): luồng dữ liệu truyền liên tục từ BS đến MS, 10 kbps
    * Reverse Control Channel (RECC)
  * Supervisory Audio Tone (SAT) được gửi trên kênh thoại
  * Signaling Tone (ST) dùng cho các tín hiệu điều khiển

Advanced Mobile Phone System (AMPS)

* Các hoạt động của mạng
  * Có 3 định danh được sử dụng trong AMPS
    * Electronic Serial Number (ESN): 32 bit, xác định duy nhất một AMPS MS
      * Gồm 3 trường: 8 bit manufacturers code (MFR), 6 bit không sử dụng, 18 bit serial number của MS
    * System Identification Numbers (SIDs): 15 bit xác định duy nhất nhà khai thác dịch vụ
    * Mobile Identification Number (MIN): 34 bit, số điện thoại di động

AMPS

- Khởi hoạt
  - Sự kiện 1. MS nhận được các tham số hệ thống, cấu hình sử dụng một trong hai mạng AMPS
  - Sự kiện 2. MS quét 21 kênh điều khiển của mạng AMPS để nhận được các thông điệp điều khiển từ mạng. Kênh điều khiển với chất lượng tín hiệu đáp ứng được chọn
  - Sự kiện 3. MS nhận thông điệp từ kênh điều khiển về các tham số của hệ thống mạng
  - Sự kiện 4. Các thông tin nhận được ở bước 3 dùng được cập nhật. Nếu SID của mạng hiện không trùng với SID cấu hình, MS chuẩn bị thực hiện chuyển mạng (roaming)
  - Sự kiện 5. MS thông báo định danh cho mạng: gửi MIN, ESN, SIDS qua RECC

AMPS

* Khởi hoạt
  * Sự kiện 6. AMPS kiểm tra các tham số của MS để xácđịnh MS có phải là MS lang thang
  * Sự kiện 7. BS gửi một thông điệp điều khiển cho MS
  * Sự kiện 8. MS chuyển sang trạng thái nhàn rỗi chờ cuộc gọi

AMPS

- Thiết lập cuộc gọi từ một MS
  - Sự kiện 1. MS gửi cho BS một thông điệp gồm MIN, ESN của MS và số gọi đến
  - Sự kiện 2. BS chuyển thông tin cho mạng xử lý
  - Sự kiện 3. BS thông báo cho MS kênh dành cho cuộc gọi
  - Sự kiện 4. Cả MS và BS chuyển sang kênh thoại
  - Sự kiện 5. BS gửi một thông điệp điều khiển qua FVC dùng SAT
  - Sự kiện 6. MS trả lời qua FVC dùng SAT
  - Sự kiện 7. Cuộc gọi được thiết lập

AMPS

- Thiết lập cuộc gọi đến một MS
  - Sự kiện 1. Định danh của MS được chuyển đến BS
  - Sự kiện 2. Các thông tin điều khiển, như kênh số, được truyền tải đến MS
  - Sự kiện 3. MS trả lời lại, gửi MIN, ESN và các thông tin điều khiển liên quan khác
  - Sự kiện 4. Cả MS và BS chuyển sang kênh thoại
  - Sự kiện 5. BS gửi một thông điệp điều khiển qua kênh FVC sử dụng SAT
  - Sự kiện 6. MS trả lời bằng SAT qua FVC
  - Sự kiện 7. Cuộc gọi được thiết lập

AMPS

- Chuyển giao cuộc gọi
  - Sự kiện 1. BS phục vụ MS phát hiện sự suy giảm của điện năng truyền của MS
  - Sự kiện 2. BS gửi yêu cầu đo mức độ chuyển giao đến MSC
  - Sự kiện 3. MSC chỉ thị các BS lân cận đo cường độ tín hiệu của MS
  - Sự kiện 4. MSC chọn một BS tốt nhất để phục vụ MS
  - Sự kiện 5. MSC cấp phát một kênh thoại cho BS được chọn
  - Sự kiện 6. BS được chọn báo nhận sự cấp phát
  - Sự kiện 7. MSC gửi thông điệp chuyển giao cho BS hiện tại
  - Sự kiện 8. BS hiện tại gửi thông điệp chuyển giao cho MS. Thông điệp này thông báo cho MS kênh thoại sử dụng và mức điện năng cho BS mới

AMPS

* Chuyển giao cuộc gọi
  * Sự kiện 9. MS trả lời BS hiện tại và chuyển sang kênh thoại
  * Sự kiện 10. MS bắt đầu quét và nhận được SAT của BS mới
  * Sự kiện 11. MS khẳng định với BS mới qua FVC sử dụng SAT
  * Sự kiện 12. BS khẳng định chuyển giao với MSC

Các hệ thống điện thoại di động thế hệ thứ hai

- Giới thiệu
  - Kỷ nguyên của điện thoại di động bắt đầu từ khi các hệ thống 1G hoạt động
  - Các hệ thống 1G đang được thay thế toàn bộ bởi các hệ thống 2G
  - Các hệ thống 2G hoàn toàn số hoá
  - So với các hệ thống 1G, 2G có các ưu điểm sau:
    - Mật mã hoá
    - Sử dụng các kỹ thuật phát hiện và sửa lỗi bit
      - Chất lượng cuộc gọi tốt hơn
      - Tốc độ cao hơn cho các ứng dụng truyền dữ liệu
      - Sử dụng phổ hiệu quả hơn
      - Dữ liệu số có thể được nén
      - Phục vụ được nhiều người dùng hơn

Các hệ thống điện thoại di động thế hệ thứ hai

- Nhiều người dùng dùng chung sóng mang RF và chỉ sử dụng khi có lưu lượng (thoại hoặc dữ liệu) truyền
- Sự phát triển của các kỹ thuật mã hoá tiếng nói số có tốc độ thấp và sự phát triển của vi mạch
- Sử dụng thêm TDMA và CDMA

Global System for Mobile Communications (GSM)

- Lịch sử
- Các dịch vụ cung cấp bởi GSM
- Kiến trúc của mạng GSM
- Mã hoá tiếng nói
- Các đặc điểm của truyền sóng radio
- Cấu trúc của kỳ bùng phát
- Mã hoá kênh
- Các hoạt động của mạng
- Xác thực và bảo mật của GSM

Lịch sử

- Xuất phát điểm của GSM từ châu Âu
- Châu Âu có một thời kỳ phát triển mạnh mẽ của các hệ thống tương tự
  - NMT ở Scandinavia
  - TACS ở Anh, Ý, Tây ban nha,
  - C-450 ở Đức, Bồ đào nha
  - Radiocom 2000 ở Pháp
  - RTMS ở Ý
- Các hệ thống không tương thích với nhau. Nhược điểm:
  - Chiếc điện thoại di động chỉ giới hạn sử dụng trong một nước
  - Thị trường bị thu hẹp

Lịch sử

- Năm 1992, hệ thống GSM được đề xuất, lấy theo tên của nhóm nghiên cứu Groupe Special Mobile, có các tiêu chí:
  - Chất lượng tiếng nói tốt
  - Giá dịch vụ và thiết bị đầu cuối rẻ
  - Hỗ trợ chuyển mạng
  - Khả năng hỗ trợ thiết bị cầm tay (handheld terminal)
  - Hỗ trợ mở rộng các dịch vụ và tiện nghi mới
  - Sử dụng phổ hiệu quả
  - Tương thích ISDN
- Hiện tại GSM là hệ thống phát triển và phổ biến nhất: 110 nước trên toàn thế giới

Lịch sử

* Có 4 phiên bản của hệ thống GSM, phụ thuộc vào tần số hoạt động
  * GSM 900: sử dụng lại tần số 900 MHz của TACS
  * GSM 1800: Digital Communication Network (DCN) ở châu Âu
  * GSM 1900: Personal Communication System (PCS) ở Mỹ
  * GSM 450: nâng cấp từ hệ thống 1G NMT thành 2G

GMS variant	Uplink frequency (MHz)	Downlink frequency (MHz)
GSM 900	890 - 915	935 – 960
GSM 1800 (DCN)	1710 – 1785	1805 – 1880
GSM 1900 (PCS)	1850 – 1910	1930 – 1990
GSM 450	450.4 – 457.6 or 478 – 486	460.4 – 467.6 or 488.8 - 496

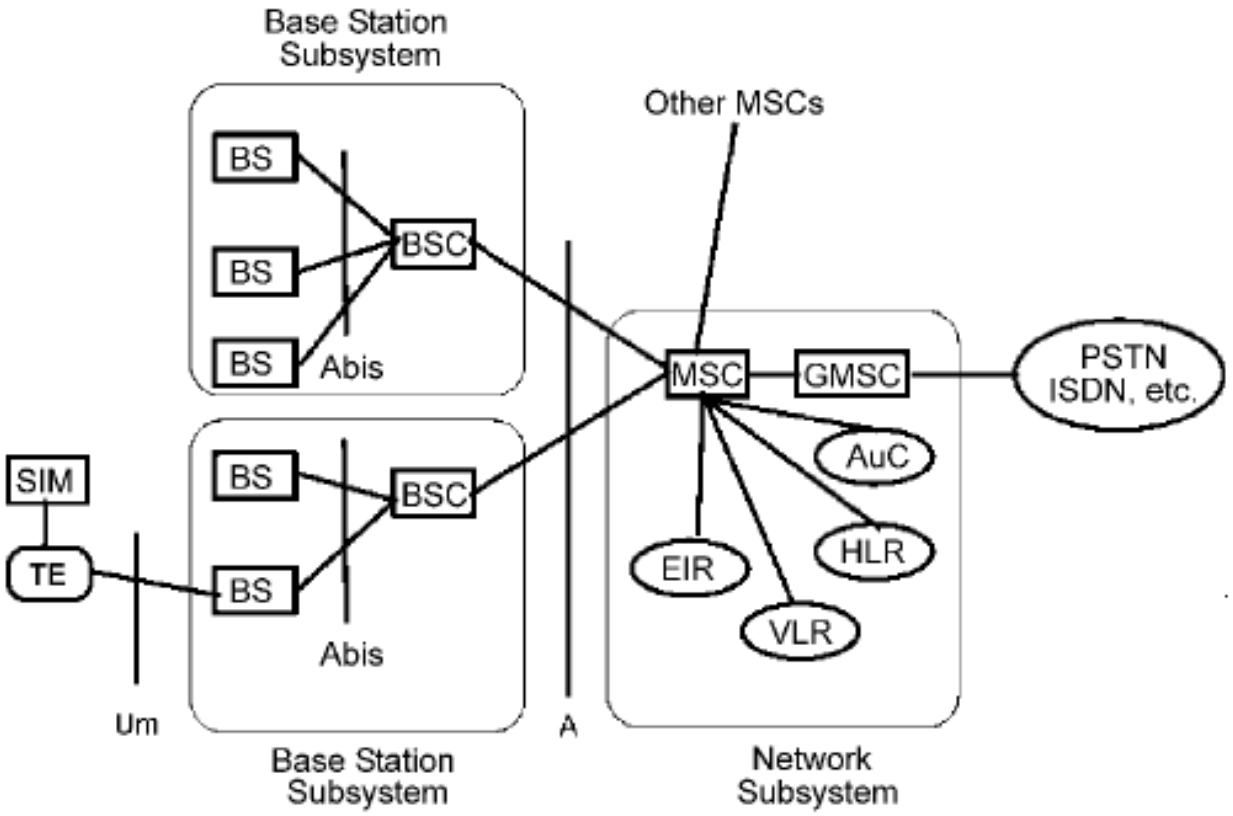
Các dịch vụ

- Dịch vụ chủ yếu là điện thoại. Tiếng nói được số hoá và truyền đi trong các luồng bit
- Dịch vụ truyền dữ liệu, tốc độ 9600 bps cho POTS (Plain Old Telephone Service), ISDN (Integrated Services Digital Network)
- Fax
- Short Message Service (SMS)
- Cell Broadcast Service (CBS)
- Caller identification
- Multiparty conversations
- Call forward, call waiting, call barring (chặn cuộc gọi)

Kiến trúc của mạng GSM

* Mạng GSM có thể chia thành 3 phần:
  * Mobile Station: thiết bị di động của người sử dụng
  * Base Station Subsystem: quản lý đường truyền sóng radio với MS qua giao diện Um
  * Network Subsystem
    * Thành phần chính là Mobile services Switching Center (MSC): thực hiện các chức năng chuyển cuộc gọi giữa các người dùng của mạng di động và với mạng điện thoại cố định
    * BSS và MSC giao tiếp qua giao diện A

Kiến trúc của mạng GSM



Mobile Station (MS)

* MS bao gồm
  * Terminal (TE)
  * Subscriber Identity Mobile (SIM)
    * Thẻ thông minh (Smart card)
    * Cho phép sự di động cá nhân
    * Chứa số điện thoại của người sử dụng
    * Chứa International Mobile Subscriber Identity (IMSI), khoá bí mật cho xác thực và một số thông tin khác

Mobile Station (MS)

* Thiết bị di động được xác định duy nhất bởi International Mobile Equipment Identity (IMEI)
* IMEI
  * 15 con số
  * Type Approval Code (TAC): qua bước kiểm thử chế tạo đúng
  * Final Assembly Code (FAC): nơi sản xuất hoặc lắp ráp cuối cùng

TAC (3 digits)	FAC (1 or 2 digits)	Serial number (up to 11 digits)	1 spare digit

Mobile Station (MS)

* IMSI
  * Xác định duy nhất thuê bao
  * Mobile Country Code (MCC): mã nước
  * Mobile Network Code (MNC): mã nhà khai thác dịch vụ
  * Mobile Subscriber Identification Code (MSIC): xác định duy nhất khách hàng của nhà khai thác

MCC (3 digits)	MNC (2 digits)	MSIC (up to 10 digits)

Base Station Subsystem (BSS)

* BSS bao gồm phần cứng và phần mềm để quản lý đường truyền radio với các MS
* Bao gồm Base Station (BS) và Base Station Controller (BSC)
* BS
  * Máy thu phát vô tuyến tạo ra một tế bào và chạy các giao thức liên kết radio với MS
  * Lưu lượng được gửi đến BSC
* BSC
  * Tập hợp các cuộc gọi từ BS và chuyển cho MSC
  * Xử lý việc thiết lập các kênh radio, chuyển giao, nhảy sóng
  * MSC định tuyến các mạch đến BSC, BSC có trách nhiệm kết nối và chuyển các cuộc gọi đến các BS
  * BSC có chức năng phân đoạn mạng nhằm quản trị lưu lượng

Network Subsystem (NS)

- Thành phần trung tâm của NS là Mobile Switching Center (MSC)
- MSC thực hiện các chức năng chuyển mạch cuộc gọi và các chức năng như:
  - Đăng ký
  - Xác thực
  - Cập nhật vị trí
  - Chuyển giao
  - Định tuyến cuộc gọi cho các thuê bao chuyển mạng
  - Giao tiếp với mạng cố định qua Gateway MSC (GMSC)
  - Sử dụng giao thức tín hiệu SS7

Network Subsystem (NS)

- Thông tin về các MS được lưu trong hai CSDL, Home Location Register (HLR) và Visitor Location Register (VLR)
- HLR và VLR cùng với MSC cung cấp khả năng định tuyến cuộc gọi và chuyển mạng trong GSM
- HLR lưu mọi thông tin về các thuê bao và vị trí hiện tại của MS hay VLR hiện tại của MS
- VLR lưu một số thông tin có lựa chọn về các MS hiện đang trong vùng quản lý của VLR
- VLR có thể được đặt cùng với MSC để giảm trao đổi tín hiệu

Network Subsystem (NS)

- Equipment Identity Register (EIR)
  - CSDL về các thiết bị di động định danh bằng IMEI
  - Đánh dấu IMEI là hợp lệ hay không hợp lệ để cung cấp dịch vụ
  - Các khả năng đánh dấu:
    - Danh sách trắng (White listed): được kết nối với mạng
    - Danh sách xám (Grey listed): cần được theo dõi
    - Danh sách đen (Black listed): bị cấm sử dụng mạng
- Authentication Center (AuC)
  - Lưu bản sao của khoá bí mật đã được lưu trong SIM của thuê bao
  - Xử lý các thủ tục xác thực với MS

Mã hoá tiếng nói

* Nhóm GSM nghiên cứu các thuật toán mã hoá tiếng nói dựa trên chất lượng thoại và độ phức tạp (giá và độ trễ xử lý, tiêu thụ năng lượng)
* Sử dụng Regular Pulse Excited-Linear Predictive Coder (RPE-LPC) có tốc độ 13 kbps
* Có codec với tốc độ giảm một nửa. Tuy nhiên chất lượng cuộc gọi giảm đi không nhiều

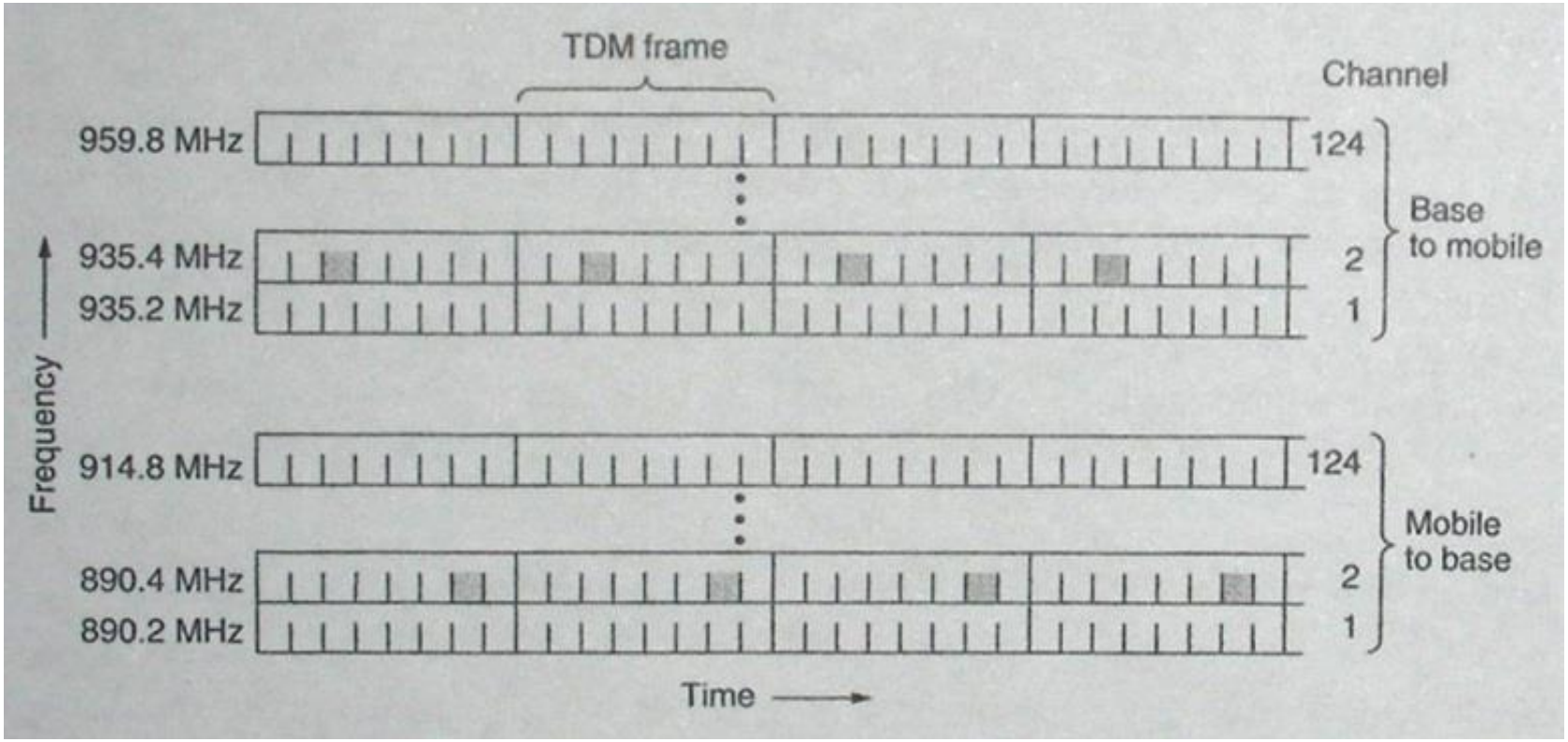
Các đặc điểm của truyền sóng radio

* GSM được cấp phát phổ trong khoảng 890-915 cho các kênh chiều đi lên (từ MS đến BS) và 935-960 cho các kênh chiều đi xuống (từ BS đến MS)
* Các tần số sử dụng cách nhau 200 KHz

Đa truy nhập và cấu trúc của kênh

- Băng thông được chia sẻ cho mọi người dùng sử dụng tổ hợp của FDMA và TDMA
  - Băng thông 25 MHz được chia thành 124 tần số cách nhau 200 KHz
  - Một tần số hoặc nhiều hơn được cấp cho một BS
  - Mỗi tần số hỗ trợ 8 kết nối sử dụng TDMA
    - Đơn vị thời gian trong kiểu TDMA được gọi là kỳ bùng phát hay một khe thời gian, diễn ra trong khoảng thời gian 15/26 ms (xấp xỉ 0.577 ms)
    - 8 kỳ bùng nổ tạo thành một khuông TDMA hay một kênh logic
    - Một kỳ bùng nổ hay một khe thời gian là một kênh vật lý
    - 8 khe đậm màu (hình sau) thuộc vào cùng một kết nối

Đa truy nhập và cấu trúc của kênh



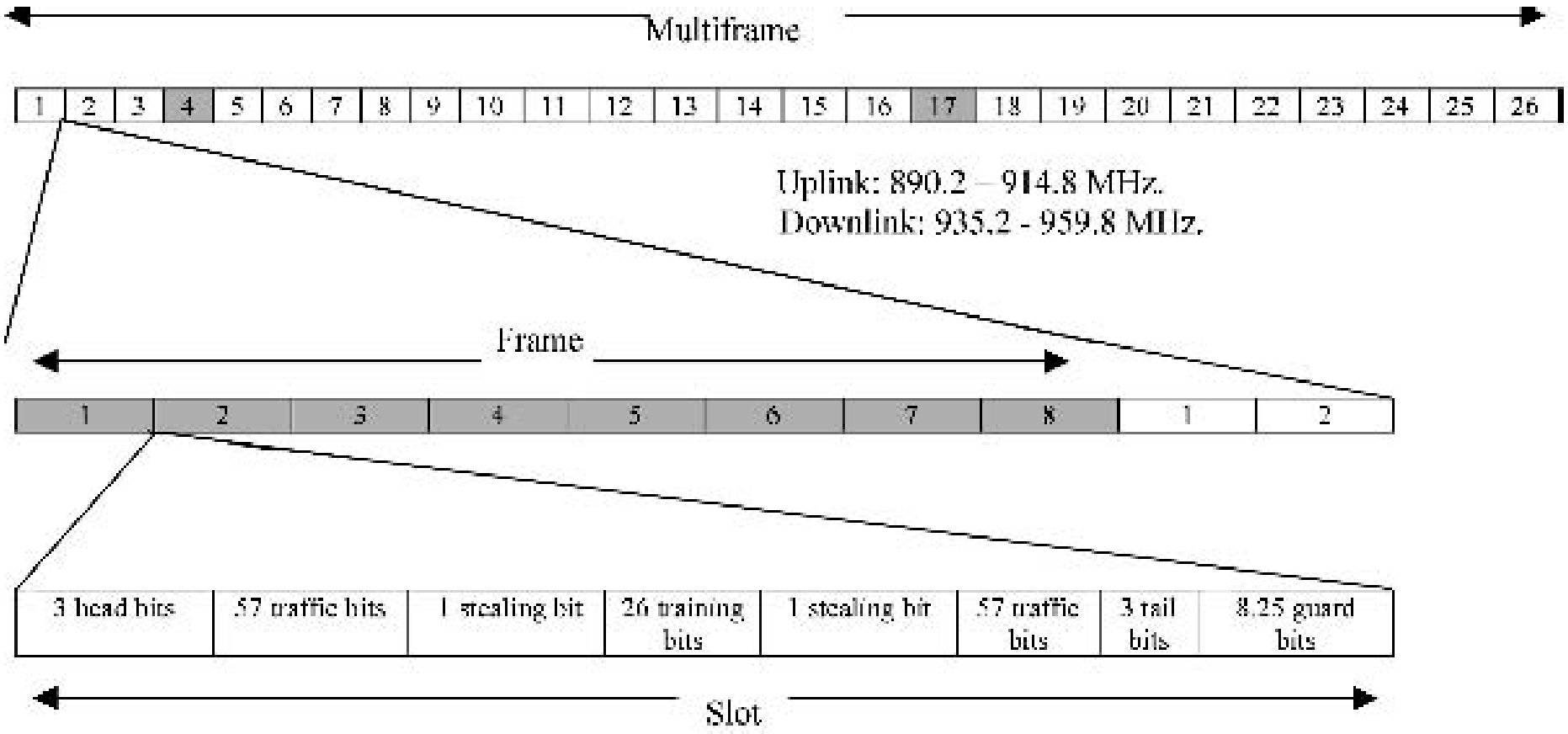
Đa truy nhập và cấu trúc của kênh

* Các kênh có thể được chia thành
  * Kênh tận hưởng/độc quyền/dành riêng (dedicated channels): cấp phát cho một MS
  * Kênh chung (common channels): các MS dùng chung trong chế độ nhàn rỗi

Kênh lưu lượng (Traffic Channels - TCH)

- Được dùng để mang lưu lượng tiếng nói và dữ liệu
- Sử dụng cấu trúc đa khuông 26 khuông
- Một đa khuông diễn ra trong 120 ms
- Trong 26 khuông
  - 24 khuông được dùng cho lưu lượng
  - 1 khuông dùng cho kênh Slow Associated Control Channel (SACCH)
  - 1 khuông không sử dụng
  - 2 khuông trên được gọi là các khuông bị lấy mất
- TCH cho kênh chiều lên và chiều xuống cách nhau 3 kỳ bùng phát hay 3 khe thời gian

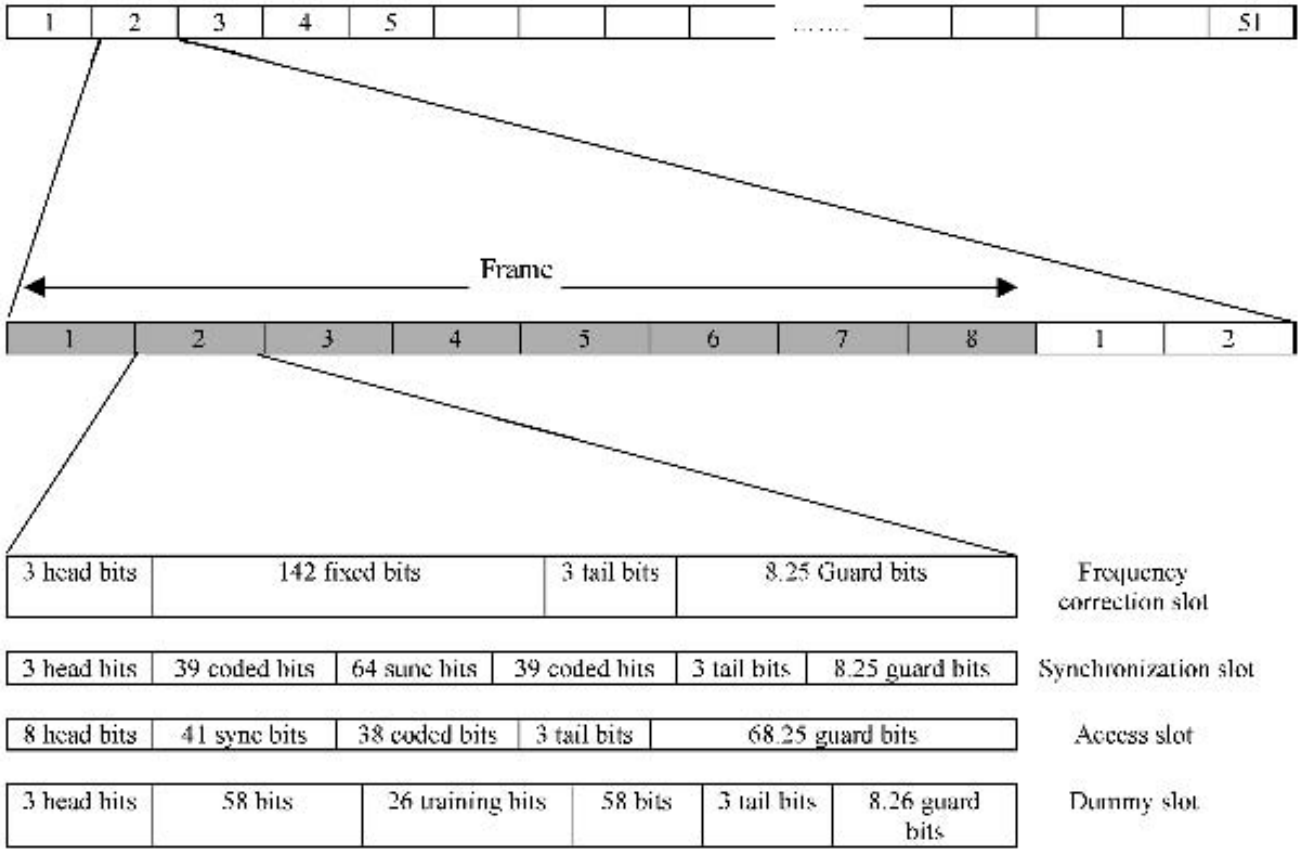
TCH


Multiframe
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Uplink: 890.2 – 914.8 MHz.
Downlink: 935.2 - 959.8 MHz.
Frame
1 2 3 4 5 6 7 8 1 2
3 head bits
57 traffic bits
1 stealing bit
26 training bits
1 stealing bit
57 traffic bits
3 tail bits
8.25 guard bits
Slot

Kênh chung (Common channels) hay kênh điều khiển (Control channels)

* MS truy nhập kênh chung cả khi trong chế độ nhàn rỗi và tận hưởng
  * Trong chế độ nhàn rỗi: trao đổi thông tin tín hiệu để chuyển sang chế độ tận hưởng
  * Trong chế độ tận hưởng: kiểm tra các BS xung quanh về thông tin chuyển giao và các thông tin khác
* Sử dụng cấu trúc đa khuông 51 khuông

Kênh chung (Common Channels)



Kênh chung (Common Channels)

* Gồm các loại kênh
  * Broadcast Control Channel (BCCH): truyền quảng bá liên tục chiều xuống các thông tin về định danh của BS, tần số …
  * Frequency Correction Channel (FCCH) và Synchronization Channel (SCH): truyền quảng bá chiều xuống, đồng bộ MS với cấu trúc khe của cell qua xác định kỳ bùng nổ và đánh số khe
  * Random Access Channel (RACH): chiều lên, kênh Aloha phân khe dùng để yêu cầu kênh truy nhập
  * Paging Channel (PCH): quảng bá chiều xuống, thông báo cho MS về một cuộc gọi đến
  * Access Grant Channel (AGCH): dùng để cấp cho MS một SDCCH sau khi nhận được yêu cầu qua RACH
  * Slow Associated Control Channel (SACCH): chiều xuống và lên, giữa các kênh lưu lượng, dành cho báo tín hiệu tốc độ thấp, không khẩn cấp
  * Fast Associated Control Channel (FACCH): chiều xuống và lên, kênh báo tín hiệu tốc độ cao, sử dụng cho thiết lập cuộc goi, xác thực người dùng, các lệnh chuyển giao20

Kiến trúc của kỳ bùng phát

- Có 5 kiểu bùng phát trong GSM
- Bùng phát thường có chiều dài 156.25 bit, truyền trong 0.577 ms, cho tốc độ gộp 270.833 kbps, tốc độ cho 1 người dùng 33.9 kbps, tốc độ thực tế 9.6 kbps do FEC và mật mã hoá
- Các kiểu bùng phát
  - Bùng phát thường
  - F, Frequency control burst, dùng trên kênh FCCH
  - S, Synchronous control burst, dùng trên kênh SCH
  - Access control burst, dùng trên kênh RACH
  - Dummy burst

Bùng phát thường

- Truyền dữ liệu và tiếng nói
- Gồm các phần:
  - Phần lưu lượng: mang theo lưu lượng tiếng nói hoặc dữ liệu, thông tin báo tín hiệu cho xử lý cuộc gọi (thiết lập, duy trì, kết thúc cuộc gọi)
  - Phần học: dành cho MS và BS "học" kênh
  - Phần các bit bị lấy mất: dùng để chỉ ra thông tin mang theo là dữ liệu hay thông tin điều khiển, dùng khi chuyển giao, sử dụng FACCH, làm giảm chất lượng thoại để truyền tải thông tin điều khiển
  - Phần đầu và đuôi: tăng hoặc giảm dần mức điện năng
  - Phần gác: tránh lỡ khe thời gian do thời gian trễ lan truyền, hay do khoảng cách xa giữa MS và BS

Các bùng phát khác

- F hay Frequency control burst
  - Đồng bộ hoá MS với tần số của hệ thống
- S hay Synchronous control burst
  - Đồng bộ hoá về thời gian giữa MS và BS
  - Chứa thông tin về vị trí và định danh của các khe trong khuông TDMA
  - Chứa các thông tin khác như định danh của BS, mã số quốc gia …
- Access control burst
  - Thông tin liên quan đến khả năng thành công của yêu cầu truy nhập kênh ngẫu nhiên
- Dummy burst
  - Lấp các khe trống

Mã hoá kênh

- GSM sử dụng mã hoá cuộn (convolutional encoding) và khối xen kẽ (block interleaving) để tránh cho tiếng nói bị lỗi bit khi truyền
- 260 bit sau mỗi 20 ms
- Các bit chia làm 3 lớp
  - Lớp Ia: 50 bit, nhậy cảm với lỗi bit
  - Lớp Ib: 132 bit, nhậy cảm vừa với lỗi bit
  - Lớp II: 78 bit, ít nhậy cảm nhất với lỗi bit
- Sau khi mã hoá: 456 bit sau mỗi 20 ms, tốc độ 22.8 kbps
- 8 khối 57 bit truyền 8 khe, mỗi bùng phát mang 2 mẫu khác nhau (khối xen kẽ)

Các hoạt động của mạng

* Khả năng chuyển mạng yêu cầu các hoạt động như đăng ký, xác thực, định tuyến, cập nhật vị trí
* Việc chia không gian thành các cell đòi hỏi cơ chế chuyển giao
* Các chức năng của Network Subsystem, chủ yếu sử dụng Mobile Application Part (MAP) dựa trên Signaling System No. 7 (SS7)

Quản lý sự di động

* Nhóm các cell vào các vùng vị trí (location area)
* Khi MS đi vào một vùng vị trí khác, Location Update Identifier (LAI) được gửi đi, cập nhật lại HLR. HLR gửi thông tin về MS cho MSC/VLR mới và thông báo cho MSC/VLR cũ để kết thúc việc đăng ký của MS
* Thực hiện thủ tục cập nhật theo chu kỳ
* Thủ tục detach/attach (tháo gỡ/sát nhập)

MCC (3 digits)	MNC (1 or 2 digits)	LAC (up to 11 digits)

Chuyển giao

- Chuyển giao cuộc gọi giữa 2 cell thuộc hai MSC khác nhau
- Có thể được khởi đầu bởi MS hoặc MSC
- Do MSC: cân bằng tải do lưu lượng
- Do MS: quét BCCH của 16 cell, chọn 6 cell tốt nhất và chuyển thông tin cho BSC và MSC
- Thuật toán chuyển giao
  - Minimum acceptable performance: tăng điện năng để cải thiện tín hiệu, chuyển giao khi chất lượng tín hiệu không tăng
  - Power budget: duy trì chất lượng tín hiệu ở một mức xác định và không thay đổi mức độ điện năng, giảm vấn đề giao thoa, ranh giới, tiêu thụ năng lượng, nhưng phức tạp

Quản lý điện năng

* 5 mức điện năng: 20, 8, 5, 2, 0.8 W
* BS và MS duy trì mức điện năng thấp nhất mà vẫn bảo đảm chất lượng tín hiệu (BER) có thể chấp nhận được
* MS đo BER và chuyển cho BS để quyết định thay đổi mức điện năng

Khởi hoạt

- 1. MS chốt vào tần số mạnh nhất và tìm FCCH
- 2. MS tìm SCH và đồng bộ thời gian với BS
- 3. MS xác định BCCH và đọc các tham số hệ thống như LAC
- 4. MS sử dụng RACH để yêu cầu SDCCH. BS trao quyền truy nhập qua AGCH
- 5. MS tiến hành thủ tục cập nhật vị trí để thông báo cho mạng về vị trí mới. LAC cũ được lưu trong bộ nhớ
- 6. Thủ tục xác thực MS được thực hiện
- 7. HLR và VLR được cập nhật và MS có thể nhận cuộc gọi

Thiết lập cuộc gọi đến MS

* 1. BS báo cho MS về cuộc gọi đến qua PCH
* 2. MS sử dụng RACH để yêu cầu SDCCH. BS chấp nhận yêu cầu qua AGCH
* 3. MS trả lời qua SDCCH
* 4. Thủ tục xác thực MS được tiến hành
* Thiết lập Temporary Mobile Station Identifier (TMSI) mà chỉ có tác dụng trong thời gian của cuộc gọi
* MS được cấp phát một TCH cho cuộc gọi

Xác thực và bảo mật

* Xác thực
  * Khoá bí mật được lưu tại SIM và AuC
  * AuC sinh ra một số ngẫu nhiên và gửi cho MS
  * MS dùng khoá để sinh ra signed response (SRES)
  * Nếu các giá trị tính bởi MS và AuC giống nhau thì MS được xác thực
* Bảo mật, mật mã hoá lưu lượng
  * Số ngẫu nhiên và khoá bí mật được dùng để mật mã hoá lưu lượng