MỤC LỤC

DANH MỤC BẢNG

DANH MỤC HÌNH VẼ

LỜI NÓI ĐẦU

Ở Việt Nam trong những năm gần đây, ngành công nghệ viễn thông đã có những bước phát triển mạnh mẽ, đặc biệt là trong lĩnh vực vô tuyến và di động. Sự phát triển của công nghệ mới kéo theo rất nhiều dịch vụ tiện ích ra đời đáp ứng được nhu cầu ngày càng cao của xã hội. Trong đó phải kể đến các dịch vụ thông tin di động. Điện thoại di động giờ không chỉ dùng để nghe gọi như trước, mà nó đã trở thành một thiết bị di động với đầy đủ các tính năng để phục vụ mọi nhu cầu của con người. Bằng chiếc điện thoại di động của mình người sử dụng có thể gửi các bản tin, nhạc chuông, logo, hình ảnh, …cho người khác, truy cập dữ liệu phục vụ việc học hành. Ngoài ra, người dùng có thể tra cứu thông tin thị trường chứng khoán, thời tiết, chương trình truyền hình …ở mọi nơi, mọi thời điểm, với tốc độ cao không thua kém gì các mạng có dây. Điều này tạo những chuyển biến tích cực trong đời sống kinh tế xã hội trên toàn thế giới, thay đổi cách sống con người.

Cùng với sự phát triển của thông tin di động mang lại nhiều lợi ích cho xã hội thì những nguy cơ và thách thức đối với các nhà cung cấp dịch vụ cũng tăng. Thông tin của người dùng truyền trong môi trường di động có thể bị tấn công hay bị nghe trộm bởi người khác, các dịch vụ của nhà cung cấp có thể bị đánh cắp hay bị phá hoại. Điều này gây thiệt hại lớn cả về kinh tế và chất lượng dịch vụ cho cả người dùng lẫn nhà cung cấp dịch vụ. Những thách thức này đặt ra các yêu cầu cho các nhà cung cấp dịch vụ về vấn đề AN NINH TRONG THÔNG TIN DI ĐỘNG để bảo vệ quyền lợi của người dùng và lợi ích của chính bản thân các nhà cung cấp. Với sự phát triển của thông tin và công nghệ máy tính người ta đã đưa ra các giải pháp về AN NINH TRONG THÔNG TIN DI ĐỘNG khác nhau.

Thế hệ đầu tiên của các hệ thống thông tin di động tổ ong có rất ít các phươnng pháp an ninh bảo vệ những người dùng và khai thác hệ thống. Hệ thống thế hệ thứ hai nhìn chung đã thực hiện điều này tốt hơn nhiều, và bảo vệ được tính bí mật và nhận thực thực tế. Mặc dù đã được cải thiện một cách đáng kể, an ninh thông tin trong thế hệ hai vẫn còn nhiều vấn đề cần phải khắc phục. Hệ thống thông tin di động 3G ra đời đã tạo dựng một kiến trúc an

ninh chắc chắn, nhờ đó cung cấp được những đặc tính an ninh cần thiết.

Hiện nay, hệ thống thông tin di động thế hệ 3G UMTS đã được ITU chấp nhận. Do đó, việc nghiên cứu AN NINH TRONG THÔNG TIN DI ĐỘNG này là một điều hết sức cần thiết.

Xuất phát từ nhu cầu thực tế trên, em đã chọn đề tài nghiên cứa "CÔNG NGHỆ 3G VÀ VẤN ĐỀ BẢO MẬT" để làm đề tài tốt nghiệp

Nội dung đồ án gồm ba chương:

Chương 1. Tổng quan hệ thống thông tin di động

Chương 2. Hệ thông thông tin di động thế hệ thứ ba

Chương 3. Bảo mật trong công nghệ 3G

Dù đã hết sức cố gắng, nhưng do thời gian nghiên cứu, tìm hiểu có hạn và số lượng kiến thức còn hạn chế nên Đồ án của em không tránh khỏi những thiếu sót. Em kính mong nhận được sự cảm thông và góp ý chân thành của các thầy cô cùng các bạn để Đồ án của em hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 25 tháng 10 năm 2010

Sinh viên

NGÔ THỊ PHƯƠNG HOA

Chương 1.
TỔNG QUAN HỆ THỐNG THÔNG TIN DI ĐỘNG

1.1. LỊCH SỬ PHÁT TRIỂN CỦA THÔNG TIN DI ĐỘNG

Từ cuối thế kỷ 18 – 19, công nghệ phát thanh số bằng truyền thông và điện đã được phát triển và sử dụng rộng rãi nhờ các phát minh của Hertz và Marconi. Nhờ các phát minh này mà thế giới đã thay đổi rất nhiều, cũng trong thời gian này hàng loạt các phát minh về tín hiệu điện, công nghệ thông tin điện tử ra đời.

Năm 1946, với kỹ thật FM (điều tần số) ở băng song 150 MHz, AT & T được cấp giấy phép cho dịch vụ điện thoại di động thực sự ở St.Louis.

Năm 1948, một hệ thống điện thoại toàn tự động đầu tiên ra đời ở Richmond, Indiana

Từ những năm 20 ở băng tần vô tuyến 2 MHz, sau thế chiến II mới xuất hiện thông tin di động điện thoại dân dụng.

Từ cuối những năm 40 quan niệm " cellular" được hình thành với Bell.Thay cho mô hình quảng bá với máy phát công suất lớn và anten cao là những cell diện tích bé có máy phát BTS công suất nhỏ. Khi các cell ở cách xa nhau đủ xa thì có thể sử dụng lại cùng một tần số

Từ những năm 60, kênh thông tin di động có dải thông tần số 30 kHz với kỹ thuật FM ở băng tần 450 MHz đưa hiệu xuất sử dụng phổ tần tăng gấp 4 lần so cới cuối thể chiến thứ II

Tháng 12 – 1971 hệ thống cellular kỹ thuật tương tự ra đời, FM, ở dải tần số 850 MHz. là sản phẩm thương nghiệp AMPS (tiêu chuẩn Mỹ) ra đời năm 1983 sản phẩm thương nghiệp AMPS (tiêu chuẩn Mỹ) ra đời.

Năm 1996, một phần mười người Mỹ có điện thoại di động, còn hệ thống điện thoại công sở- vô tuyến đã bao gồm 40 triệu máy, trên 60 triệu điện thoại kéo dài được dùng, dịch vụ PCS thương mại đã được áp dụng ở Washington. Trong thời gian 10 năm qua, các máy điện thoại di động (thiết bị đầu cuối) đã giảm kích thước trọng lượng và giá thành 20% mỗi năm.

Đầu những năm 90, thế hệ đầu tiên của thông tin di động cellular đã bao gồm hàng loạt hệ thống ở các nước khác nhau: TACS, NMTS, NAMTS, C, v.v…

Ngày nay để đáp ứng nhu cầu ngày càng tăng của người sử dụng mà các nhà cung cấp dịch vụ viễn thông trên thế giới đã không ngừng khám phá sáng tạo và phát triển nhiều loại hình mới như CDMA có nhiều dịch vụ mới cũng như đặc tính ưu việt. Công nghệ này sử dụng kỹ thuật trải phổ và đã có ứng dụng chủ yếu trong quân sự, được thành lập năm 1985. Đến nay công nghệ này đã trở thành công nghệ thống trị ở Bắc Mỹ hay các hệ thống nâng cấp CDMA2000, WCDMA…Những hệ thống viễn thông này có thể đáp ứng mọi tiện ích, nhu cầu mà người sử dụng có thể yêu cầu ở nhà cung cấp dịch vụ viễn thông.

1.2. CÁC ĐẶC ĐIỂM CƠ BẢN CỦA HỆ THỐNG THÔNG TIN DI ĐỘNG

- Sử dụng kỹ thuật điều chế số tiên tiến nên hiệu suất sử dụng phổ tần số cao hơn.
- Mã hóa số tín hiệu thoại với tốc độ bít ngày càng thấp, cho phép ghép nhiều kênh thoại hơn với dòng bít tốc độ chuẩn.
- Giảm tỷ lệ tin tức báo hiệu, dành tỷ lệ lớn hơn cho tin tức người sử dụng.
- Áp dụng kỹ thật mã hóa kênh và mã hóa nguồn của truyền dẫn số
- Hệ thống số chống nhiễu kênh chung CCI (Cochannel Interference) và nhiễu kênh kề ACI (Adjacent-Channel Interference) hiệu quả hơn. Điều này cuối cùng tăng dung lượng hệ thống.
- Điều khiển động trong việc cấp phát kênh liên lạc làm cho sử dụng phổ tần số hiệu quả hơn.
- Có nhiều dịch vụ mới: nhận thực, số liệu, mật mã hóa, kết nối với ISDN.
- Điều khiển truy cập và chuyển giao hoàn hỏa hơn. Dung lượng tăng, diện tích cell nhỏ đi, chuyển giao nhiều hơn, báo hiệu tất bật đều dễ dàng xử lý bằng phương pháp số.

1.3. CÁC ĐẶC ĐIỂM TRUYỀN SÓNG

Đặc điểm truyền sóng trong thông tin di động là tín hiệu thu được ở máy thu thay đổi so với tín hiệu phát đi cả về tần số, biên độ, pha và độ trễ.

Các thay đổi này có tính chất rất phức tạp, ngẫu nhiên ảnh hưởng tới chất lượng liên lạc. Về cơ bản chúng có thể phân chia các ảnh hưởng truyền sóng này thành: Ảnh hưởng của hiệu ứng Doppler, tổn hao đường truyền, phadinh đa đường và trải trễ

Hiệu ứng Doppler là sự thay đổi tần số của tín hiệu so với tín hiệu được phát đi, gây bởi chuyển động tương đối giữa máy phát và máy thu trong quá trình truyền sóng. Tổn hao trên đường truyền là sự suy giảm mức điện thu so với mức điện phát. Trong không gian truyền sóng tự do, mức điện trung bình thu do công suất tín hiệu trên một đơn vị diện tích của mặt cầu sóng giảm theo bình phương khoảng cách giữa các anten thu và phát.

Pha-dinh là hiện tượng cường độ điện trường tại điểm thu thay đổi do sự bức xạ nhiều tia.

Trong thông tin di động số, ảnh hưởng của đặc tính truyền dẫn đa đường còn phụ thuộc nhiều vào tỷ số giữa độ dài một dấu (sysmbol) và độ trải trễ (delay spread) của kênh vô tuyến biến đổi theo thời gian. Độ trải trễ có thể xem như độ dài tín hiệu thu được khi một xung cực hẹp được truyền đi. Nếu số liệu được truyền đi với tốc độ thấp thì sự trải trễ có thể được giải quyết rõ ràng tại phần thu.

Ra đời đầu tiên vào cuối năm 1940, đến nay thông tin di động đã trải qua nhiều thế hệ. Dựa vào các đặc điểm và phân loại mà các hệ thống thông tin di động được chia ra làm 3 loại:

- Hệ thống thông tin di động thế hệ thứ nhất (1G)
- Hệ thông thông tin di động thế hệ thứ hai (2G)
- Hệ thông thông tin di động thế hệ thứ ba (3G)

1.4. HỆ THỐNG THÔNG TIN DI ĐỘNG THẾ HỆ THỨ NHẤT(1G)

Hệ thống thông tin di động thế hệ thứ nhất (1G), sử dụng công nghệ analog gọi là đa truy nhập phân chia theo tần số (FDMA) để truyền kênh thoại trên sóng vô tuyến đến thuê bao điện thoại di động.Nhược điểm của các hệ thống này là chất lượng thấp, vùng phủ sóng hẹp và dung lượng nhỏ., nay gọi là CDMA.Trên thị trường vào những năm 1980, một trong những công nghệ 1G phổ biến là NMT được sử dụng ở các nước Bắc Âu, Tây Âu và Nga. Cũng có một số công nghệ khác như AMPS được sử dụng ở Mỹ và Úc.

1.5. HỆ THỐNG THÔNG TIN DI ĐỘNG THẾ HỆ THỨ HAI(2G)

Sau đó, xuất hiện các điện thoại kỹ thuật số, dùng công nghệ 2G, với sóng Digital. Hệ thống thông tin di động thế hệ thứ hai 2G của mạng di động chính thức ra mắt trên chuẩn GSM của Hà lan, do công ty Radiolinja triển khai vào năm 1991.Thiết kế 2G nhấn mạnh hơn về tính tương thích, khả năng chuyển mạng phức tạp và sử dụng truyền dẫn tiếng số hoá trên giao diện vô tuyến.

Tất cả hệ thống thông tin di động thế hệ 2 sử dụng điều chế số, và chúng sử dụng 2 phương pháp đa truy cập:

- Đa truy cập phân chia theo thời gian (TDMA)
- Đa truy cập phân chia theo mã (CDMA)

1.5.1. Đa truy cập phân chia theo thời gian (TDMA)

Khả năng công nghệ về mã hóa thoại và nén dữ liệu cho phép trừ bỏ độ dư và khoảng lặng trong truyền thoại, cũng cho phép giảm thời gian cần thiết để trình diễn tín hiệu thoại.Các thuê bao truy cập kênh theo một chương trình. Phổ qui định cho liên lạc di động được chia thành các dải tần liên lạc, mỗi dải tần liên lạc này dùng chung cho N kênh liên lạc, mỗi kênh liên lạc là một khe thời gian trong chu kỳ một khung. Các thuê bao khác dùng chung kênh nhờ cài xen thời gian, mỗi thuê bao được cấp phát một khe thời gian trong cấu trúc khung, đặc điểm:

- Tín hiệu của thuê bao được truyền dẫn số
- Liên lạc song công mỗi hướng thuộc các dải tần liên lạc khác nhau
- Giảm nhiễu giao thoa
- Giảm số máy thu phát ở BTS
- Hệ thống TDMA điển hình là hệ thống thông tin di động toàn cầu GSM.

1.5.2. Đa truy cập phân chia theo mã (CDMA)

Mỗi MS được gán một mã riêng biệt và kỹ thuật trải phổ tín hiệu giúp cho các MS không gây nhiễu lẫn nhau trong điều kiện có thể cùng một lúc chung dải tần số.

Đặc điểm:

- Dải tần tín hiệu rộng hàm MHz

- Sử dụng kỹ thuật trải phổ phức tạp
- Kỹ thuật trải phổ cho phép tín hiệu vô tuyến sử dụng có cường độ trường hiệu quả hơn FDMA, TDMA

Một số hệ thống 2G đang tiến hóa đến ít nhất một phần các yêu cầu trên. Điều này dẫn đến một hậu quả không mong muốn là lam sai lệch thuật ngữ"các thế hệ". Chẳng hạn GSM với hỗ trợ số liệu kênh được phân loại như hệ thống 2G thuần túy. Khi tăng cường thêm dịch vụ vô tuyến gói chung (GPRS), nó trở nên phù hợp với nhiều tiêu chuẩn 3G. Dẫn đến nó không hẳn là 2G cũng như 3G mà là loại "giữa các thế hệ", vì thế hệ thống GSM được tăng cường GPRS hiện nay được gọi là hệ thống 2,5G.Trong khi thực tế vẫn thuộc loại 2G, ít nhất là về phương diện công nghệ truyền dẫn vô tuyến.

1.5.3. Hệ thống thông tin di động thế hệ 2,5G-GPRS

Có thể coi GPRS là phần mở rộng của cấu trúc mạng GSM đã có sẵn từ trước sử dụng kỹ thuật gói để truyền báo hiệu cũng như truyền số liệu một cách hiệu quả nhất. GPRS tối ưu hóa việc sử dụng các nguồn tài nguyên vô tuyến cũng như hạ tầng mạng. Việc tách riêng các hệ thống vô tuyến (radio-system) với hệ thống con của mạng (network Subsystem) cho phép phần hệ thống con của mạng có khả năng sử dụng các công nghệ truy nhập vô tuyến khác nhau. GPRS không làm thay đổi các chức năng cơ bản sẵn có của GSM mà tận dụng một cách tối đa các thiết bị hiện có trong mạng GSM.

Mục tiêu chính của GSM là cung cấp một chế độ truyền dẫn gói hiệu quả từ đầu đến cuối cho phép người sử dụng có thể truy cập mạng mà không cần sử dụng thêm một thiết bị phụ trợ nào khác với chi phí thấp.

Điểm quan trọng và cơ bản nhất của giải pháp GPRS là hệ thống sử dụng một cách hiệu quả tài nguyên vô tuyến, nghĩa là nhiều khách hàng có thể chia sẻ cùng băng thông và được một cell duy nhất phục vụ.

GPRS còn hỗ trợ giao thức IP. Đây là một giao thức được dùng phổ biến nhất trên thế giới để truyền số liệu vì vậy GPRS có khả năng kết nối với nhiều thiết bị hệ thống khác nhau. Một đặc điểm khác cũng rất quan trọng của GPRS là nó sử dụng các giao diện mở. Các giao diện sử dụng trong GPRS đều là các giao diện chuẩn, do vậy người sử dụng có thể sử dụng các thiết bị do các nhà sản xuất khác nhau cung cấp.

Ta xét các kiểu hoạt động của MS trong GPRS:

Bảng 1. Các kiểu hoạt động của MS trong GPRS

Lớp	Cơ chế hoạt động
A	Các dạng gói đồng thời và chuyển mạch kênh
B	Tự động chọn dạng chuyển mạch kênh hay chuyển mạch gói
C	Chuyển mạch gói

Một MS của GPRS bao gồm các kết cuối Mobile (MT), là thiết bị tạo ra cơ chế cho việc thu phát tín hiệu dữ liệu và bên cạnh đó là thiết bị kết cuối (TE) là một thiết bị giống như một PC mà các ứng dụng có thể chạy trên đó. Chức năng của MS hoạt động theo 3 cơ chế trên

1.6. HỆ THỐNG THÔNG TIN DI ĐỘNG THẾ HỆ THỨ BA (3G)

Thông tin di động thế hệ 2 mặc dù sử dụng công nghệ số nhưng là hệ thống băng hẹp và được xây dựng trên cơ chế chuyển mạch kênh nên không thể đáp ứng được dịch vụ mới này. 3G công nghệ thế hệ thứ ba là giai đoạn mới nhất trong sự tiến hóa của ngành viễn thông di động. Nếu (1G)của điện thoại di động là những thiết bị analog, chỉ có khả năng truyền thoại. (2G)của ĐTDĐ gồm cả hai công năng truyền thoại và dữ liệu giới hạn dựa trên kỹ thuật số. Trong bối cảnh đó ITU đã đưa ra đề án tiêu chuẩn hóa hệ thống thông tin di động thế hệ thứ 3 với tên gọi IMT – 2000. IMT – 2000 đã mở rộng đáng kể khả năng cung cấp dịch vụ và cho phép sử dụng nhiều phương tiện thông tin.

Mục đích của IMT – 2000 là đưa ra nhiều khả năng mới nhưng cũng đồng thời đảm bảo sự phát triển liên tục của hệ thống thông tin di động thế hệ thứ hai (2G) vào những năm 2000. 3G mang lại cho người dùng các dịch vụ giá trị tăng cao cấp, giúp chúng ta thực hiện truyền thông thoại và dữ liệu (như e-mail và tin nhắn dạng văn bản), download âm thanh và hình ảnh với băng tần cao. Các ứng dụng 3G thông dụng gồm hội nghị video di động; chụp và gửi ảnh kỹ thuật số nhờ điện thoại máy ảnh, gửi và nhận e-mail và file đính kèm dung lượng lớn, tải tệp tin video và MP3, thay thế cho modem để kết nối đến máy tính xách tay hay và nhắn tin dạng chữ với chất lượng cao…

Tốc độ của hệ thống thông tin di động thứ 3 được quy định:

- 384Kb/s đối với vùng phủ sóng rộng.
- 2Mb/s đối với vùng phủ sóng địa phương

Các chỉ tiêu chung để xây dựng hệ thống thông tin di động thế hệ 3:

- Sử dụng dải tần quy định quốc tế 2GHz như sau:
  - ✓ Đường lên: 1885 – 2025 MHz;
  - ✓ Đường xuống: 2110 -2200 MHz.

IMT-2000 hỗ trợ tốc độ đường truyền cao hơn: tốc độ tối thiểu là 2Mbps cho người dùng văn phòng hoặc đi bộ; 348Kbps khi di chuyển trên xe. Trong khi đó, hệ thống viễn thông 2G chỉ có tốc độ từ 9,6Kbps tới 28,8Kbps.

- Là hệ thống thông tin di động toàn cầu cho các loại hình thông tin vô tuyến:
  - ✓ Tích hợp các mạng thông tin hữu tuyến và vô tuyến
  - ✓ Tương tác cho mọi loại dịch vụ viễn thông từ cố định, di động, thoại dữ liệu, dữ liệu, internet đến các dịch vụ đa phương tiện
- Có thể hỗ trợ các dịch vụ như:
  - ✓ Các phương tiện tại nhà ảo trên cơ sở mạng thông minh, di động các nhân và chuyển mạng toàn cầu
  - ✓ Đảm bảo chuyển mạng quốc tế cho phép người dùng có thể di chuyển đến bất kỳ quốc gia nào cũng có thể sử dụng một số điện thoại duy nhất.
  - ✓ Đảm bảo các dịch vụ đa phương tiện đồng thời cho tiếng, số liệu chuyển mạch kênh và số liệu chuyển mạch gói.
  - ✓ Dễ dàng hỗ trợ các dịch vụ mới xuất hiện.
- Môi trường hoạt động của IMT – 2000 được chia thành 4 vùng với tốc độ bit R như sau:
  - ✓ Vùng 1: Trong nhà, ô pico, $R_b \leq 2$ Mbit/s
  - ✓ Vùng 2: Thành phố, ô macrô, $R_b \leq 384$ kbit/s
  - ✓ Vùng 2: Ngoại ô, ô macrô, $R_b \leq 144$ kbit/s
  - ✓ Vùng 4: Toàn cầu, $R_b = 9,6$ kbit/s.

1.7. TỔNG KẾT MỘT SỐ NÉT CHÍNH CỦA CÁC NỀN TẢNG CÔNG NGHỆ THÔNG TIN DI ĐỘNG TỪ THẾ HỆ 1 ĐẾN THẾ HỆ 3

Bảng 2. Những nét chính của thông tin di động từ thế hệ 1 đến thế hệ 3

Thế hệ thông tin di động	Hệ thống	Dịch vụ chung	Chú thích
Thế hệ 1 (1G)	AMPS,TACS, NMT	Tiếng thoại	FDMA, tương tự
Thế hệ 2 (2G)	GSM, IS-136, IS-95	Chủ yếu cho dich vụ tiếng và bản tin ngắn	TDMA hoặc CDMA, số, băng hẹp (8-13kbps)
Thế hệ trung gian (2,5G)	GPRS, EDGE, CDMA 2000-1x	Trước hết là dịch vụ tiếng có đưa thêm các dịch vụ gói	TDMA, CDMA, Sử dụng chồng lên phổ tần của thế hệ 2 nếu không sử dụng phổ tần mới, tăng cường truyền số liệu cho thế hệ 2
Thế hệ 3 (3G)	CDMA 2000 WCDMA	Các dịch vụ tiếng và số liệu gói được thiết kế để truyền tiếng và số liệu đa phương tiện. Là nền tảng thực sự của thế hệ 3	CDMA, CDMA kết hợp với TDMA, băng rộng, sử dụng chồng lần lên hệ thống thứ 2 hiện có nếu không sử dụng phổ tần mới.

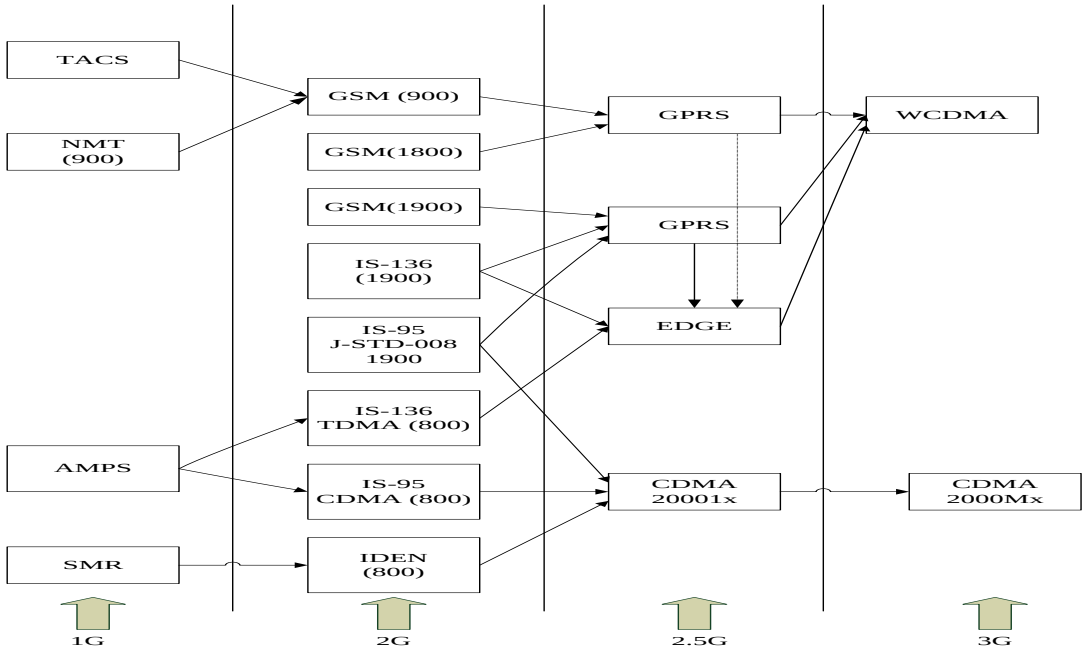
Chương 2.
HỆ THỐNG THÔNG TIN DI ĐỘNG THẾ HỆ THỨ 3

2.1. MỞ ĐẦU

Xu thế chung của công nghệ di động là phải đáp ứng nhu cầu ngày càng cao về chất lượng, dung lượng, tính tiện lợi, giá cả, tính đa dạng về dịch vụ của người sử dụng. Vì vậy sau khi tồn tại một thời gian thì các công nghệ 2G đã bộc lộ các điểm yếu là không thể đáp ứng được yêu cầu trên mà phải đợi đến công nghệ 3G. Đối với các nhà khai thác dịch vụ di động cũng vậy, họ không chỉ dừng lại ở công nghệ đang khai thác mà luôn có lộ trình cho việc phát triển các công nghệ tiếp theo.Trong tiến trình phát triển lên công nghệ không dây thế hệ tiếp theo (3G) nổi lên 2 hướng phát triển theo hai tiêu chuẩn chính đã được ITU-T công nhận đó là CDMA2000 và W-CDMA

+ WCDMA là sự nâng cấp của các hệ thống thông tin di động thế hệ 2 sử dụng công nghệ TDMA như: GSM, IS-36.

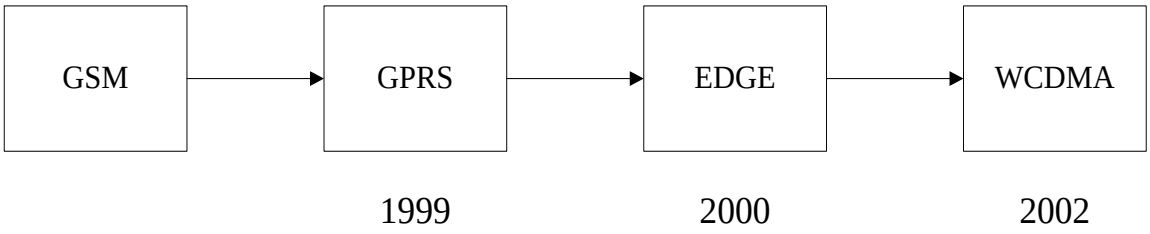
+ CDMA2000 là sự nâng cấp của hệ thống thông tin di động thế hệ 2 sử dụng công nghệ CDMA: IS-95.



Hình 2.1. Quá trình phát triển của các hệ thống thông tin di động từ thế hệ 1 đến thế hệ 3

2.1.1. Hướng phát triển lên 3G sử dụng công nghệ WCDMA.

WCDMA là một tiêu chuẩn thông tin di động 3G của IMT-2000 được phát triển chủ yếu ở châu Âu với mục đích cho phép các mạng cung cấp khả năng chuyển vùng toàn cầu và để hỗ trợ nhiều dịch vụ thoại, dịch vụ đa phương tiện. Các mạng WCDMA được xây dựng trên cơ sở mạng GSM, tận dụng cơ sở hạ tầng sẵn có của các nhà khai thác mạng GSM. Quá trình phát triển từ GSM lên CDMA qua các giai đoạn trung gian, có thể được tóm tắt trong sơ đồ sau đây:



Hình 2.2. Quá trình phát triển lên 3G theo nhánh WCDMA

2.1.1.1. GPRS.

GPRS là một hệ thống vô tuyến thuộc giai đoạn trung gian, là bước đệm quan trọng để tiến tới 3G của các hệ thống GSM, nhưng vẫn là hệ thống 3G nếu xét về mạng lõi. GPRS cung cấp các kết nối số liệu chuyển mạch gói với tốc độ truyền lên tới 171,2Kpbs (tốc độ số liệu đỉnh) và hỗ trợ giao thức Internet TCP/IP và X25, nhờ vậy tăng cường đáng kể các dịch vụ số liệu của GSM.

Mạng lõi GSM được tạo thành từ các kết nối chuyển mạch kênh được mở rộng bằng cách thêm vào các nút chuyển mạch số liệu và gateway mới, được gọi là GGSN (Gateway GSM Support Node) và SGSN (Serving GPRS Support Node). GPRS là một giải pháp đã được chuẩn hóa hoàn toàn với các giao diện mở rộng và có thể chuyển thẳng lên 3G về cấu trúc mạng lõi.

2.1.1.2. EDGE

EDGE là một kỹ thuật truyền dẫn 3G đã được chấp nhận và có thể triển khai trong phổ tần hiện có của các nhà khai thác TDMA và GSM. EDGE sử dụng băng tần tái sử dụng sóng mang và cấu trúc khe thời gian của GSM, và được thiết kế nhằm tăng tốc độ số liệu của người sử dụng trong mạng GPRS hoặc HSCDS bằng cách sử dụng các hệ thống cao cấp và công nghệ tiên tiến khác. Vì vậy cơ sở hạ tầng và thiết bị đầu cuối hoàn toàn phù hợp với EDGE hoàn toàn tương thích với GSM và GPRS.

2.1.1.3. WCDMA

WCDMA là một công nghệ truy nhập vô tuyến được phát triển mạnh ở Châu Âu. Hệ thống này hoạt động ở chế độ FDD và dựa trên kỹ thuật trải phổ chuỗi trực tiếp, sử dụng tốc độ chip 3,84Mcps bên trong băng tần 5MHz. Băng tần rộng hơn và tốc độ trải phổ cao làm tăng độ lợi xử lý và một giải pháp thu đa đường tốt hơn, đó là một đặc điểm quyết định để chuẩn bị cho IMT-2000.

WCDMA hỗ trợ trọn vẹn cả dịch vụ chuyển mạch kênh và chuyển mạch gói tốc độ cao và đảm bảo sự hoạt động đồng thời các dịch vụ hỗn hợp với chế độ gói hoạt động ở mức hiệu quả nhất. Hơn nữa WCDMA có thể hỗ trợ các tốc độ số liệu khác nhau, dựa trên thủ tục điều chỉnh tốc độ.

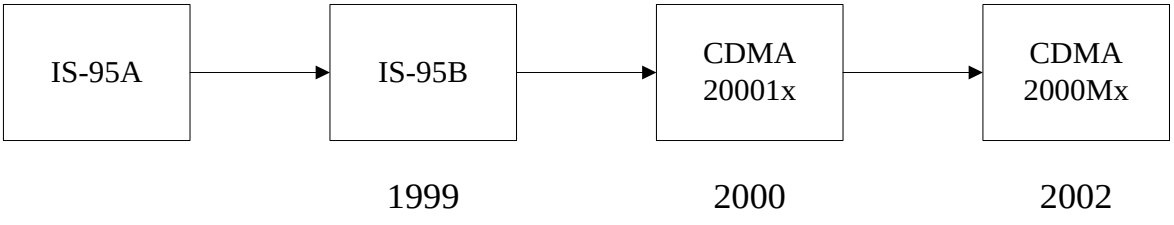
Chuẩn WCDMA hiện thời sử dụng phương pháp điều chế QPSK, một phương pháp điều chế tốt hơn 8-PSK, cung cấp tốc độ số liệu đỉnh là 2Mbps với chất lượng truyền tốt trong vùng phủ rộng.

WCDMA là công nghệ truyền dẫn vô tuyến mới với mạng truy nhập vô tuyến mới, được gọi là UTRAN, bao gồm các phần tử mạng mới như RNC (Radio Network Controller) và node B (tên gọi trạm gốc mới trong UMTS)

Tuy nhiên mạng lõi GPRS/EDGE có thể được sử dụng lại và các thiết bị đầu cuối hoạt động ở nhiều chế độ có khả năng hỗ trợ GSM/GPRS/EDGE và cả WCDMA

2.1.2. Hướng phát triển lên 3G sử dụng công nghệ CDMA2000.

Hệ thống CDMA2000 gồm một số nhánh hoặc giai đoạn phát triển khác nhau để hỗ trợ các dịch vụ phụ được tăng cường. Nói chung CDMA2000 là một cách tiếp cận đa sóng mang cho các sóng có độ rộng n lần 1,25MHz hoạt động ở chế độ FDD. Những công việc chuẩn hóa tập trung vào giải pháp một sóng mang đơn 1,25MHz (1x) với tốc độ chip gần giống IS-95. CDMA2000 được phát triển từ các mạng IS-95 của hệ thống thông tin di động 2G, có thể mô tả quá trình phát triển trong hình vẽ sau:



Hình 2.3. Quá trình phát triển lên 3G theo nhánh CDMA2000

2.1.2.1. IS-95B

IS-95B hay CDMA One được gọi là công nghệ thông tin di động 2,5G thuộc nhánh phát triển CDMA2000, là một tiêu chuẩn khá linh hoạt cho phép cung cấp dịch vụ số liệu lên đến 115Kbps.

2.1.2.2. CDMA20001xRTT

Giai đoạn đầu của CDMA2000 được gọi là 1xRTT hay chỉ là 1xEV-DO, được thiết kế nhằm cải thiện dung lượng thoại của IS-95B và để hỗ trợ khả năng truyền số liệu ở tốc độ đỉnh lên tới 307,2Kbps. Tuy nhiên các thiết bị đầu cuối thương mại của 1x mới chỉ cho phép tốc độ số liệu đỉnh lên tới 153,6Kbps. Những cải thiện so với IS-95 đạt được nhờ đưa vào một số công nghệ tiên thiến như điều chế QPSK và mã hóa Turbo cho các dịch vụ số liệu cùng với khả năng điều khiển công suất nhanh ở đường xuống và phân tập phát.

2.1.2.3. CDMA20001xEV-DO

1xEV-DO, được hình thành từ công nghệ HDR (High Data Rate) của Qualcomm, được chấp nhận với tên này như là một tiêu chuẩn thông tin di động 3G vào tháng 8 năm 2001 và báo hiệu cho sự phát triển của giải pháp đơn sóng mang với truyền số liệu gói riêng biệt.

Nguyên lý cơ bản của hệ thống này là chia các dịch vụ thoại và dịch vụ số liệu tốc độ cao vào các sóng mang khác nhau. 1xEV-DO có thể được xem như một mạng số liệu xếp chồng, yêu cầu một sóng mang riêng. Để tiến hành các cuộc gọi vừa có thoại, vừa có số liệu trên cấu trúc xếp chồng này cần có các thiết bị hoạt động ở 2 chế độ 1x và 1xEV-DO.

2.1.2.4. CDMA2000 1xEV-DV

Trong công nghệ 1xEV-DO có sự dư thừa về tài nguyên do sự phân biệt cố định tài nguyên dành cho thoại và tài nguyên dành cho số liệu. Do đó, nhóm phát triển CDMA, khởi đầu pha thứ 3 của CDMA2000 đưa các dịch vụ thoại và số liệu quay về chỉ dùng một sóng mang 1,25MHz và tiếp tục duy trì sự tương thích ngược với 1xRTT. Tốc độ số liệu cực đại của người sử dụng lên tới 3,1Mbps tương ứng với kích thước gói dữ liệu 3940 bit trong khoảng thời gian 1,25ms.

Mặc dù kỹ thuật truyền dẫn cơ bản được định hình, vẫn có nhiều đề xuất công nghệ cho các thành phần chưa được quyết định kể cả tiêu chuẩn cho đường xuống của 1xEV-DV.

2.1.2.5. CDMA20003x (MC-CDMA)

CDMA20003x hay 3xRTT, đề cập đến sự lựa chọn đa sóng mang ban đầu trong cấu hình vô tuyến CDMA2000 và được gọi là MC-CDMA thuộc IMT-MC trong IMT-2000. Công nghệ này liên quan đến việc sử dụng 3 sóng mang 1x để tăng tốc độ số liệu và được thiết kế cho dải tần 5MHz (gồm 3 kênh 1,25MHz). Sự lựa chọn đa sóng mang này chỉ áp dụng được trong truyền dẫn đường xuống. Đường lên trải phổ trực tiếp, giống như WCDMA với tốc độ chip hơi thấp hơn một chút 3,6864 Mcps (3 lần 1,2288cps).

Để phát triển lên 3G thì các nhà khai thác đã phải trải qua nhiều công nghệ trung gian như đã trình bày ở trên. Trong đó có các công nghệ trung gian quan trọng để tiến đến 3G theo em thấy đó là: GPRS, EDGE, CDMA 20001x.

2.1.3. Công nghệ GPRS

2.1.3.1. Tổng quan mạng GPRS

Dịch vụ này sẽ đem lại cơ hội mới cho các nhà cung cấp dịch vụ điện thoại di động qua việc triển khai thêm các ứng dụng IP và thu hút thêm nhiều khách hàng. Điểm quan trọng và cơ bản nhất của giải pháp GPRS là hệ thống sử dụng một cách hiệu quả tài nguyên vô tuyến (phổ tần – nghĩa là nhiều khách hàng có thể cùng chia sẻ băng thông và được một cell duy nhất phục vụ). Nhằm cung cấp dịch vụ một cách mềm dẻo, với nhiều phương thức tính cước khác nhau (tính theo thời gian truy nhập, tính theo dung lượng dữ liệu trao đổi…).

GPRS là một dịch vụ mới dành cho GSM nhằm cải thiện và đơn giản hóa truy cập không dây tới các mạng dữ liệu gói, ví dụ như mạng Internet. Nó áp dụng nguyên tắc vô tuyến gói để truyền các gói dữ liệu của người sử dụng một cách hiệu quả từ máy di động GPRS đến các mạng chuyển mạch.

Mục tiêu chính của GPRS là cung cấp một chế độ truyền dẫn gói hiệu quả từ đầu đến cuối cho phép người sử dụng có thể truy nhập mạng mà không cần sử dụng thêm một thiết bị phụ trợ nào khác với chi phí thấp.

Dịch vụ vô tuyến gói đa năng GPRS là một chuẩn của Châu Âu. Đây là một kỹ thuật mới áp dụng cho mạng thông tin di động GSM. Nó cung cấp dịch vụ dữ liệu gói bên trong mạng PLMN và giao tiếp với các mạng ngoài qua cổng đấu nối trực tiếp như TCP/IP, X.25…Điều này cho phép các thuê bao di động GPRS có thể truy nhập vào mạng Internet và truyền dữ liệu lên đến 171 Kb/s. Trong mạng GPRS, một MS chỉ được dành tài nguyên vô tuyến

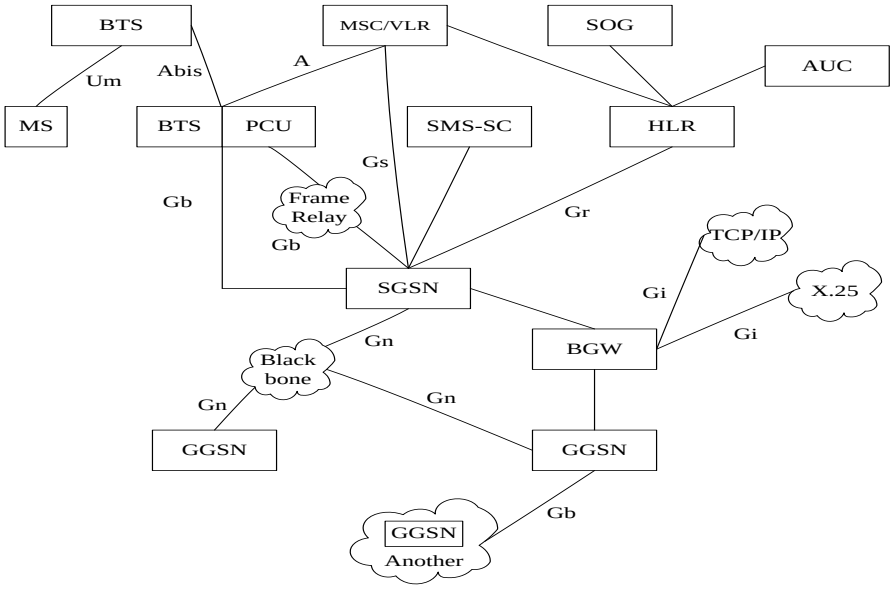
khi có số liệu cần phát và ở thời điểm khác những người sử dụng có thể dùng chung một tài nguyên vô tuyến. Nhờ vậy mà hiệu quả sử dụng băng tần lên đáng kể.

GPRS có hai mục tiêu chính:

+ Kết hợp các kênh và đưa ra các kế hoạch mã hóa kênh mới để đạt được tốc độ truyền dẫn cao hơn.

+ Sử dụng các tài nguyên vô tuyến một cách hiệu quả hơn bằng cách sử dụng GPRS đã khắc phục được các nhược điểm chính của thông tin chuyển mạch kênh truyền thống, bằng cách chia nhỏ số liệu thành từng gói nhỏ rồi truyền đi theo một trật tự qui định và chỉ sử dụng tài nguyên vô tuyến khi cần phát hoặc thu.

2.1.3.2. Kiến trúc mạng GPRS



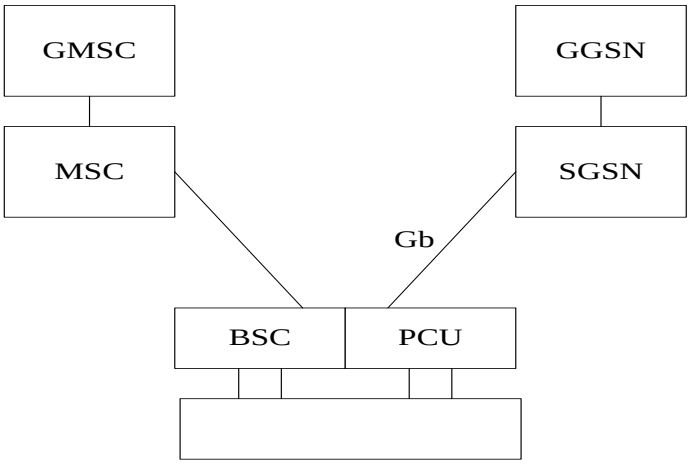
Hình 2.4. Kiến trúc mạng GPRS

GPRS được phát triển trên cơ sở mạng GSM sẵn có. Các phần tử của mạng GSM chỉ cần nâng cấp về phần mềm, ngoại trừ BSC phải nâng cấp về phần cứng. GSM lúc đầu được thiết kế cho chuyển mạch kênh nên việc đưa dịch vụ chuyển mạch gói vào mạng đòi hỏi phải bổ sung thêm thiết bị mới. Đó là node GSN, hai node được thêm vào để làm nhiệm vụ quản lý chuyển mạch gói là node hỗ trợ GPRS dịch vụ (SGSN) và node hỗ trợ cổng (GGSN). Hai node này thực hiện thu phát các gói số liệu giữa các MS và các thiết bị đầu cuối số liệu cố định của mạng cố định công cộng (PDN). GSN còn cho

phép thu – phát các gói số liệu đến các MS ở các mạng thông tin di động GSM khác.

2.1.3.3. Cấu trúc BSC trong GPRS

Để nâng cấp mạng GSM lên GPRS, ngoài việc nâng cấp phần mềm ta cần bổ sung vào trong BSC một phần cứng gọi là khối kiểm soát gói PCU (Packet Control Unit). Khối này có nhiệm vụ xử lý việc truyền dữ liệu gói giữa máy đầu cuối và SGSN trong mạng GPRS.



Hình 2.5. Giao diện Gb mở kết nối PCU với SGSN

PCU quản lý các lớp MAC và RLC của giao diện vô tuyến, các lớp dịch vụ mạng của giao diện Gb (giao diện giữa PCU và SGSN) . Nó bao gồm phầm mềm trung tâm, các thiết bị phần cứng và các phần mềm vùng (RPPs). Chức năng RPP là phân chia các khung PCU giữa các giao diện Gb và Abis. Chúng có thể được thiết lập để làm việc với giao diện Abis hay với cả hai giao diện Abis và Gb. Giải pháp bổ sung PCU vào BSC là một giải pháp hiệu quả về mặt chi phí hệ thống.

Về mặt truyền dẫn thì giao diện Abis được sử dụng cho cả chuyển mạch kênh và chuyển mạch gói trên GPRS nhưng giao diện giữa BSS và SGSN lại dựa trên giao diện mở Gb. Thông qua Abis các đường truyền dẫn và báo hiệu hiện tại của GSM được sử dụng lại trong GPRS nên đem lại hiệu suất cao và hiệu quả trong giá thành. Giao diện Gb là một đề xuất mới nhưng nó có thể lưu thông Gb một cách trong suốt thông qua MSC.

2.1.4. Công nghệ EDGE

Để tiếp tục tối ưu hóa hệ thống GSM của mình, nhà khai thác có thể sử dụng công nghệ EDGE. EDGE là một bước phát triển cao hơn của GPRS

nhằm tiếp cận hơn với yêu cầu của 3G, nó có thể triển khai trên phổ tần sẵn có của nhà khai thác TDMA và GSM. So với GPRS, EDGE tập trung vào cải thiện phần truy nhập vô tuyến bằng cách sử dụng các phương thức điều chế mức cao và một số kỹ thuật mã hóa tiên tiến khác. Nhờ vậy tốc độ dữ liệu tối đa của người sử dụng trên một sóng mang 200KHz có thể đạt được là 473.6kbps.

Việc quy hoạch mạng vô tuyến sẽ ít bị ảnh hưởng khi triển khai công nghệ EDGE. Cụ thể các BTS được tiếp tục sử dụng, các nút chuyển mạch gói GPRS cũng không bị ảnh hưởng do chức năng độc lập với tốc độ bit của thuê bao. Toàn bộ thay đổi với các nút chuyển mạch của mạng chỉ là việc nâng cấp phần mềm. Thiết kế cũng cho phép đầu cuối EDGE nhỏ gọn và giá cả cạnh tranh được.

Các kênh truyền dẫn trong EDGE cũng thích hợp cho các dịch vụ GSM và không có sự phân biệt giữa dịch vụ EDGE, GPRS hay GSM. Xét trên quan điểm nhà khai thác thì các dịch vụ EDGE nên triển khai trước tiên cho các khu vực nóng sau đó mở rộng dần theo nhu cầu cụ thể. Việc nâng cấp phần cứng BSS theo công nghệ EDGE có thể quan niệm như nâng cấp và mở rộng mạng để đáp ứng phát triển thuê bao thông thường. Khả năng 3G băng rộng có thể thực hiện từng bước bằng cách triển khai dần giao diện vô tuyến mới 3G trên mạng lõi GSM hiện tại. Điều này đảm bảo an toàn đầu tư và chính sách khách hàng cho nhà khai thác.

Đối với các nhà khai thác có giấy phép cho băng tần mới 2GHz thì có thể triển khai IMT-2000 cho các khu vực phủ sóng sớm có nhu cầu lớn nhất về các dịch vụ 3G. Đầu cuối 2 chế độ EDGE/IMT-2000 sẽ cho phép thuê bao thực hiện chuyển vùng và chuyển giao giữa các hệ thống. So với phương án xây dựng mạng 3G hoàn toàn mới thì việc phát triển dần trên mạng GSM sẽ nhanh chóng và rẻ tiền hơn. Các bước trung gian GPRS và EDGE cũng có thuận lợi là phát triển lên 3G dễ dàng.

Thực tế, viêc tăng tốc dữ liệu trên giao diện vô tuyến đòi hỏi thiết kế lại các phương thức truyền dẫn vật lý, khuôn dạng khung, giao thức báo hiệu tại các giao diện mạng khác nhau. Do vậy, tùy thuộc vào yêu cầu cụ thể về tốc độ dữ liệu để lựa chọn phương án nâng cấp hệ thống nhằm tăng tốc độ dữ liệu trên các giao diện Abis. EDGE vẫn dựa vào công nghệ chuyển mạch kênh và

chuyển mạch gói với tốc độ tối đa đạt được là 384Kbps nên sẽ khó khăn trong việc hỗ trợ các ứng dụng đòi hỏi việc chuyển mạch linh động và tốc độ truyền dữ liệu lớn hơn. Lúc này sẽ thực hiện nâng cấp EDGE lên W-CDMA và hoàn tất nâng cấp GSM lên 3G.

Các kế hoạch và biện pháp khi áp dụng EDGE trên GSM

Để có thể thực hiện EDGE trên GSM, việc cần thiết là phải tiến hành từng bước thông qua các kế hoạch phủ sóng, tần số, quản lý kênh, điều khiển công suất để không làm ảnh hưởng đến việc khai thác.

+ Kế hoạch phủ sóng: Tỉ lệ sóng mang / nhiễu thấp chỉ làm giảm tốc độ truyền dữ liệu. Một tế bào EDGE sẽ cùng phục vụ cho nhiều người sử dụng với tốc độ yêu cầu khác nhau, tốc độ bit trung tâm sẽ cao và bị giới hạn ở biên tế bào.

+ Kế hoạch tần số: Nhờ kỹ thuật tương hợp đường kết nối trên EDGE vẫn sử dụng mẫu tần số 3/9 vì ảnh hưởng tỉ số nhiễu cùng kênh không tác động đến chất lượng mạng.

+ Điều khiển công suất: Các hệ thống GSM sử dụng tính năng điều khiển công suất tự động ở máy đầu cuối và trạm thu – phát BTS. Tính năng này cho phép giảm công suất khi thuê bao tiến lại gần trạm và tăng công suất khi thuê bao rời xa trạm. Việc tự động này sẽ tăng tuổi thọ hệ thống và pin máy đầu cuối đồng thời nâng cao chất lượng cuộc gọi. EDGE cũng hỗ trợ chức năng này mặc dù cũng có một số điểm khác biệt so với GSM.

+ Quản lý kênh: Mỗi kênh vật lý trong tế bào có thể là một trong các loại như: Thoại GSM và dữ liệu chuyển mạch kênh, dữ liệu gói GPRS, dữ liệu chuyển mạch kênh EDGE – ECSD hay dữ liệu gói EDGE cho phép hỗn hợp giữa GPRS và EGPRS.

2.1.5. Công nghệ CDMA 20001X

1X là công nghệ tiếp theo của IS-95. Thuật ngữ 1X là viết tắt của 1XRTT. Tổ chức viễn thông quốc tế ITU đã công nhận chính thức 1X là công nghệ 3G vào năm 1999. Hệ thống CDMA 20001X được đưa vào sử dụng lần đầu tiên tại Hàn Quốc do công ty SK – Telecom vào tháng 10 năm 2000 và tiếp theo đó được triển khai tại một số nước ở Châu Á, Mỹ và Châu Âu. Có thể nối số thuê bao của hệ thống này tăng trưởng một cách nhanh chóng theo, con số thống kê thì mỗi ngày số thuê bao của hệ thống này tăng 700.000

người, điều này cho thấy chất lượng cũng như dịch vụ của hệ thống CDMA được đánh giá rất cao.

Hệ thống CDMA 20001X là hệ thống theo các chuẩn báo hiệu như SS7 và IS-41, trung tâm dịch vụ bản tin ngắn, hệ thống Voicemail, các dịch vụ trả trước, hệ thống dữ liệu gói và PSTN. Giải pháp mạng đảm bảo cho phép có thể thực hiện các dịch vụ thoại và dữ liệu đồng thời, các dịch vụ dữ liệu gói trên cơ sở giao thức IP.

Có thể nói CDMA 2001x là một bước phát triển đầy tự nhiên của công nghệ CDMA trong đó sự kết hợp chặt chẽ với các dịch vụ dữ liệu gói đã tồn tại trong các mạng khác. Các nhà cung cấp dịch vụ của hệ thống CDMA có thể triển khai các dịch vụ dữ liệu gói đã tồn tại trong các mạng khác. Các nhà cung cấp dịch vụ của hệ thống CDMA có thể triển khai các dịch vụ dữ liệu của hệ thống 1x bằng việc sử dụng cơ sở hạ tầng sẵn có của mạng CMDA One đã tồn tại. Với việc cung cấp các dịch vụ gói dữ liệu và tốc độ truyền dữ liệu không dây với tốc độ cao lên đến 144Kbps thì mạng CDMA 20001x cho phép các khách hàng có thể truy cập vào mạng Internet hoặc mạng Lan của các công ty lớn.

2.1.6. Tổng kết.

Như vậy trên thế giới hiện đang tồn tại các công nghệ khác để xây dựng hệ thống thông tin di động 3G, và thực hiện theo hướng triển khai 3G hỗ trợ cho 2G, phát triển 3G từ 2G lên, đặc biệt hỗ trợ cho các mạng đã thành công của 2G. Hiện nay mạng thông tin di động ở Việt Nam đang sử dụng chủ yếu công nghệ GSM, tuy nhiên trong tương lai mạng thông tin này sẽ không đáp ứng dược các nhu cầu về thông tin di động,do đó việc nghiên cứu và triển khai mạng thông tin di động CDMA là một tất yếu. Ở Bắc Mỹ, công nghệ này đã trở thành công nghệ thống trị và là nền tảng của thông tin di động thế hệ 3. Ở Đồ án này em đi sâu, tìm hiểu về hướng phát triển lên 3G sử dụng công nghệ CDMA2000.

2.2. CÔNG NGHỆ CDMA 2000

2.2.1. Nguyên lý CDMA

2.2.1.1. Tổng quan

Lý thuyết về CDMA đã được xây dựng từ những năm 1950 và được áp dụng trong thông tin quân sự từ những năm 1960. Cùng với sự phát triển của công nghệ bán dẫn và lý thuyết thông tin trong những năm 1980, CDMA đã được thương mại hóa từ phương pháp thu GPS và Ommi - TRACS, phương pháp này cũng đã được đề xuất trong hệ thống tổ ong của Qualcomm - Mỹ vào năm 1990.

Trong thông tin CDMA thì nhiều người sử dụng chung thời gian và tần số, mã PN với sự tương quan chéo thấp được ấn định cho mỗi người sử dụng. Người sử dụng truyền tín hiệu nhờ trải phổ tín hiệu truyền có sử dụng mã PN đã ấn định. Đầu thu tạo ra một dãy giả ngẫu nhiên như ở đầu phát và khôi phục lại tín hiệu dự định nhờ việc trải phổ ngược các tín hiệu đồng bộ thu được.

2.2.1.2. Thủ tục thu phát tín hiệu

+ Tín hiệu số liệu thoại (9,6 Kb/s) phía phát được mã hoá, lặp, chèn và được nhân với sóng mang fo và mã PN ở tốc độ 1,2288 Mb/s (9,6 Kb/s x 128).

+ Tín hiệu đã được điều chế đi qua một bộ lọc băng thông có độ rộng băng 1,25MHz sau đó phát xạ qua anten.

+ Ở đầu thu, sóng mang và mã PN của tín hiệu thu được từ anten được đưa đến bộ tương quan qua bộ lọc băng thông độ rộng băng 1,25 MHz và số liệu thoại mong muốn được tách ra để tái tạo lại số liệu thoại nhờ sử dụng bộ tách chèn và giải mã.

2.2.1.3. Các đặc điểm của CDMA

- **Tính đa dạng của phân tập**

Trong hệ thống điều chế băng hẹp như điều chế FM analog sử dụng trong hệ thống điện thoại tổ ong thế hệ đầu tiên thì tính đa đường tạo nên nhiều fading nghiêm trọng. Tính nghiêm trọng của vấn đề fading đa đường được giảm đi trong điều chế CDMA băng rộng vì các tín hiệu qua các đường khác nhau được thu nhận một cách độc lập.

Nhưng hiện tượng fading xảy ra một cách liên tục trong hệ thống này do fading đa đường không thể loại trừ hoàn toàn được vì với các hiện tượng

fading đa đường xảy ra liên tục đó thì bộ giải điều chế không thể xử lý tín hiệu thu một cách độc lập được.

Phân tập là một hình thức tốt để làm giảm fading, có 3 loại phân tập là theo thời gian, theo tần số và theo khoảng cách.

- **Công suất phát thấp**

Việc giảm tỷ số Eb/No (tương ứng với tỷ số tín hiệu/nhiễu) chấp nhận được không chỉ làm tăng dung lượng hệ thống mà còn làm giảm công suất phát yêu cầu để khắc phục tạp âm và giao thoa. Việc giảm này nghĩa là giảm công suất phát yêu cầu đối với máy di động. Nó làm giảm giá thành và cho phép hoạt động trong các vùng rộng lớn hơn với công suất thấp khi so với các hệ thống analog hoặc TDMA có công suất tương tự. Hơn nữa, việc giảm công suất phát yêu cầu sẽ làm tăng vùng phục vụ và làm giảm số lượng BTS yêu cầu khi so với các hệ thống khác.

- **Bảo mật cuộc gọi**

Hệ thống CDMA cung cấp chức năng bảo mật cuộc gọi mức độ cao và về cơ bản là tạo ra xuyên âm, việc sử dụng máy thu tìm kiếm và sử dụng bất hợp pháp kênh RF là khó khăn đối với hệ thống tổ ong số CDMA bởi vì tín hiệu CDMA đã được scrambing (trộn). Về cơ bản thì công nghệ CDMA cung cấp khả năng bảo mật cuộc gọi và các khả năng bảo vệ khác, tiêu chuẩn đề xuất gồm khả năng xác nhận và bảo mật cuộc gọi được định rõ trong EIA/TIA/IS-54-B. Có thể mã hoá kênh thoại số một cách dễ dàng nhờ sử dụng DES hoặc các công nghệ mã tiêu chuẩn khác.

- **Bộ mã - giải mã thoại và tôc độ số liệu biến đổi**

Bộ mã – giải mã thoại của hệ thống CDMA được thiết kế bởi các tốc độ biến đổi 8 Kb/s. Dịch vụ thoại 2 chiều của tốc độ số liệu biến đổi cung cấp thông tin thoại có sử dụng thuật toán mã – giải mã thoại tốc độ số liệu biến đổi động giữa BS và máy di động. Bộ mã – giải mã thoại phía phát lấy mẫu tín hiệu thoại để tạo ra các gói tín hiệu thoại được mã hóa dùng để truyền tới bộ mã – giải mã thoại phía thu. Bộ mã – giải mã thoại phía thu sẽ giải mã các gói tín hiệu thoại thu được thành các mẫu tín hiệu thoại.

Hai bộ mã – giải mã thoại thông tin với nhau ở 4 nấc tốc độ truyền dẫn là 9600 b/s, 4800 b/s, 2400 b/s,1200b/s, các tốc độ này được chọn theo điều

kiện hoạt động và theo bản tin hoặc số liệu. Thuật toán mã – giải mã thoại chấp nhận CELP (mã dự đoán tuyến tính thực tế). Thuật toán dùng cho hệ thống CDMA là QCELP.

Bộ mã – giải mã thoại biến đổi sử dụng ngưỡng tương thích để chọn tốc độ số liệu. Ngưỡng được điều khiển theo cường độ của tạp âm nền và tốc độ số liệu sẽ chỉ chuyển đổi thành tốc độ cao khi có tín hiệu thoại vào. Do đó, tạp âm nền bị triệt đi để tạo ra sự truyền dẫn thoại chất lượng cao trong môi trường tạp âm

- **Máy di động có chuyển vùng mềm**

Sau khi cuộc gọi được thiết lập thì máy di động tiếp tục tìm tín hiệu của BTS bên cạnh để so sánh cường độ tín hiệu của ô bên cạnh với cường độ tín hiệu của ô đang sử dụng. Nếu cường độ tín hiệu đạt đến một mức nhất định nào đó có nghĩa là máy di động đã di chuyển sang một vùng phục vụ của một BTS mới và trạng thái chuyển vùng mềm có thể bắt đầu. Máy di động chuyển một bản tin điều khiển tới MSC để thông báo về cường độ tín hiệu và số hiệu của BTS mới. Sau đó, MSC thiết lập một đường nối mới giữa máy di động và BTS mới và bắt đầu quá trình chuyển vùng mềm trong khi vẫn giữ đường kết nối ban đầu. Trong trường hợp máy di động đang trong một vùng chuyển đổi giữa hai BTS thì cuộc gọi được thực hiện bởi cả hai BTS sao cho chuyển vùng mềm có thể thực hiện được mà không có hiện tượng ping-pong giữa chúng. BTS ban đầu cắt đường kết nối cuộc gọi khi việc đấu nối cuộc gọi với BTS mới đã thực hiện thành công

- **Dung lượng**

Trong hệ thống CDMA thì một kênh băng tần rộng được sử dụng chung bởi tất cả các BTS.

Các tham số chính xác định dung lượng của hệ thống tổ ong số CDMA bao gồm: độ lợi xử lý, tỷ số Eb/No (bao gồm cả giới hạn fading yêu cầu), chu kỳ công suất thoại, hiệu quả tái sử dụng tần số và số lượng búp sóng của anten BTS. Hơn nữa, càng nhiều kênh thoại được cung cấp trong hệ thống CDMA có cùng một tỷ lệ cuộc gọi bị chặn và hiệu quả trung kế cũng tăng lên thì càng nhiều dịch vụ thuê bao được cung cấp trên một kênh.

- **Tách tín hiệu thoại**

Trong thông tin hai chiều song công tổng quát thì tỷ số chiếm dụng tải của tín hiệu thoại không lớn hơn khoảng 35%. Trong trường hợp không có tín hiệu thoại trong hệ thống TDMA và FDMA thì khó áp dụng yếu tố tích cực thoại vì trễ thời gian định vị lại kênh tiếp theo là quá dài. Nhưng do tốc độ truyền dẫn số liệu giảm nếu không có tín hiệu thoại trong hệ thống CDMA nên giao thoa ở người sử dụng khác giảm một cách đáng kể. Dung lượng hệ thống CDMA tăng khoảng 2 lần và suy giảm truyền dẫn trung bình của máy di động giảm khoảng 1/2 vì dung lượng được xác định theo mức giao thoa ở những người sử dụng khác.

- **Tái sử dụng tần số và vùng phủ sóng**

Tất cả các BTS đều tái sử dụng kênh băng rộng trong hệ thống CDMA. Giao thoa tổng ở tín hiệu máy di động thu được từ BTS và giao thoa tạo ra trong các máy di động của cùng một BTS và giao thoa tạo ra trong các máy di động của BTS bên cạnh. Nói cách khác, tín hiệu của mỗi một máy di động giao thoa với tín hiệu của tất cả các máy di động khác. Giao thoa tổng từ tất cả các máy di động bên cạnh bằng một nửa của giao thoa tổng từ các máy di động khác trong cùng một BTS. Hiệu quả tái sử dụng tần số của các BTS không định hướng là khoảng 65%, đó là giao thoa tổng từ các máy di động khác trong cùng một BTS với giao thoa từ tất cả các BTS

- **Giá trị Eb/No thấp (hay C/I) và chống lỗi**

Eb/No là tỷ số của năng lượng trên mỗi bit đối với mật độ phổ công suất tạp âm, đó là giá trị tiêu chuẩn để so sánh hiệu suất của phương pháp điều chế và mã hoá số.

Khái niệm Eb/No tương tự như tỷ số sóng mang tạp âm của phương pháp FM analog. Do độ rộng kênh băng tần rộng được sử dụng mà hệ thống CDMA cung cấp một hiệu suất và độ dư mã sửa sai cao. Nói cách khác thì độ rộng kênh bị giới hạn trong hệ thống điều chế số băng tần hẹp, chỉ các mã sửa sai có hiệu suất và độ dư thấp là được phép sử dụng sao cho giá trị Eb/No cao hơn giá trị mà CDMA yêu cầu. Mã sửa sai trước được sử dụng trong hệ thống CDMA cùng với giải điều chế số hiệu suất cao. Có thể tăng dung lượng và giảm công suất yêu cầu với máy phát nhờ giảm Eb/No.

- **Dung lượng mềm**

Hiện tại FCC (Uỷ ban thông tin liên bang của Mỹ) ấn định phổ tần 25 MHz cho hệ thống tổ ong, hệ thống này được phân bổ đồng đều cho 2 công ty viễn thông theo các vùng. Dải phổ này được phân phối lại giữa các ô để cho phép sử dụng lớn nhất là 57 kênh FM analog cho một BTS 3 - búp sóng. Do đó, thuê bao thứ 58 sẽ không được phép có cuộc gọi khi lưu lượng bị nghẽn. Khi đó thậm chí một kênh cũng không được phép thêm vào hệ thống này và dung lượng sẽ giảm khoảng 35% do trạng thái tắc cuộc gọi. Nói cách khác thì hệ thống CDMA có mối liên quan linh hoạt giữa số lượng người sử dụng và loại dịch vụ. Ví dụ, người sử dụng hệ thống có thể làm tăng tổng số kênh trong đa số thời gian liên tục đưa đến việc tăng lỗi bit. Chức năng đó có thể làm tránh được việc tắc cuộc gọi do tắc nghẽn kênh trong trạng thái chuyển vùng.

Trong hệ thống analog và hệ thống TDMA số thì cuộc gọi được ấn định đối với đường truyền luân phiên hoặc sự tắc cuộc gọi xảy ra trong trường hợp tắc nghẽn kênh trong trạng thái chuyển vùng. Nhưng trong hệ thống CDMA thì có thể thoả mãn cuộc gọi thêm vào nhờ việc tăng tỷ lệ lỗi bit cho tới khi cuộc gọi khác hoàn thành.

Cũng vậy, hệ thống CDMA sử dụng lớp dịch vụ để cung cấp dịch vụ chất lượng cao phụ thuộc vào giá thành dịch vụ và ấn định công suất (dung lượng) nhiều cho các thuê bao sử dụng dịch vụ lớp cao. Có thể cung cấp thứ tự ưu tiên cao hơn đối với dịch vụ chuyển vùng của người sử dụng lớp dịch vụ cao so với người sử dụng thông thường.

2.2.1.4. Ưu điểm của CDMA

- **Tăng dung lượng hệ thống, nâng cao chất lượng cuôc gọi**

Các hệ thống điện thoại cellular sử dụng công nghệ CDMA cung cấp âm thanh có chất lượng cao hơn và ít xảy ra rớt cuộc gọi hơn các hệ thống hoạt động hoạt động dựa trên những công nghệ khác. Có nhiều đặc tính tồn tại trong hệ thống CDMA đã tạo ra những khả năng đó:

+ Các phương pháp sửa lỗi tiên tiến làm tăng khả năng chính xác cho các khung nhận được.

+ Các bộ mã hóa tinh vi cho phép mã hóa tố độ cao và giảm tạp âm nền.

+ CDMA sử dụng ưu điểm của nhiều loại phân tập khác nhau để nâng cao chất lượng thoại:

- Phân tập tần số: Bảo bệ khỏi những ảnh hưởng của Phadinh nhanh.
- Phân tập không gian: Khi MS di chuyển giữa các ô làm chung tần số thì nó thực hiện chuyển giao mềm, thiết lập các kênh truy nhập với BTS mới trước khi cắt bỏ kênh cũ. Trong giai đoạn quá độ thì MS làm việc đồng thời với 2 BTS tương ứng với việc mạng làm việc phân tập theo không gian.
- Phân tập thời gian: Dùng cài xen và mã hóa
- Phân tập đường truyền: Sử dụng bộ thu Rake để khắc phục sự thu nhận một tín hiệu qua nhiều đường gây ra nhiễu giao thoa và nâng cao chất lượng âm thanh

- **Quá trình thiết kế được đơn giản hóa**

Tất cả thuê bao sử dụng chung một nhóm sóng mang CDMA, cùng chia sẻ một phổ tần với nhau. Hệ số sử dụng lại tần số bằng 1 là một yếu tố quan trọng đã làm cho dung lượng của CDMA lớn hơn nhiều AMPS và các công nghệ khác, đồng thời nó còn làm cho việc thiết kế hệ thống đơn giản, dễ hiểu hơn. Nhà khai thác sẽ không phải lập kế hoạch sử dụng tần số - một công việc hết sức phức tạp trong hệ thông tương tự và TDMA. Quan trọng hơn, kể cả việc điều chỉnh lại tần số để mở rộng cũng được loại bỏ. Nếu nhà khai thác muốn thêm một cell hay một kênh mới thì không cần thiết phải lập lại toàn bộ tần số của hệ thống.

- **Nâng cao tính bảo mật thông tin**

Thông tin trong CDMA được bảo mật rất cao, việc xâm nhập bất hợp pháp vào tín hiệu CDMA là cực kỳ khó. Đó là vì các khung thông tin đã số hóa được trải phổ trên một nền phổ rộng. Hơn thế nữa, trong tương lai CDMA có các kế hoạch mã hóa số mới để tạo ra các mức bảo mật và an toàn hơn nhiều.

- **Cải thiện vùng phủ sóng**

Một cell CDMA có vùng phủ sóng lớn hơn nhiều so với cell tương tự hay số khác vì CDMA sử dụng thiết bị thu có độ nhạy lớn hơn các kỹ thuật khác. Do đó, để phủ sóng một vùng địa lý như nhau thì số cell CDMA phải dùng sẽ ít hơn. Tùy thuộc vào yêu cầu tải của hệ thống và nhiễu giao thoa mà việc giảm số cell có thể tới 50% so với GSM.

- **Tăng thời gian sử dụng pin**

Do việc điều khiển công suất chính xác và các đặc tính khác của hệ thống, các máy mobile CDMA thường chỉ truyền công suất bằng một phần nhỏ công suất so với các máy tương tự và TDMA. Điều này cho phép các thuê bao tăng thời gian sử dụng pin của máy mobile.

- **Cung cấp dải thông theo yêu cầu**

Một kênh CDMA băng rộng cung cấp tài nguyên chung mà tất cả các mobile trong hệ thống cùng dùng chung, tùy theo ứng dụng là truyền thoại, dữ liệu, fax hay ứng dụng khác. Tại một thời điểm bất kỳ, phần dải thông không được sử dụng bởi mobile này thì có thể cung cấp cho một mobile khác. Điều này làm cho CDMA thực sự linh hoạt và được khai thác để tạo ra các khả năng mạnh hơn như dịch vụ dữ liệu tốc độ cao. Thêm vào đó, vì mobile hoàn toàn độc lập khi sử dụng "bandwidth pool" nên đặc trưng đó có thể dễ dàng cùng tồn tại trên một kênh CDMA.

2.2.1.5. Nhược điểm của CDMA

+ Khả năng roamming hạn chế

+ Giá thành thiết bị đầu cuối đắt hoặc người sử dụng phải mua thiết bị của nhà khai thác

2.2.2. Điều khiển công suất CDMA

Hệ thống CDMA cung cấp chức năng điều khiển công suất 2 chiều (từ BS đến máy di động và ngược lại) để cung cấp một hệ thống có dung lượng lưu lượng lớn, chất lượng dịch vụ cuộc gọi cao và các lợi ích khác. Mục đích của điều khiển công suất phát của máy di động là điều khiển công suất phát của máy di động sao cho tín hiệu phát của tất cả các máy di động trong cùng một vùng phục vụ có thể được thu với độ nhạy trung bình tại bộ thu của BS. Khi công suất phát của tất cả các máy di động trong vùng phục vụ được điều khiển như vậy thì tổng công suất thu được tại bộ thu của BS trở thành công suất thu trung bình của nhiều máy di động.

Bộ thu CDMA của BS chuyển tín hiệu CDMA thu được từ máy di động tương ứng thành thông tin số băng hẹp. Trong trường hợp này thì tín hiệu của các máy di động khác còn lại chỉ như là tín hiệu tạp âm của băng rộng. Thủ tục thu hẹp băng được gọi là độ lợi xử lý nhằm nâng cao tỷ số tín

hiệu/ giao thoa (db) từ giá trị tạp âm lên đến một mức đủ lớn để cho phép hoạt động được với lỗi bit chấp nhận được.

Một mong muốn là tối ưu các lợi ích của hệ thống CDMA bằng cách tăng số lượng các cuộc gọi đồng thời trong một băng tần cho trước. Dung lượng hệ thống là tối đa khi tín hiệu truyền của máy di động được thu bởi BS có tỷ số tín hiệu/giao thoa ở mức yêu cầu tối thiểu qua việc điều khiển công suất của máy di động.

Hoạt động của máy di động sẽ bị giảm chất lượng nếu tín hiệu của các máy di động mà BS thu được là quá yếu. Nếu các tín hiệu của các máy di động đủ khỏe thì hoạt động của các máy này sẽ được cải thiện nhưng giao thoa đối với các máy di động khác cùng sử dụng một kênh sẽ tăng lên làm cho chất lượng cuộc gọi của các thuê bao khác sẽ bị giảm nếu như dung lượng tối đa không giảm.

Một tiến bộ lớn hơn của việc điều khiển công suất trong hệ thống CDMA là làm giảm công suất phát trung bình. Trong đa số trường hợp thì môi trường truyền dẫn là thuận lợi đối với CDMA. Trong các hệ thống băng hẹp thì công suất phát cao luôn luôn được yêu cầu để khắc phục fading tạo ra theo thời gian. Trong hệ thống CDMA thì công suất trung bình có thể giảm bởi vì công suất yêu cầu chỉ phát đi khi có điều khiển công suất và công suất phát chỉ tăng khi có fading

2.2.3. Chuyển giao CDMA

2.2.3.1. Khái quát về chuyển giao trong các hệ thống thông tin di động

Ở các hệ thống thông tin di động tổ ong, chuyển giao xảy ra khi trạm di động đang làm các thủ tục thâm nhập mạng hoặc đang có cuộc gọi. Mục đích của chuyển giao là để đảm bảo chất lượng đường truyền khi một trạm di động rời xa trạm gốc đang phục vụ nó. Khi đó, nó phải chuyển lưu lượng sang một trạm gốc mới hay một kênh mới.

Chuyển giao là một phần cần thiết cho việc xử lý sự di động của người sử dụng đầu cuối. Nó đảm bảo tính liên tục của các dịch vụ vô tuyến khi người sử dụng di động di chuyển từ qua ranh giới các ô tế bào.

Trong các hệ thống tế bào thế hệ thứ nhất như AMPS, việc chuyển giao tương đối đơn giản. Sang hệ thống thông tin di động thế hệ 2 như GSM và PACS thì có nhiều cách đặc biệt hơn bao gồm các thuật toán chuyển giao

được kết hợp chặt chẽ trong các hệ thống này và trễ chuyển giao tiếp tục được giảm đi. Khi đưa ra công nghệ CDMA, một ý tưởng khác được đề nghị để cải thiện quá trình chuyển giao được gọi là chuyển giao mềm.

2.2.3.2. Các loại chuyển giao.

Chuyển giao cứng

Chuyển giao cứng được thực hiện khi cần chuyển lưu lượng sang một kênh tần số mới. Chuyển giao cứng thực hiện phương thức cắt trước khi nối. Ở chuyển giao này kết nối với kênh cũ bị cắt trước khi kết nối với kênh mới. Nhược điểm của chuyển giao này là có thể rớt cuộc gọi do chất lượng của kênh mới quá xấu trong khi kênh cũ đã cắt. Các sơ đồ chuyển giao cứng bao gồm:

+ Chuyển giao CDMA đến CDMA: Trạm di động chuyển dịch giữa các ô hay đoạn ô làm việc ở tần số CDMA khác nhau.

+ Chuyển giao cứng CDMA đến tương tự: Trạm di động chuyển kênh lưu lượng CDMA đến kênh tiếng tương tự.

Chuyển giao mềm

Chuyển giao mềm xảy ra khi MS tạo được kết nối mới rồi mới ngắt bỏ kết nối cũ. Có 2 trường hợp:

+ MS nằm trong vùng chồng lấn phủ sóng giữa 2 ô, làm việc trên 2 kênh với 2 BTS khác nhau thì 2 BTS này phải thông báo để có cùng mã PN. BSC chọn khung có tiếng nói tốt của 2 kênh.

+ MS nằm trong vùng chồng lấn của 3 ô. BSC chọn một trong ba kênh tiếng nói của 3 BTS

Chuyển giao mềm làm tăng độ tin cậy của truyền tin và không bị gián đoạn. Chuyển giao mềm chỉ có thể thực hiện ở hệ thống thông tin di động tổ ong CDMA vì ở đây sử dụng chung một kênh tần số nên trạm di động không cần thay đổi kênh tần số khi nó di chuyển vào vùng phục vụ mới.

Chuyển giao siêu mềm

Chuyển giao từ anten định hướng này sang anten định hướng khác của cùng trạm gốc.

Chuyển giao mềm mềm hơn

MS ở vùng chuyển giao của 2 dải quạt 1 ô và ô thứ hai, ở đây sẽ vừa lựa chọn theo mức cường độ trường, vừa lựa chọn theo không gian

2.2.4. Máy thu Rake

Phân tập là một kỹ thuật thông tin áp dụng trong các hệ thống nhiễu và pha đinh, chúng cho ta sự cải thiện kết nối vô tuyến với giá thành tương đối thấp. Khác với san bằng, phân tập không cần đòi hỏi một sự tập dượt trước. Hơn thế nữa, có rất nhiều cách để thực hiện phân tập, tất cả đều rất thực tế và cho sự cải thiện kết nối một cách đáng kể với giá thành phụ thêm ít.

Tín hiệu trải phổ không có khả năng chống phadinh vì các thành phần nhiều đường cùng mang thông tin về một tín hiệu được gửi đi và các thành phần này lại độc lập với nhau. Do vậy, nếu một trong các thành phần nhiều đường bị suy giảm do pha dinh thì các thành phần khác có thể không bị ảnh hưởng bởi phadinh để đưa ra quyết định về tín hiệu thu được. Máy thu CDMA sử dụng tín hiệu nhiều đường để thu phân tập được gọi là máy thu Rake.

2.2.5. Tổ chức kênh trong CDMA2000

kênh trong CDMA2000 được tổ chức thành hai loại kênh là kênh đường lên (hướng từ MS tới BTS) và kênh đường xuống (hướng từ BTS tới MS). Các kênh này lại được chia thành kênh vật lý và kênh logic.

2.2.5.1. Kênh vật lý

Ký hiệu tên kênh và chức năng của kênh vật lý được cho dưới bảng sau:

Bảng3: Bảng ký hiệu kênh và chức năng của kênh vật lý

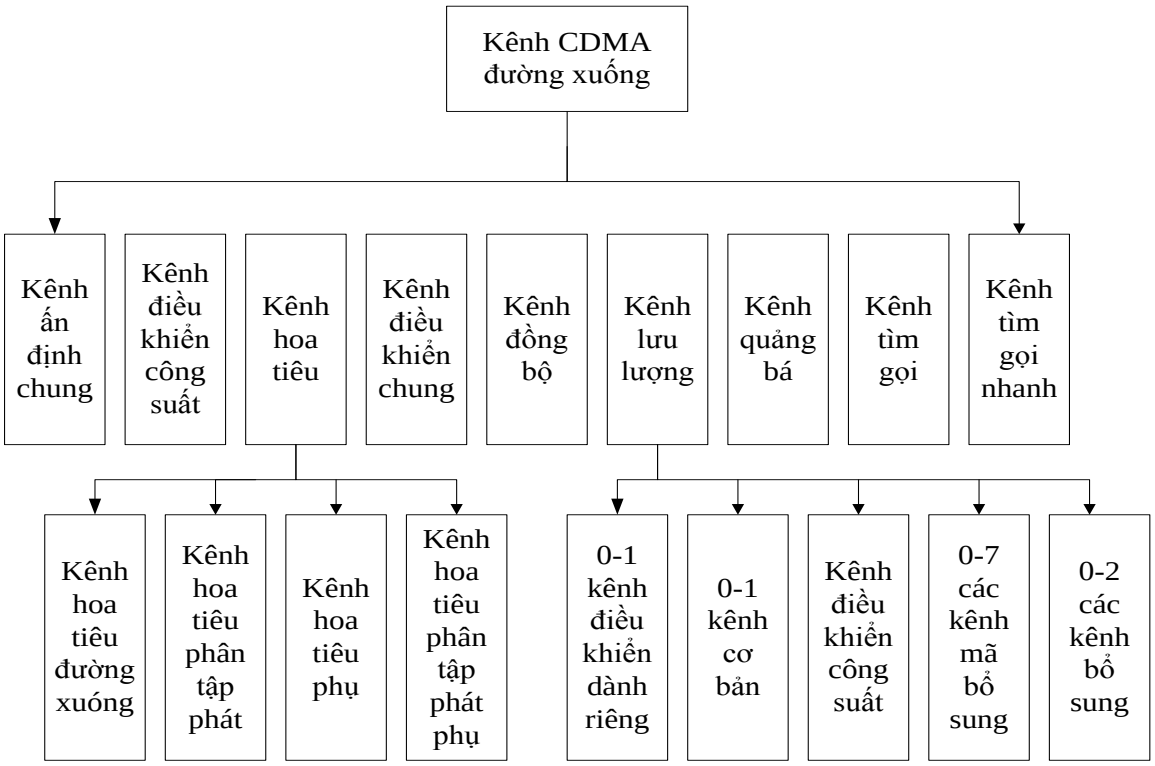
Tên kênh	Kênh vật lý
F/R-PICH	Kênh hoa tiêu đường xuống/lên (Forward/Reverse Pilot Channel)
F/SYNC	Kênh đồng bộ đường xuống (Forward Sync Channel)
F-TDPICH	Kênh phân tập phát đường xuống (Forward Transmit Diversyti Pilot Channel)
F-PCH	Kênh tìm gọi đường xuống (Forward Paging Channel)
F-BCCH	Kênh điều khiển quảng bá đường xuống (Foraward Broadcast Control Channel)
F-QPCH	Kênh tìm gọi nhanh đường xuống (Forward Quick Paging Channel)
F-CPCCH	Kênh điều khiển công suất chung đường xuống (Forward Common Power Control Channel)
F-CACH	Kênh ấn định chung đường xuống (Forward Common Assigment Channel)
F/R-CCCH	Kênh điều khiển chung đường xuống/lên (Forward/Reverse Common Control Channel)
F/R-DCCH	Kênh điều khiển riêng đường xuống /lên (Forward/Reverse Dedicated Control Channel)
F/R-FCH	Kênh cơ bản đường xuống lên (Forward/Reverse Fundamental Channel)
F/R-SCH	Kênh bổ xung đường xuống/lên (Forward/Reverse Supplemental Channel)
R-ACH	Kênh thâm nhập đường lên (Reverse Access Channel)
F-EACH	Kênh truy nhập tăng cường đường lên (Forward Enhanced Channel)
F-APICH	Kênh hoa tiêu phụ đường xuống (Forward Auxiliary Pilot Channel)
F-ATDPICH	Kênh hoa tiêu phân tập phát bổ xung đường xuống (Forward Auxiliary Transmit Diversyti Pilot Channel)
F/R-SCCH	Kênh bổ xung mã đường xuống/lên (Forward/Reverse Supplemental Code Channel)

Kênh vật lý hướng xuống

Từ cấu trúc trên ta thấy BS phát nhiều kênh chung cũng như một số kênh dành riêng cho thuê bao trong vùng phủ sóng của nó. Mỗi kênh CDMA được ấn định một kênh lưu lượng đường xuống như sau:

+ Kênh F-FCH
+ 0-7 kênh F-SCH cho cấu hình RC1 và RC2
+ 0-2 kênh F-SCH cho cấu hình RC1 đến RC3

Các kênh F-FCH được sử dụng cho thoại còn các kênh F-SCH được sử dụng cho kênh số liệu.



Hình 2.6. Các kênh vật lý đường xuống

- **Kênh hoa tiêu đường xuống F-PICH**

Kênh hoa tiêu được phát quảng bá liên tục bởi các trạm BS trên các kênh CDMA hướng xuống để cung cấp thông tin định thời và pha. Hoa tiêu chung là một tín hiệu không được điều chế trải phổ chuỗi trực tiếp bằng hàm Walsh. F-PICH được dùng chung cho tất cả các kênh lưu lượng và được sử dụng để:

+ Cung cấp pha chuẩn cho giải điều chế nhất quán tại máy thu MS

+ Phát hiện các tia đa đường để ấn định các ngón của RAKE đến đa đường mạnh nhất.

+ Bắt ô.

+ Cung cấp các phương tiện so sánh cường độ tín hiệu giữa các trạm gốc để chuyển giao.

Bằng kênh hoa tiêu chung có thể phát tín hiệu hoa tiêu mà không cần thông tin bổ sung cho người sử dụng. Hệ thống sử dụng hoa tiêu chung có thể đạt hiệu quả cao hơn hệ thống sử dụng hoa tiêu cho từng người. Đối với lưu lượng thoại, hoa tiêu chung có thể đảm bảo đánh giá kênh tốt hơn và cần ít thông tin bổ sung hơn, vì thế cải thiện chất lượng thu. Ngoài ra nó có thể đảm bảo tìm kiếm tốt hơn và hoạt động chuyển giao tốt hơn.

- **Kênh hoa tiêu phụ đường xuống F-APICH**

Là tín hiệu không được trải phổ chuẩn trực tiếp được phát liên tục từ BTS. F-APICH được sử dụng cho các ứng dụng tạo búp anten và búp hẹp. Các búp hẹp có thể sử dụng cho các ứng dụng phủ cho một vùng địa lý đặc iệt hoặc tăng dung lượng ở các vùng nóng.

- **Kênh hoa tiêu phân tập phát phụ đường xuống F-TDPICH**

Đây là một kênh liên kết với kênh hoa tiêu phụ F-APICH. Hai kênh này cung cấp chuẩn pha để tách sóng nhất quán các kênh CDMA đường xuống liên kết với kênh hoa tiêu phụ và thực hiện phân tập phát.

- **Kênh đồng bộ đường xuống F-SYNC**

Đây là một kênh mã được các MS trong vùng phủ sóng của BS sử dụng để bắt bản tin đồng bộ lúc đầu. Có hai kiểu kênh F-SYNC:

+ F-SYNC chia sẻ: Đảm bảo dịch vụ cho cả hai IS-95B và CDMA khi sử dụng F-SYNC ở kênh IS-95B bị chồng lấn. Chế độ này chỉ áp dụng cho hệ thống chồng lấn.

+ F-SYNC băng rộng: được điều chế trên toàn bộ băng rộng . F-SYNC được điều chế như một kênh riêng trong vật lý chung đường xuống. Chế độ này được áp dụng cho cả chế độ chồng lấn và không chồng lấn

- **Kênh tìm gọi đường xuống F-PCH**

Đây là một kênh mã ở đường xuống của kênh CDMA để phát thông tin điều khiển và các tìm gọi từ BS đến MS. Một BS của CDMA có thể có rất

nhiều kênh tìm gọi. Kênh tìm gọi được sử dụng để phát các thông tin điều khiển và các bản tin tìm gọi từ MS đến các máy di động và làm việc ở chế độ 9.6Kbps hay 4.8 Kbps (giống IS-95). F-PCH mang các bản tin bổ sung, công nhận, ấn định kênh, các yêu cầu trạng thái và cập nhật số liệu chia sẻ bảo mật SDD (Secret Shared Data) từ BS đến MS.

Có hai kiểu kênh tìm gọi là: F-PCH chia sẻ và F-PCH băng rộng. F-PCH chia sẻ đảm bảo dịch vụ cho cả hai IS-95 và CMDA khi sử dụng F-PCH ở kênh IS-95B bị chồng lấn. Chế độ này chỉ áp dụng cho các cấu hình chồng lấn.

- **Kênh tìm gọi nhanh F-QPCH**

Là một tín hiệu trải phổ được điều chế bật / tắt phát đi từ BTS để thông báo cho các MS trong chế độ chia khe ở trạng thái rỗi có xuất hiện kênh điều khiển chung đường xướng. F-QPCH cho phép tăng thời hạn acqui của MS bằng cách giảm thời gian phân tích các tìm gọi không dành cho nó. MS giám sát F-QPCH và khi cờ chỉ thị tìm gọi được lập, nó sẽ kiếm bản tin tìm gọi.

- **Kênh điều khiển chung đường xuống F-CCCH**

Là một kênh điều khiển được sử dụng để truy nhập thông tin điều khiển số từ BS đến một hay nhiều MS. F-CCCH truyền bản tin điều khiển lớp 3 và MAC từ BS đến MS như: 5ms, 10ms, 20ms phụ thuộc vào môi trường khai thác.

- **Kênh quảng bá chung đường xuống F-BCCH**

Đây là kênh tìm gọi dành riêng cho các bản tin điều khiển bổ sung và các bản tin quảng bá của SMS. Nhờ vậy, các bản tin bổ sung cho điều khiển của kênh tìm gọi được chuyển sang một kênh quảng bá riêng. Biện pháp này cải thiện thời gian khởi đầu MS và hiệu quả hoạt động truy nhập hệ thống. Ngoài ra, nhờ việc giảm số bản tin trên kênh F-PCH dung lượng tìm gọi tăng.

- **Kênh cơ bản đường xuống F-FCH**

Là một bộ phận của kênh lưu lượng đường xuống để mang tín hiệu ghép của số liệu tốc độ cao và thông tin điều khiển công suất. Mỗi kênh F-FCH được phát trên một kênh mã trực giao khác nhau và sử dụng kích cỡ khung tương ứng 20ms và 5ms.

- **Kênh bổ xung đường xuống F-SCH**

Được sử dụng cho các cuộc gọi dữ liệu tốc độ cao. Mỗi kênh lưu lượng đường F-TCH có thể chứa tới hai kênh F-SCH. Trạm BS sẽ phát thông tin dữ

liệu trên kênh F-SCH ở các tốc độ: 1200, 2400, 4800, 9600, 19200, 38400, 78600,153600bps. Trạm BS phát kênh F-SCH sử dụng chuỗi PN_I, PN_Q giống như trên kênh hoa tiêu F-PICH.

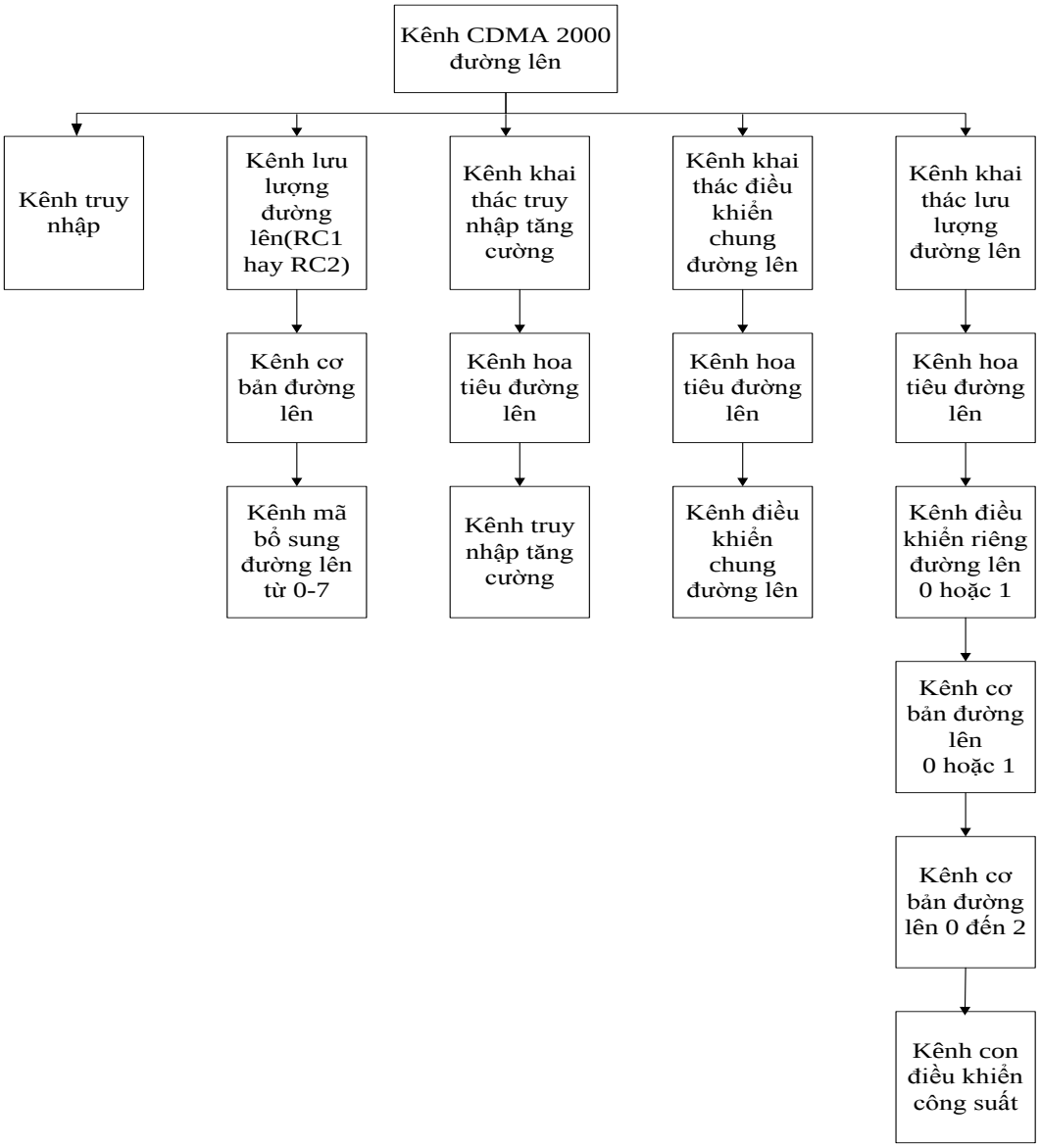
- **Kênh điều khiển riêng đường xuống F-DCCH**

Được sử dụng để truyền thông tin người sử dụng và báo hiệu trong quá trình thực hiện cuộc gọi. Mỗi kênh F-TCH có thể chứa một kênh F-DCCH. Trạm BS sẽ phát thông tin trên kênh F-DCCH ở tốc độ không đổi 9600bps với tốc độ dài khung là 20ms và sử dụng các chuỗi PN_I, PN_Q giống như kênh hoa tiêu F-PICH cho việc trải phổ tín hiệu.

Đặc điểm của kênh CDMA2000 đường xuống:

+ Truyền dẫn đơn và đa sóng mang
+ Phân tập phát
+ Điều chế trực giao

Kênh vật lý đường lên



Hình 2.7. Các kênh vật lý đường lên

Kênh truy nhập đường lên R-ACH

R-ACH được các MS sử dụng để liên lạc với BTS cho các bản tin báo hiệu ngắn như: Khởi đầu cuộc gọi, trả lời tìm gọi, đăng ký, R-ACH là các kênh truy nhập ngẫu nhiên được chia khe.

Kênh điều khiển chung đường lên R-CCCH

Là một bộ phận của kênh CDMA đường lên, được sử dụng để truyền thông tin điều khiển số từ một hay nhiều MS đến một BTS. R-CCCH có thể làm việc ở chế độ truy nhập dành trước hay truy nhập ấn định. Nó có thể hỗ trợ chuyển giao mềm trong chế độ truy nhập dành trước.

R-CCCH được sử dụng để truyền bản tin MAC lớp 3 từ MS đến BTS. R-CCCH khác R-ACH ở chỗ R-CCCH cung cấp nhiều khả năng hơn R-ACH.

Kênh hoa tiêu đường lên R-PICH

Là một tín hiệu không được điều chế trải phổ trực tiếp, được MS phát liên tục. R-PICH cung cấp chuẩn pha cho giải điều chế nhất quán ở BTS và có thể cung cấp phương tiện để đo cường độ tín hiệu. Kênh hoa tiêu cho các kênh riêng đường lên gồm: Một giá trị tham khảo cố định và thông tin điều khiển công suất đường xuống ghép chung. Thông tin điều khiển công suất ghép theo thời gian được gọi là kênh con điều khiển công suất.

Kênh con điều khiển công suất trên kênh R-PICH được MS sử dụng để điều khiển công suất BTS khi BTS này làm việc trên kênh lưu lượng đường xuống với cấu hình vô tuyến từ RC3 đến RC9. Kênh con này cung cấp thông tin về chất lượng đường xuống ở tốc độ 1 bit trên nhóm công suất điều khiển công suất PCG (Power Control Group). Sự lặp điều khiển công suất có nghĩa là giá trị bit này không thay đổi trong thời gian lặp ký hiệu. Bit điều khiển công suất sử dụng phần cuối cùng của mỗi nhóm PCG.

R-PICH được sử dụng để bắt đầu, bám thời gian, khôi phục chuẩn nhất quán cho máy thu Rake và đo công suất.

Kênh lưu lượng đường lên

Là kênh lưu lượng để truyền báo hiệu và số liệu từ MS đến BTS. Đối với cấu hình RC1 và RC2 kênh lưu lượng đường lên bao gồm một kênh R-FCH và đến 7 kênh R-SCH. Đối với cấu hình RC3 và RC6 kênh lưu lượng đường lên gồm một kênh R-FCH, một kênh R-DCCH hoặc cả hai và tới hai kênh R-SCH.

Kênh cơ bản đường lên R-FCH

Là một bộ phận của kênh lưu lượng để mang số liệu tốc độ cao và thông tin điều khiển từ MS đến BTS

R-FCH được truyền ở các tốc độ vô tuyến khác nhau cho cấu hình vô tuyến khác nhau.

Kênh bổ sung đường lên R-SCH

R-SCH sử dụng cho các cuộc gọi số liệu và có thể hoạt động ở các tốc độ bit khác nhau.

Kênh điều khiển riêng đường lên R-DCCH

Là một bộ phận của kênh lưu lượng đường lên được sử dụng để truyền số liệu mức cao và thông tin điều khiển từ MS đến BTS.

Phụ thuộc vào hoàn cảnh phục vụ, kênh R-DCCH, R-FH, R-SCH được sử dụng hoặc không sử dụng. Mỗi kênh vật lý được trải phổ bằng một chuỗi mã Waslh để đảm bảo phân kênh trực giao cho các kênh logic.

Kênh số liệu truy nhập tăng cường R-EACH

Số liệu ở chế truy nhập cơ sở hoặc chế độ truy nhập có điều khiển công suất được phát trên kênh R-EACH, còn chế độ ở chế độ truy nhập dành trước được phát trên kênh R-CCCH

Đặc điểm của kênh CDMA2000 đường lên:

+ Dạng sóng liên tục
+ Các kênh trực giao đối với các chuỗi Waslh độ dài khác nhau
+ Thích ứng tốc độ
+ Các búp trên phổ thấp
+ Các kênh số liệu độc lập
+ Điều khiển công suất đường lên
+ Kênh điều khiển riêng cách biệt
+ Độ dài khung.

2.2.5.2. Kênh logic.

Bao gồm kênh lưu lượng và kênh báo hiệu. Tên và chức năng của chúng như sau:

- **Kênh lưu lượng riêng F/R-DTCH**

DTCH là một kênh logic đường lên hoặc đường xuống được sử dụng để mang số liệu của người sử dụng.

- **Kênh lưu lượng chung F/R-CTCH**

CTCH là một kênh logic đường lên hoặc xuống được sử dụng để mang cụm số liệu ngắn liên quan đến dịch vụ số liệu.

- **Kênh MAC riêng F/R-CMCH-Control**

CMCH-Control là kênh logic đường lên hoặc xuống được sử dụng để mang các bản tin MAC: Mudium Access Control – điều khiển truy nhập môi trường.

- **Kênh MAC chung đường lên: R-CMCH-Control**

Đây là kênh logic đường lên được MS sử dụng và dịch vụ số liệu được truyền đến MS khi nó ở trạng thái chờ. Kênh logic này được sử dụng để mang các bản tin MAC và được chia sẻ cho một nhóm di động với ý nghĩa truy nhập đến kênh này.

- **Kênh MAC chung đường xuống F-CMCH-Control**

Kênh này được sử dụng bởi BTS ở dịch vụ số liệu trong trạng thái ngủ/rỗi.Kênh logic này được sử dụng để mang các bản tin MAC.

- **Kênh báo hiệu riêng DSCH**

Kênh này mang số liệu báo hiệu riêng cho các lớp cao cho một BS

- **Kênh báo hiệu chung CSCH**

Kênh này mang báo hiệu số liệu lớp cao với truy nhập chung cho nhiều MS

2.2.6. Kỹ thuật trải phổ và mã trải phổ

Kỹ thuật điều chế trải phổ này hay còn được gọi tắt là kỹ thuật trải phổ là một kỹ thuật thông tin vô tuyến dùng giải thông truyền dẫn lớn hơn gấp nhiều lần so với dải thông của thông tin hay tốc độ số liệu của một thuê bao bất kỳ. Một hệ thống ứng dụng kỹ thuật trải phổ được gọi là một hệ thống thông tin trải phổ nếu nó thỏa mãn đủ 3 yếu tố sau:

+ Tín hiệu sau trải phổ chiếm 1 độ rộng băng tần ruyền dẫn lớn hơn nhiều băng tần truyền dẫn tối thiểu cần thiết để truyền thông tin đi.

+ Trải phổ được thực hiện nhờ tín hiệu trải phổ và thường được gọi là mã trải phổ, mã trải phổ này được độc lập với dữ liệu.

+ Tại phía thu, việc nén phổ nhằm khôi phục lại tín hiệu ban đầu được thực hiện nhờ tương quan giữa tín hiệu thu được với bản sao đồng bộ mã trải phổ được sử dụng ở phía phát.

Tuy nhiên có một số kỹ thuật điều chế và giải điều chế sử dụng băng tần truyền dẫn lớn hơn độ rộng băng tối thiểu cần thiết để truyền dữ liệu ban đầu. Song không phải là điều chế trải phổ do không thỏa mãn cả 3 yêu cầu trên chẳng hạn như: điều tần, điều chễ xung mã dẫn tới tăng độ rộng băng truyền nhưng không thỏa mãn yêu cầu 1, 2 nên cũng ko phải là kỹ thuật trải phổ.

Các ưu điểm của hệ thống trải phổ:

Có 3 ưu điểm chính nổi bật là

Khả năng triệt nhiễu

Nhiễu là tín hiệu có hại tác động xấu đến tín hiệu mong muốn. Nhiễu có rất nhiều loại như nhiễu xung, nhiễu liên tục, nhiễu trắng, nhiễu cộng….trong đó có nhiễu tạp âm trắng có năng lượng phân bố đều khắp thang tần số nên năng lượng tổng cộng của nó là rất lớn. Tuy nhiên chỉ có các thành phần phổ nằm trong không gian phổ tín hiệu mới ảnh hưởng xấu tới chất lượng truyền dẫn do đó việc truyền dẫn vẫn đạt hiệu quả.

Đối với các loại nhiễu dải hẹp cùng lọt vào máy thu với tín hiệu có ích thì thông qua việc giải điều chế trải phổ tại nơi thu mà nó bị suy yếu đi. Điều này là do các tín hiệu nhiễu này tuy được thu cùng với tín hiệu có ích nhưng chúng ko có được sự tương quan cần thiết cho việc giải trải phổ. Do dó thông qua việc giải trải phổ, phổ của nhiễu sẽ bị trải ra và mật độ năng lượng cũng bị giảm đi nhiều. Trong khi đó phổ của tín hiệu có ích sau khi giải trải phổ mật độ sẽ được khôi phục

Đối với nhiễu công Gaussian thì hệ thống trải phổ không thể cải thiện được chất lượng truyền dẫn. Tạp âm trắng luôn tồn tại ngay cả khi đã trải phổ. Ngoài ra còn nhiễu cùng kênh do các MS sử dụng chung băng tần, tín hiệu của MS này lại là nhiễu đối với tín hiệu MS khác. Do có sự đồng bộ chính xác giữa các mã trải phổ phía phát và phía thu nên hệ thống có thể khắc phục được loại nhiễu này.

Để đối phó với nhiễu phá, hệ thống trải phổ không dùng toàn bộ các tọa độ trực giao có thể kết nối thông tin mà chỉ dùng một tập con trong đó. Nếu

tín hiệu có bề rộng phổ W, thời gian tồn tại là T thì số phân lượng phổ là 2WT. Một phân lượng phổ tương ứng với một ô vuông có một chiều dài là một đơn vị thời gian, và một chiều là đơn vị bề rộng phổ. Tín hiệu trải phổ có bề rộng càng lớn thì số tọa độ trực giao càng lớn và nhiễu phá càng khó có thể xác định được tập con nào đang được sử dụng để gây nhiễu.

Giảm được mật độ năng lượng

Trong hệ thống trải phổ, do tín hiệu trước khi truyền đi được trải phổ thành tín hiệu có phổ lớn hơn nhiều so với tín hiệu gốc cần truyền nên công suất trung bình của tín hiệu được trải đều và giảm nhỏ trên toàn bộ miền trải phổ. Với đặc điểm này thì hệ thống trải phổ có một ưu điểm rất lớn là: Tín hiệu truyền đi rất khó bị phát hiện do có mật độ thấp, tín hiệu truyền đi được chìm trong nền tạp âm, điều này làm cho các đối tượng khác khó có thể nghe trộm tín hiệu, đồng thời làm giảm can nhiễu cho các máy thu khác. Đây là cơ sở để xây dựng hệ thống thông tin có tính bảo mật cao.

Đa truy nhập theo mã CDMA

CDMA là phương thức đa truy nhập phân chia theo mã nhờ kỹ thuật trải phổ. Do hiệu quả nén tạp âm rất cao nên mỗi người sử dụng được chỉ định một mã trải phổ duy nhất (mỗi mã trải phổ tương ứng với một kênh thông tin độc lập) dễ dàng phân biệt với những người sử dụng khác cùng phát đi đồng thời và trong cùng một băng tần. Như vậy hệ thống CDMA có hiệu suất sử dụng băng tần rất cao và có dung lượng lớn.

Phương pháp trải phổ tín hiệu sử dụng mã trải phổ băng rộng điều chế tín hiệu sóng mang đã được điều chế bởi dữ liệu gọi là trải phổ dãy trực tiếp (DS/SS). Trong phương pháp này mã trải phổ trực tiếp tham gia vào quá trình điều chế, trong các phương pháp trải phổ khác mã trải phổ không trực tiếp tham gia vào quá trình điều chế mà sử dụng để điều chế như dùng để điều khiển tần số hay thời gian truyền dẫn tín hiệu sóng mang đã được điều chế bởi dữ liệu. Có hai kỹ thuật trải phổ dãy trực tiếp dùng trong CDMA 2000 là: DS-BPSK và DS-QPSK.

2.2.6.1. Trải phổ dãy tực tiếp sử dụng phương pháp điều chế BPSK

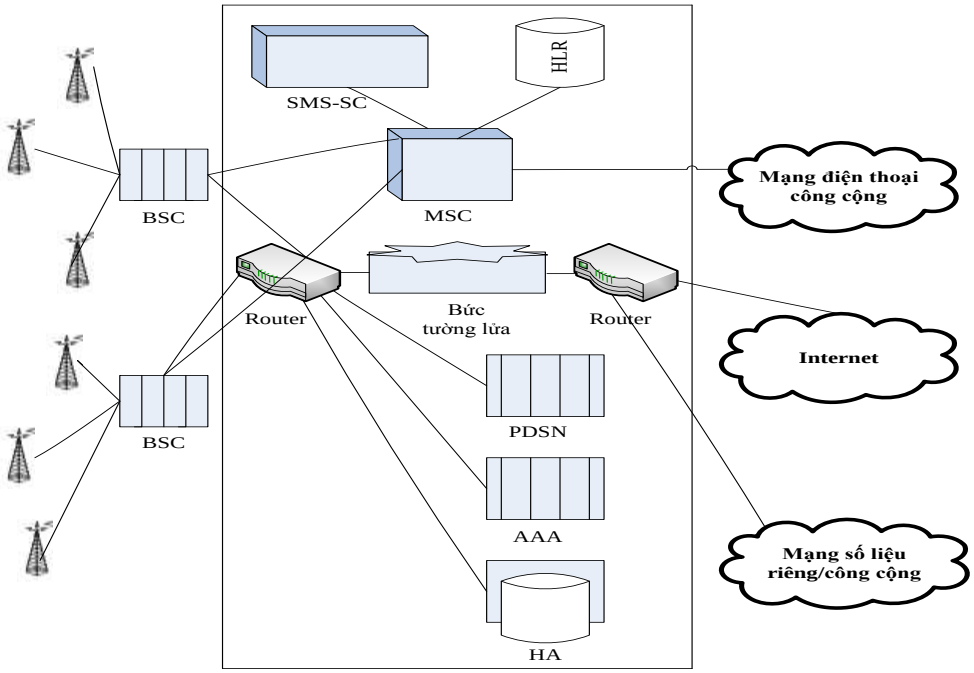
Phương pháp này sử dụng hai lần điều chế, lần điều chế thứ nhất điều chế dữ liệu theo phương pháp điều chế số thông thường, lần điều chế thứ hai sử dụng điều chế dịch pha nhị phân BPSK như ghép trải phổ, điều đó có nghĩa

là lần điều chế thứ hai người ta sử dụng mã trải phổ điều chế tín hiệu sóng mang đã được điều chế bởi tín hiệu (ở lần điều chế thứ nhất) theo kiểu BPSK.

2.2.6.2. Trải phổ dãy trực tiếp sử dụng phương pháp điều chế QPSK

Điều chế pha 4 mức QPSK sử dụng nguyên lý 2 bit thành một ký hiệu và được mô tả bằng một trạng thái pha của sóng mang, như thế với cùng một độ rộng băng truyền dẫn sử dụng phương pháp điều chế pha QPSK có tốc độ bit truyền dẫn đạt được gấp 2 lần so với trường hợp điều chế pha BPSK.

2.2.7. Kiến trúc mạng CDMA 2000



Hình 2.8. Sơ đồ kiến trúc mạng CDMA 2000

2.2.7.1. Nút phục vụ số liệu gói PDSN

PDSN (Packet Data Serving Node) là một phần tử mới liên quan đến hệ thống CDMA 2000. Đây là một phần tử quan trọng để xử lý các dịch vụ gói. PDSN có nhiệm vụ hỗ trợ các dịch vụ gói và thực hiện các chức năng sau:

+ Thiết lập, duy trì và kết cuối các phiên của giao thức điểm đến điểm (PPP: Point – to – Point Protocol)

+ Hỗ trợ các dịch vụ gói đơn giản và IP.

+ Thiết lập, duy trì và kết thúc các liên kết logic với mạng vô tuyến (RN) và giao diện vô tuyến gói (R-P)

+ Khởi đầu, nhận thực, trao quyền và thanh toán (AAA) đến AAA Server cho khách hàng di động.

+ Tiếp nhận các thông số dịch vụ từ AAA Server cho khách hàng di động.

+ Định tuyến các gói đến và từ các mạng số liệu ngoài.

+ Thu thập số liệu sử dụng để chuyển đến AAA. Tổng dung lượng của PDSN được xác định bằng thông lượng và số phiên PPP được phục vụ. Cần lưu ý rằng dung lượng chỉ là một khía cạnh của quá trình định cỡ và cần phải lưu ý đến yếu tố tin cậy của toàn mạng trong quá trình định cỡ.

2. 2.7.2. Nhận thực, Trao quyền và Thanh toán (AAA)

AAA Server là một phần tử mới liên quan đến CDMA 2000. AAA cung cấp chức năng nhận thực, trao quyền và thanh toán cho mạng số liệu gói của CDMA 2000 và sử dụng giao thức RADIUS (Remote Access Dial-In User Service). AAA chỉ liên lạc với PDSN qua mạng IP và thực hiện chức năng chính ở mạng CDMA 2000 như sau:

+ Nhận thực liên quan đến kết nối PPP và MIP
+ Trao quyền (lý lịch dịch vụ, phân phối khóa bảo an và quản lý)
+ Thanh toán

2.2.7.3. Tác nhân nhà HA

HA là phần tử chính thứ ba của mạng dịch vụ gói trong hệ thống CDMA 2000, nó tuân theo tiêu chuẩn IS-853. HA thực hiện nhiều nhiệm vụ liên quan đến theo dõi vị trí của thuê bao MIP khi thuê bao này chuyển động từ một vùng chuyển mạch gói này đến vùng chuyển mạch gói khác. Trong quá trình theo dõi máy di động, HA đảm bảo rằng các gói được chuyển đúng đến máy di động.

2.2.7.4. Router

Router có chức năng định tuyến các gói đến và từ các phần tử mạng khác nhau trong hệ thống CDMA 2000. Router cũng có nhiệm vụ gửi và nhận các gói đến và từ các mạng khác.

Bức tường lửa để duy trì bảo mật khi nối với các ứng dụng số liệu của mạng khác.

2.2.7.5. Bộ ghi định vị thường trú HLR

HLR để lưu giữ thông tin thuê bao giống như ở thế hệ 2, ngoài ra nó cũng lưu giữ thông tin liên quan đến việc đưa vào các dịch vụ gói. HLR thực hiện nhiệm vụ đối với dịch vụ gói cũng giống như đối với các dịch vụ thoại. Nó lưu giữ các tùy chọn dịch vụ số liệu gói và các khả năng của đầu cuối cùng với các thông tin về dịch vụ thoại. Thông tin dịch vụ được HLR nạp xuống bộ ghi định vị tạm trú VLR của MSC liên quan trong quá trình đăng ký thành công.

2.2.7.6. Trạm thu phát gốc BTS

BTS chịu trách nhiệm các tài nguyên gồm tần số, công suất và mã định kênh (Walsh) cho thuê bao. BTS chứa các thiết bị vô tuyến để phát và thu các tín hiệu CDMA 2000. BTS giao diện với mạng CDMA 2000 và thiết bị của người sử dụng UE. BTS điều khiển tính năng của hệ thống liên quan đến hoạt động của mạng.

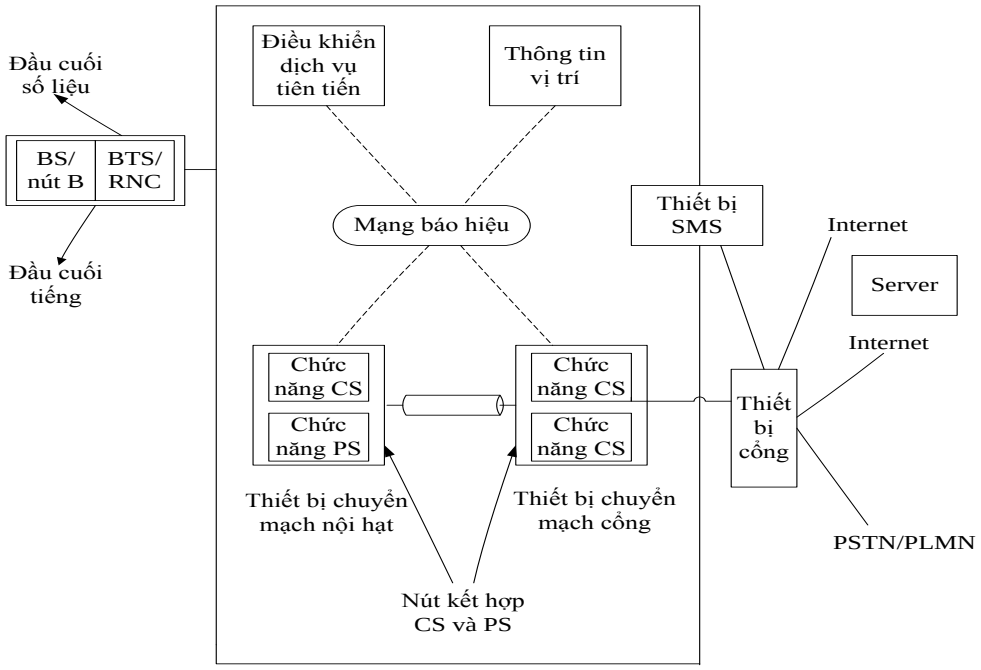
2.2.7.7. Bộ điều khiển trạm gốc BSC.

BSC chịu trách nhiệm điều khiển toàn bộ các BTS trong vùng quản lý của mình. BSC định tuyến các gói đến và từ PDSN. Ngoài ra, BSC định tuyến lưu lượng ghép kênh theo thời gian đến chuyển mạch kênh MSC.

2.3. KIẾN TRÚC TỔNG QUÁT MẠNG 3G

Mạng thông tin di động 3G lúc đầu sẽ là mạng kết hợp giữa các vùng chuyển mạch gói (PS) và chuyển mạch kênh (CS) để truyền số liệu gói và tiếng.

Các trung tâm chuyển mạch gói sẽ là các chuyển mạch sử dụng công nghệ ATM. Trên đường phát triển đến mạng toàn IP, chuyển mạch kênh sẽ dần được thay thế bằng chuyển mạch gói. Các dịch vụ kể cả số liệu lẫn thời gian thực (như tiếng và video) cuối cùng sẽ được truyền đi trên cùng một môi trường IP bằng các chuyển mạch gói. Hình vẽ dưới đây là kiến trúc tổng quát của mạng 3G kết hợp cả CS và PS trong mạng lõi.



Hình 2.9. Cấu trúc chung mạng3G

Các miền chuyển mạch kênh (CS) và chuyển mạch gói (PS) được thể hiện bằng một nhóm các đơn vị chức năng logic: trong thực tế các miền chức năng này được đặt vào các thiết bị và các nút vật lý. Chẳng hạn có thể thực hiện chức năng chuyển mạch kênh CS (MSC/GMSC) và chức năng chuyển mạch gói (SGSN/GGSN) trong một nút duy nhất để được một hệ thống tích hợp cho phép chuyển mạch và truyền dẫn các kiểu phương tiện khác nhau: từ lưu lượng tiếng đến lưu lượng số liệu dung lượng lớn.

Chương 3.
BẢO MẬT TRONG CÔNG NGHỆ 3G

3.1. AN NINH TRONG THÔNG TIN DI ĐỘNG

3.1.1. Tạo lập môi trường an ninh

An ninh đầu cuối là sự đảm bảo cho truyền dẫn số liệu được an toàn, nguyên vẹn trên toàn bộ đường truyền từ đầu phát đến đầu thu. Để đảm bảo được điều này, ta cần xét đến toàn bộ môi trường truyền thông. Nó bao gồm truy nhập mạng; các phần tử trung gian và các ứng dụng máy khách. Có năm mục tiêu quan trọng và liên quan đến việc tạo lập môi trường an ninh:

3.1.1.1. Nhận thực

Nhận thực là quá trình kiểm tra tính hợp lệ của các đối tượng tham gia thông tin trong các mạng không dây. Quá trình này được thực hiện tại hai lớp: lớp mạng và lớp ứng dụng. Lớp mạng đòi hỏi người sử dụng phải được nhận thực, trước khi được phép truy nhập. Lớp ứng dụng nhận thực quan trọng tại hai mức máy khách (Client) và máy chủ (Server). Để được truy nhập mạng Client phải chứng tỏ với Server rằng bản tin của nó phải hợp lệ. Đồng thời trước khi Client cho phép một Server nối đến nó, Server phải tự mình nhận thực với ứng dụng Client. Cách nhận thực đơn giản nhất kém an toàn là sử dụng Username và Password. Một số phương pháp tiên tiến hơn là sử dụng chứng nhận số (chữ ký điện tử).

3.1.1.2. Toàn vẹn số liệu

Toàn vẹn số liệu là sự đảm bảo số liệu truyền thông không bị thay đổi hay phá hoại trong quá trình truyền từ nơi phát đến nơi thu. Bằng cách áp dụng một giải thuật cho bản tin, một mã nhận thực bản tin MAC (MAC: Message Authentication Codes) được gõ bở người sử dụng của một may tính cho các tài khoản truy cập hoặc cổng thông tin. Mã này được đính kèm vào tin nhắn hoặc yêu cầu gửi của người dùng. Nếu chúng giống nhau thì chứng tỏ bản tin gốc không bị thay đổi, nếu nó khác nhau thì phía thu sẽ loại bỏ bản tin này.MAC thường được sử dụng trong các quỹ giao dịch chuyển điện tử (EFTs) để duyu trì tính toàn vẹn thông tin.

3.1.1.3. Bảo mật

Bảo mật là một khía cạnh rất quan trọng của an ninh và vì thế thường được nói đến nhiều nhất. Mục đích của nó là để đảm bảo tính riêng tư của số liệu làm cho dữ liệu không thể đọc được bởi bát cứ ai, ngoại trừ những ai được cho phép đọc. Cách phổ biến nhất được sử dụng là mật mã hóa số liệu. Quá trình này bao gồm mã hóa bản tin vào dạng không đọc được đối với bất kỳ máy thu nào, ngoại trừ máy thu chủ định.

3.1.1.4. Trao quyền

Trao quyền là quá trình quy định mức độ truy nhập của người sử dụng, người sử dụng được quyền thực hiện một số hành động. Trao quyền liên quan mật thiết với nhận thực. Một khi người sử dụng đã được nhận thực, hệ thống có thể quyết định người sử dụng được làm gì. Dành sách điều khiển truy cập ACL thường được sử dụng cho quá trình này, đối với một hệ thống tập tin máy tính, là một danh sách các quyền gắn liền với một đối tượng. ACL quy định cụ thể mà người dùng hay các quy trình hệ thống được cấp quyền truy cập vào các đối tượng, cũng những gì được phép hoạt động trên các đối tượng nhất định. Mỗi mục trong một ACL điển hình quy định cụ thể một chủ đề và hoạt động một. Ví dụ, một người sử dụng chỉ có thể truy nhập để đọc một tập tin số liệu. Trong khi đó nhà quản lý hoặc một nguồn tin cậy khác có thể truy nhập để viết, sửa chữa tập tin số liệu đó.

3.1.1.5. Cấm từ chối

Cấm từ chối là biện pháp buộc các phía phải chịu trách nhiệm về giao dịch mà chúng đã tham gia, không được phép từ chối tham gia giao dịch. Điều này có nghĩa là cả bên phát và bên thu đều có thể chứng minh răng phía đã phát bản tin, phía thu đã thu được bản tin tương tự. Để thực hiện quá trình này, mỗi giao dịch phải được ký bằng một chữ ký điện tử và được phía thứ ba tin cậy kiểm tra và đánh dấu thời gian.

3.1.2. Các đe dọa an ninh

Muốn đưa ra các giải pháp an ninh, trước hết ta cần nhận biết các đe dọa tiềm ẩn có nguy hại đến an ninh của hện thống thông tin. Sau đây là các đe dọa an ninh.

3.1.2.1. Đóng giả

Là ý định cảu kẻ truy nhập trái phép vào một ứng dụng hoặc một hệ thống bằng cách đóng giả người khác. Nếu kẻ đóng giả truy hập thành công, họ có thể tạo ra các câu trả lời giả dối với các bản tin để đạt được hiểu biết sâu hơn và truy nhập vào các bộ phận khác của hệ thống. Đóng giả là vấn đề chính đối với an ninh Internet và vô tuyến Internet, kẻ đóng giả có thể làm cho người sử dụng chính thông tin rằng mình đang thông tin với một nguôn tin cậy. Điều này vô cùng nguy hiểm, vì thế người sử dụng này có thể cung cấp thông tin bổ sung có lợi cho kẻ tấn công để chúng có thể truy nhập thành công các bộ phận khác của hệ thống.

3.1.2.2. Giám sát

Mục đích của giám sát là theo dõi, giám sát dòng số liệu trên mạng. Trong khi giám sát có thể được sử dụng cho các mục đích đúng đắn, thì nó lại thường được sử dụng để sao chép trái phép số liệu mạng. Thực chất giám sát là nghe trộm điện tử, bằng cách này kẻ không được phép truy nhập có thể lấy được các thông tin nhậy cảm gây hại cho người sử dụng, các ứng dụng và các hệ thống. Giám sát thường được sử dụng kết hợp với đóng giả. Giám sát rất nguy hiểm vì nó dễ thực hiện nhưng khó phát hiện. Để chống lại các công cụ giám sát tinh vi, mật mã hóa số liệu là phương pháp hữu hiêu nhất. Dù kẻ sử dụng trái phép có truy nhập thành công vào số liệu đã được mật mã nhưng cũng không thể giải mật mã được số liệu này. Vì vậy, ta cần đảm bảo rằng giao thức mật mã được sử dụng hầu như không thể bị phá vỡ.

3.1.2.3. Làm giả

Làm giả số liệu hay còn gọi là đe dọa tính toàn vẹn liên quan đến việc thay đổi số liệu so với dạng ban đầu với ý đồ xấu. Quá trình này liên quan đến cả chặn truyền số liệu lẫn các số liệu được lưu trên các Server hay Client. Số liệu bị làm giả (thay đổi) sau đó được truyền đi như bản gốc. Áp dụng mật mã hóa, nhận thực và trao quyền là các cách hữu hiệu để chống lại sự làm giả số liệu.

3.1.2.4. Ăn cắp

Ăn cắp thiết bị là vấn đề thường xảy ra đối với thông tin di động. Ta không chỉ mất thiết bị mà còn mất cả thông tin bí mật lưu trong đó. Điều này đặc biệt nghiêm trọng đối với các Client thông minh, vì chúng thường chứa số

liệu không đổi và bí mật. tính toán của các thiết bị di động khác có chứa ít nhất một số dữ liệu kinh doanh, chẳng hạn như danh sách liên lạc, mật khẩu tài khoản, mật e-mail và file đính kèm.. Một 2005 Nokia nghiên cứu cho thấy 21% nhân viên Mỹ thực hiện PDA và 63% mang theo điện thoại di động sử dụng cho kinh doanh.. Trong khi những thiết bị này đang ngày càng được kết nối tốt, họ là phần lớn không có bảo đảm và có thể gây ra rủi ro đáng kể cho mạng lưới kinh doanh và dữ liệu.Giảm được rủi ro đó bắt đầu với việc thành lập một chính sách an ninh thông tin rằng thỏa thuận với cả hai nhân viên mua và công ty sở hữu các thiết bị di động. Vì thế, ta cần tuân thủ theo các quy tắc sau để đảm bảo an ninh đối với các thiết bị di động:

+ Khóa thiết bị bằng Usernam và Password để chống lại truy nhập dễ dàng

+ Yêu cầu nhận thực khi truy nhập đến các ứng dụng lưu trong thiết bị

+ Tuyệt đối không lưu mật khẩu trên thiết bị

+ Mật mã tất cả các phương tiện lưu số liệu cố định

+ Áp dụng các chính sách an ninh đối với những người sử dụng di động Nhận thực, mật mã và các chính sách an ninh là các biện pháp để ngăn chặn việc truy nhập trái phép số liệu từ các thiết bị di động bị mất hoặc bị lấy cắp.

3.1.3. Các công nghệ an ninh

3.1.3.1. Công nghệ mật mã

Mục đích chính của mật mã là đảm bảo thông tin giữa hai đối tượng trên kênh thông tin khong an ninh, để đối tượng thứ ba không thể hiểu được thông tin được truyền là gì. Thoạt nhìn có vẻ mật mã là khái niệm đơn giản, nhưng thực chất nó rất phức tạp, nhất là với các mạng di động băng rộng như 3G UMTS

Các giải pháp và giao thức

Công nghệ mật mã hoạt động trên nhiều mức, mức thấp nhất là các giải thuật mật mã. Các giải thuật mật mã trình bày các bước cần thiết để thực hiện một tính toán, thường là chuyển đổi số liệu từ một khuôn dạng này vào khuôn dạng khác. Giao thức lại được xây dựng trên giải thuật này, giao thức mô tả

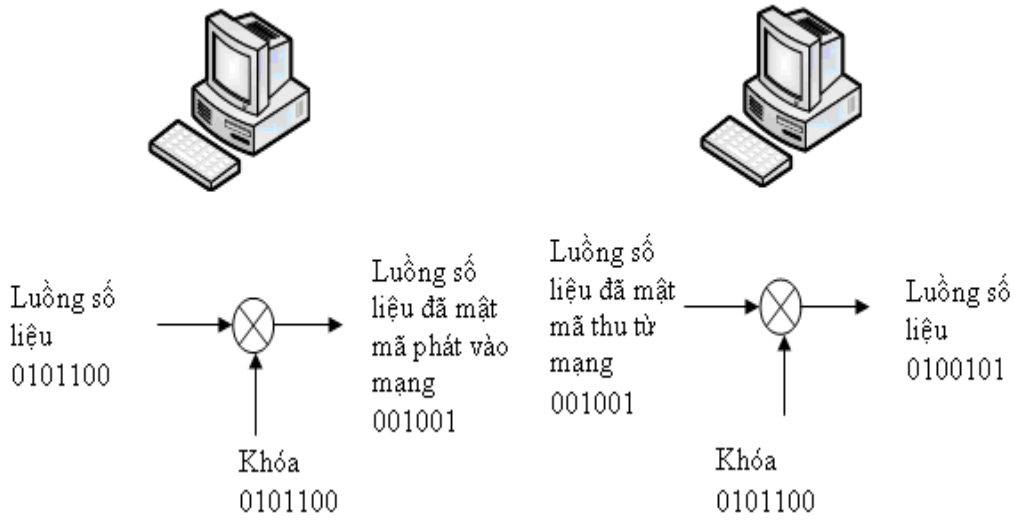
toàn bộ quá trình thực hiện các hoạt động của công nghệ mật mã. Một giải thuật mật mã tuyệt hảo không nhất thiết được coi là giao thức mạnh. Giao thức chịu trách nhiệm cho cả mật mã số liệu lẫn truyền số liệu và trao đổi khóa. Đỉnh của giao thức là ứng dụng, một giao thức mạnh chưa thể đảm bảo an ninh vững chắc. Vì bản thân ứng dụng có thể dẫn đến vấn đề khác, vì thế để tạo ra một giải pháp an ninh cần một giao thức mạnh cũng như thực hiện ứng dụng bền chắc.

Mật mã hóa số liệu

Nền tảng của mọi hệ thống mật mã là mật mã hóa. Quá trình này được thực hiện như sau: tập số liệu thông thường (văn bản thô) được biến đổi về dạng không thể đọc được (văn bản đã mật mã). Mật mã cho phép ta đảm bảo tính riêng tư của số liệu nhạy cảm, ngay cả khi những kẻ không được phép truy nhập thành công vào mạng. Cách duy nhất có thể đọc được số liệu là giải mật mã. Các giải thuật hiện đại sử dụng các khóa để điều khiển mật mã và giải mật mã số liệu. Một khi bản tin đã được mật mã, người sử dụng tại đầu thu có thể dùng mã tương ứng để giải mật mã, các giải thuật sử dụng khóa mật mã gồm hai loại: Đối xứng và bất đối xứng.

3.1.3.2. Các giải thuật đối xứng

Các giải thuật đối xứng sử dụng khóa duy nhất cho cả mật mã hóa lẫn giải mật mã hóa tất cả các bản tin. Phía phát sử dụng khóa để mật mã hóa bản tin, sau đó gửi nó đến phía thu xác định. Sau khi nhận được bản tin phía thu sử dụng chính khóa này để giải mật mã. Giải thuật này chỉ làm việc tốt khi có cách an toàn để trao đổi khóa giữa bên phát và bên thu. Rất tiếc là phần lớn vấn đề xảy ra khi trao đổi khóa giữa hai bên. Trao đổi khóa là một vấn đề mà bản thân mật mã hóa đối xứng không thể tự giải quyết được, nếu không có phương pháp trao đổi khóa an toàn. Mật mã hóa đối xứng còn được gọi là mật mã hóa bằng khóa bí mật, dạng phổ biến nhất của phương pháp này là tiêu chuẩn mật mã hóa số liệu (DES) được phát triển từ những năm 1970. Từ đó đến nay, nhiều dạng mật mã hóa đối xứng an ninh đã được phát triển, đứng đầu trong số chúng là tiêu chuẩn mật mã hóa tiên tiến (AES) dựa trên giải thuật Rijindael, DES 3 lần, giải thuật mật mã hóa số liệu quốc tế (IDEA), Blowfish và họ các giải thuật của Rivert (RC2, RC4, RC5, RC6). Để giải thích mật mã hóa đối xứng ta xét quá trình mật mã cơ sở sau:



Hình 3.1. Minh họa cơ chế cơ sở của mật mã bằng khóa duy nhất.

Luồng số liệu (văn bản thô) sử dụng khóa riêng duy nhất (một luồng số liệu khác) thực hiện phép tính cộng để tạo ra luồng số liệu thứ ba (văn bản đã được mật mã). Sau đó văn bản này được gửi qua kênh thông tin để đến bên thu. Sau khi thu được bản tin, phía thu sử dụng khóa chia sẻ (giống khóa bên phát) để giải mật mã (biến đổi ngược) và được văn bản gốc. Phương pháp trên có một số nhược điểm: trước hết không thực tế khi khóa phải có độ dài bằng độ dài số liệu, mặc dù khóa càng dài càng cho tính an ninh cao và càng khó mở khóa. Thông thường các khóa ngắn được sử dụng (64 hoặc 128bit) và chúng được lặp lại nhiều lần cho số liệu. Các phép toán phức tạp hơn có thể được sử dụng vì phép cộng không đủ để đảm bảo. Tiêu chuẩn mật mã hóa số liệu (DES) thường được sử dụng, mặc dù không phải là đảm bảo nhất. Nhược điểm thứ hai là phía phát và phía thu đều sử dụng một khóa chung (khóa chia sẻ). Vậy làm thế nào để gửi khóa này một cách an toàn từ phía phát đến phía thu. Phải chăng điều này có nghĩa rằng cấu tạo ra một khóa riêng duy nhất và chuyển đến đối tác cần thông tin? Phần mật mã hóa khóa công khai sẽ trả lời cho cầu hỏi này.

3.1.3.3. Các giải thuật bất đối xứng

Các giải thuật bất đối xứng giải quyết vấn đề chính xảy ra đối với các hệ thống khóa đối xứng. Năm 1975, Whitfield Diffie và Martin Hellman đã phát triển một giải pháp, trong đó hai khóa liên quan với nhau được sử dụng, một được sử dụng để mật mã hóa (khóa công khai) và một được sử dụng để giải mật mã hóa (khóa riêng). Khóa thứ nhất được phân phối rộng rãi trên các đường truyền không an ninh cho mục đích sử dụng công khai. Khóa thứ hai không bao giờ được truyền trên mạng và nó chỉ được sử dụng bởi phía đối tác cần giải mật mã số liệu. Hai khóa này liên hệ với nhau một cách phức tạp bằng cách sử dụng rất nhiều số nguyên tố và các hàm một chiều. Kỹ thuật này dẫn đến không thể tính toán được khóa riêng dựa trên khóa công khai. Khóa càng dài thì càng khó phá vỡ hệ thống. Các hệ thống khóa 64bit như DES, có thể bị tấn công rễ ràng bằng cách tìm từng tổ hợp khóa đơn cho đến khi tìm được khóa đúng. Các hệ thống khóa 128bit phổ biến hơn (ví dụ ECC đã được chứng nhận là không thể bị tấn công bằng cách thức như trên).

Khóa riêng và khóa công khai được tạo lập bởi cùng một giải thuật (giải thuật thông dụng là RSA_ giải thuật mật mã của 3 đồng tác giả Ron Rivest, Adi Shamir và Leonard Adelman). Người sử dụng giữ khóa riêng của mình và đưa ra khóa công khai cho mọi người, khóa riêng không được chia sẻ cho một người nào khác hoặc truyền trên mạng. Có thể sử dụng khóa công khai để mật mã hóa số liệu, nhưng nếu không biết khóa riêng thì không thể giải mật mã số liệu được. Sở dĩ như vậy là các phép toán được sử dụng trong kiểu mật mã này không đối xứng. Nếu User A muốn gửi số liệu được bảo vệ đến User B, User A sử dụng khóa công khai của User B để mật mã hóa số liệu và yên tâm rằng chỉ có User B mới có thể giải mật mã và đọc được số liệu này.

Các kỹ thuật mật mã khóa riêng và khóa công khai là các công cụ chính để giải quyết các vấn đề an ninh. Tuy nhiên, chúng không phải là các giải pháp đầy đủ, cần nhận thực để chứng minh rằng nhận dạng là của các người sử dụng chân thật. Phần dưới sẽ xét cách có thể sử dụng mật mã để giải quyết một số vấn đề an ninh cơ sở.

Cũng có thể mật mã bản tin bằng khóa riêng và giải mật mã bằng khóa công khai, nhưng để cho mục đích khác. Cách này có thể được sử dụng cho

các số liệu không nhậy cảm để chứng minh rằng phía mật mã đã thật sự truy nhập vào khóa riêng.

Giải thuật khóa bất đối xứng nổi tiếng đầu tiên được đưa ra bởi Ron Rivest, Adishamir và Leonard Adelman vào năm 1977 với tên gọi là RSA. Các giải thuật phổ biến khác bao gồm ECC và DH. RSA bị thất thế trong môi trường di động do ECC rẻ tiền hơn xét về công suất xử lý và kích thước khóa.

Tuy nhiên, đây chưa phải là các giải pháp hoàn hảo, chọn một khóa riêng không phải là việc dễ, nếu chọn không cẩn thận sẽ dễ dàng bị phá vỡ. Ngoài ra, các bộ mật mã hóa bất đối xứng cung cấp các giải pháp cho vấn đề phân phối khóa bằng cách sử dụng khóa công khai và khóa riêng. Do phức tạp hơn nên tính toán chậm hơn các bộ mật mã đối xứng. Đối với các tập số liệu lớn, đó sẽ là vấn đề không nhỏ. Trong các trường hợp này việc kết hợp giữa các hệ thống đối xứng và bất đối xứng là một giải pháp lý tưởng. Sự kết hợp này cho ta ưu điểm về hiệu năng cao hơn các giải thuật đối xứng bằng cách gửi đi khóa bí mật trên các kênh an ninh, dựa trên cơ sở sử dụng các hệ thống khóa công khai. Sau khi cả hai phía đã có khóa bí mật chung, quá trình tiếp theo sẽ sử dụng các giải thuật khóa đối xứng để mật mã và giải mật mã. Đây là nguyên lý cơ sở của công nghệ mật mã khóa công khai được sử dụng trong nhiều giao diện hiện nay.

3.1.3.4. Nhận thực

Dựa vào đâu mà một người sử dụng có thể tin chắc rằng họ đang thông tin với bạn của mình chứ không bị mắc lừa bởi người khác? Nhận thực có thể giải quyết bằng sử dụng mật mã hóa khóa công khai.

Một ví dụ đơn giản: Bản thân bạn là người được cấp cho 2 khóa điện tử khóa 1 (public key) và khóa 2(private key). Bạn phải giữ gìn khóa 2 cẩn thận như giữa chiếc chìa khóa xe của mình. Khi có một người dùng khóa 1 để mã hóa một bức thư rồi gửi cho bạn, bạn phải dung khóa 2 để giải mã thì mới đọc được bức thư này. Đồng nghiệp hay người thân của bạn dù có biết bức thư này cũng chịu vì không tài nào giải mã được. Dùng khóa 2, cùng với một phần mềm phù hợp, bạn có thể ký tên lên một văn bản hay tập tin dữ liệu nào đó. Chữ ký điện tử này tương tự như một con tem độc nhất vô nhị dán lên văn bản, khó có thể giả mạo được. Ngoài ra, chữ ký còn đảm bảo phác giác được bất kỳ sự thay đổi nào trên dữ liệu đã được "ký". Để ký lên một văn bản, phần

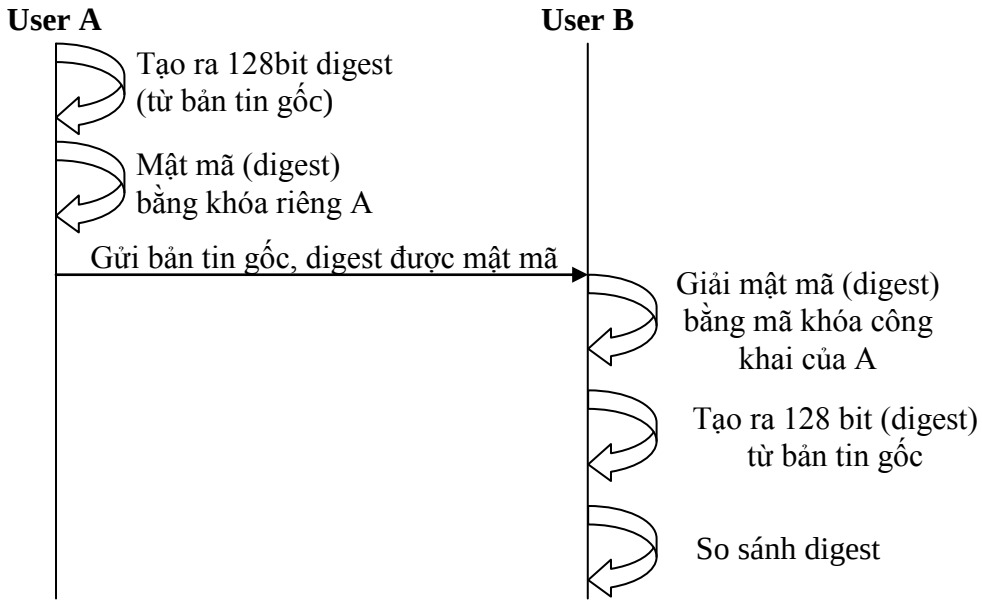
mềm ký tên của bạn sẽ nghiền dữ liệu để "túm lại" bằng một vài dòng, được gọi là thông báo tóm tắt, bằng một tiến trình được gọi là "kỹ thuật băm", rồi tạo thành chữ ký điện tử. Cuối cùng, phần mềm ký tên của bạn sẽ gắn chữ ký điện tử này vào văn bản. Khi bạn gửi văn bản đã ký tên này đến cho một đồng nghiệp thì anh ta dùng khóa 1 giải mã chữ ký ngược trở lại thành một thông báo tóm tắt để biết có phải chính bạn đã ký tên váo văn bản này hay không. Đồng thời anh ta cũng dùng phần mềm của mình tạo một thông báo tóm tắt từ dữ liệu trên văn bản và so sánh với thông báo tóm tắt do bạn tạo ra. Nếu hai thông báo tóm tắt này giống nhau tức là dữ liệu trên văn bản là toàn vẹn, không bị thay đổi bởi người khác.

3.1.3.5. Các chữ ký điện tử và tóm tắt bản tin

Chữ ký điện tử được sử dụng để kiểm tra xem bản tin nhận được có phải là từ phía phát hợp lệ hay không? Nó dựa trên nguyên tắc chỉ người tạo ra chữ ký mới có khóa riêng và có thể kiểm tra khóa này bằng khóa công khai. Chữ ký điện tử được tạo ra bằng cách tính toán tóm tắt bản tin gốc thành bản tin tóm tắt (MD). Sau đó, MD được kết hợp với thông tin của người ký, nhãn thời gian và thông tin cần thiết khác. MD là một hàm nhận số liệu đầu vào có kích cỡ bất kỳ và tạo ra ở đầu ra một kích cỡ cố định (vì thế được gọi là tóm tắt, digest). Tập thông tin này, sau đó được mật mã hóa bằng khóa riêng của phía phát và sử dụng các giải thuật bất đối xứng. Khối thông tin nhận được sau mật mã hóa được gọi là khóa điện tử.

Do MD là một hàm nên nó cũng thể hiện phần nào trạng thái hiện thời của bản tin gốc. Nếu bản tin gốc thay đổi thì MD cũng thay đổi. Bằng cách kết hợp MD vào chữ ký điện tử, phía thu có thể dễ dàng phát hiện bản tin gốc có bị thay đổi kể từ khi chữ ký điện tử được tạo hay không. Sau đây, ta xét quá trình sử dụng các digest (tóm tắt) bản tin để tạo các chữ ký điện tử.

Sau đây, ta xét quá trình sử dụng các digest (tóm tắt) bản tin để tạo các chữ ký điện tử.



Hình 3.2. Quá trình sử dụng tóm tắt bản tin để cung cấp các chữ ký điện tử

User A tạo ra một digest từ bản tin gốc, digest thực ra là một xâu có độ dài cố định được tạo ra từ một đoạn có độ dài bất kỳ của bản tin gốc. Rất khó để hai bản tin có cùng một digest, nhất là khi digest có độ dài ngắn nhất là 128bit. Các giải thuật thường được sử dụng để tạo ra một digest là MD5, thuật toán rối an ninh (SHA). Quá trình tạo ra một digest và mật mã nó bằng khóa riêng A nhanh hơn rất nhiều so với mật mã toàn bộ bản tin. Sau đó, User A gửi đi bản tin gốc và digest được mật mã đến User B, sau khi nhận được bản tin User B có thể sử dụng khóa công khai của User A để giải mật mã digest, đồng thời User B cũng tạo ra một digest từ văn bản gốc và so sánh hai xâu bit này với nhau. Nếu hai digest giống nhau thì User B có thể tin tưởng rằng bản tin văn bản gốc không bị phá rối trên đường truyền.

Vấn đề chính của quá trình xét ở trên là ta phải giả thiết rằng User B có khóa công khai hợp lệ với User A. Nhưng bằng cách nào mà User B biết được đã nhận được khóa công khai hợp lệ? làm cách nào mà người sử dụng biết rằng email cùng với khóa công khai thực sự là của nhà quản lý ngân hàng? Để giải quyết các vấn đề trên ý tưởng sử dụng các chứng chỉ số đã ra đời. Cơ quan cấp chứng chỉ là một tổ chức phát hành các giấy ủy nhiệm điện tử và

cung cấp các chứng chỉ số. Một chứng chỉ số thường gồm: tên người sử dụng, thời hạn và khóa công khai của người sử dụng. Chứng chỉ được cơ quan cấp chứng chỉ ký bằng số, để người sử dụng có thể kiểm tra chứng chỉ là đúng.

3.1.3.6. Các chứng chỉ số

Chứng chỉ số đảm bảo khóa công khai thuộc về đối tượng mà nó đại diện. Cần đảm bảo rằng chứng nhận số đại diện cho thực thể yêu cầu (cá nhân hoặc tổ chức), một đối tượng thứ ba là thẩm quyền chứng nhận (CA). Các thẩm quyền chứng nhận nổi tiếng là Verisign, Entrust và Certicom. Người sử dụng có thể mua chứng nhận số từ CA và sử dụng chúng để nhận thực và phân phối khóa riêng của họ. Khi phía thu đã nhận được khóa riêng của họ thì có thể yên tâm rằng phía thu chính là nơi họ yêu cầu.Sau đó, phía phát có thể gửi các bản tin được mật mã bằng khóa công khai đến phía thu. Phía thu có thể giải mật mã chúng bằng khóa riêng của mình. Thông thường chứng nhận số bao gồm:

+ Tên người sử dụng, thông tin nhận dạng duy nhất người này;
+ Khóa công khai của người sở hữu;
+ Thời gian chứng nhận có hiệu lực;
+ Chữ ký số từ CA để dễ dàng phát hiện nếu truyền dẫn bị làm giả.

Người sử dụng sở hữu chứng nhận số cũng có thể tự ký chứng nhận số để trởthành CA. Khi đó CA này là đáng tin cậy nếu được ký nhận bởi một khóa đáng tin cậy khác. Khuôn dạng hàng đầu cho các chứng nhận số là X.509 (tiêu chuẩn để nhận thực). Các chứng nhận này thường xuất hiện trong các ứng dụng Internet. Trong giao diện vô tuyến, một dạng khác của giao diện vô tuyến được sử dụng là chứng nhận an ninh lớp truyền tải (WLTS).

3.1.3.7. Hạ tầng khóa công khai PKI

PKI là một thuật ngữ dùng để mô tả một tổ chức hoàn thiện của các hệ thống, quy tắc để xác định một hệ thống an ninh. Nhóm đặc trách kỹ thuật Internet (IEFT) X.509 định nghĩa PKI như sau: “PKI là một tập bao gồm phần cứng, phần mềm, con người và các thủ tục cần thiết để tạo lập, quản lý, lưu trữ và hủy các chứng nhận số dựa trên mật mã khóa công khai”.

PKI gồm:

+ Thẩm quyền chứng nhận (CA): Có nhiệm vụ phát hành và hủy các

chứng chỉ số

+ Thẩm quyền đăng ký: Có nhiệm vụ ràng buộc khóa công khai với các nhận dạng của các sở hữu khóa

+ Các sở hữu khóa: Là những người sử dụng được cấp chứng nhận số và sử dụng các chứng chỉ số này để kí các tài liệu số

+ Kho lưu các chứng nhận số và danh sách hủy chứng nhận

+ Chính sách an ninh: Quy định hướng dẫn mức cao nhất của tổ chức về an ninh.

PKI là một khái niệm an ninh quan trọng, các khóa công khai được sử dụng để kiểm tra các chữ ký số (chứng chỉ số) trong kết nối mạng số liệu. Bản thân nó không mang bất cứ thông tin gì về thực thể cung cấp các chữ ký. Công nghệ nối mạng số liệu thừa nhận vấn đề này và tiếp nhận các chứng nhận an ninh, để ràng buộc khóa công khai và nhận dạng thực thể phát hành khóa. Thực thể phát hành khóa lại được kiểm tra bằng cách sử dụng một khóa công khai được tin tưởng đã biết, bằng cách sử dụng một chứng nhận được phát đi từ CA ở phân cấp cao hơn. Các chứng nhận được phát hành và thi hành bởi một thẩm quyền chứng nhận (CA). CA này được phép cung cấp các dịch vụ cho các thực thể được nhận dạng hợp lệ, khi chúng yêu cầu. Để thực hiện được các chức năng đó các CA phải được tin tưởng bởi các thực thể (các thành viên của PKI) dựa trên các dịch vụ mà nó cung cấp.

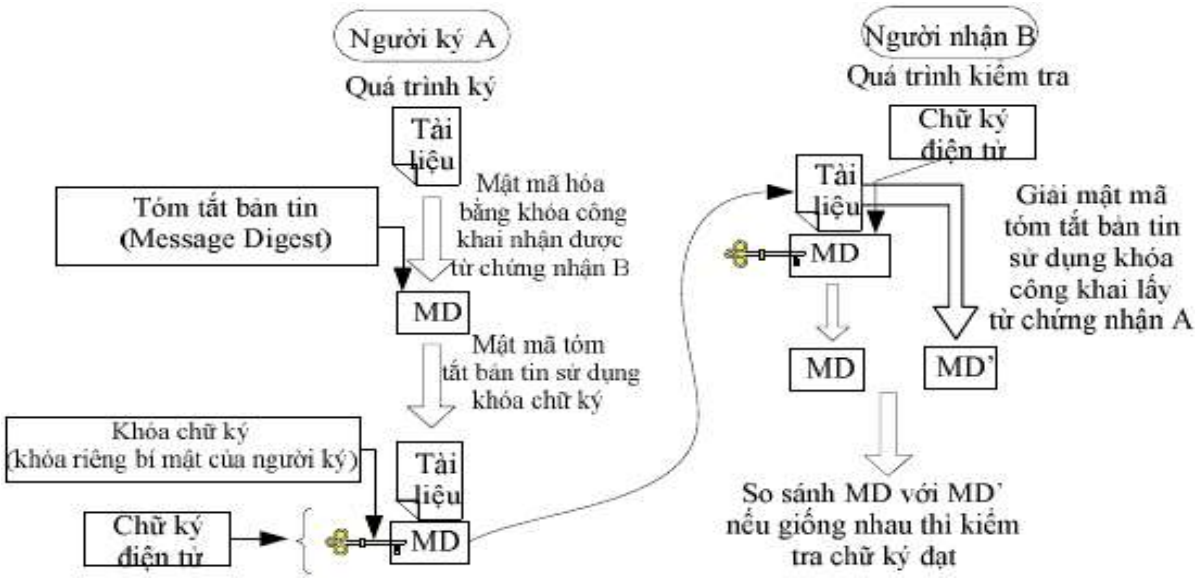
Tất cả các chứng nhận được ký bởi một khóa riêng của CA, người sử dụng chứng nhận có thể xem, kiểm tra thông tin của chứng nhận đó có hợp lệ hay không? Bằng cách giải mật mã chữ ký bằng một khóa kiểm tra công khai, có thể kiểm tra, xem nó có phù hợp với MD của nội dung nhận được trong chứng nhận hay không? Chữ ký thường là một MD được mật mã hóa.

Các thành viên PKI có thể thỏa thận thời gian hiệu lực tiêu chuẩn cho một chứng nhận. Vì thế, có thể xác định khi nào một chứng nhận bị hết hạn. Mặt khác thẩm quyền chứng nhận (CA) có thể công bố một danh sách hủy chứng nhận (CRL) để các thành viên PKI biết chứng nhận không còn hợp lệ với CA nữa.

Các quan hệ tin tưởng giữa CA và các thành viên PKI khác phải được thiết lập trước khi diễn ra giao dịch PKI. Các quan hệ này thường nằm ngoài

phạm vi PKI và vì thế cũng nằm ngoài phạm vi công nghệ nối mạng. Các quan hệ tin tưởng PKI có thể được thiết lập trên cơ sở địa lý, chính trị, xã hội, dân tộc và có thể mở rộng cho các nền công nghiệp, các nước, các nhóm dân cư hay các thực thể khác được ràng buộc bởi các mối quan tâm chung. Về mặt lý thuyết thì các mô hình tin tưởng PKI có thể dựa trên một CA duy nhất, được sử dụng để tạo lập PKI trên toàn cầu giống như Internet hay một phân cấp phân bố các CA.

Quá trình trao đổi bí mật (khóa chia sẻ phiên hay thông tin để tạo ra khóa này) giữa hai phía A và B được minh họa ở hình sau:



Hình 3.3. Nhận thực bằng chữ ký điện tử

Người ký A nhận được khóa công khai từ chứng nhận B. Vì chứng nhận B được ký bởi khóa riêng của thẩm quyền chứng nhận bên B, nên nó có thể được kiểm tra tại thẩm quyền chứng nhận bên B bằng khóa công khai mà B nhận được từ thẩm quyền chứng nhận của mình. Đồng thời chứng nhận CA của B lại được kiểm tra bằng khóa công khai nhận được từ CA gốc và khóa này được đảm bảo là hợp lệ. Vì nó đã được chuyển thành mã của PKI Client trong modem phần mềm của A. Sau khi đã có được khóa công khai của B, A mật mã hóa bí mật bằng cách sử dụng khóa này. Và sau đó bản tin được mật mã này được gửi đến B cùng với chứng nhận CA của A và tóm tắt bản tin

MD của bí mật được mật mã hóa, được tính toán theo khóa riêng của A. Khi nhận được bản tin này, B kiểm tra như sau: trước hết B giải mật mã hóa bản tin bằng khóa riêng của mình, tính toàn MD từ kết quả nhận được, sử dụng khóa công khai của A để giải mật mã MD nhận được từ A, rồi sau đó so sánh MD' với MD. Nếu bằng thì nhận thực thành công và bí mật nhận được sau khi giải mật mã là bí mật cần truyền.

Chứng nhận có thể được gửi đi ở các khuôn dạng khác nhau, tiêu chuẩn an ninh được tiếp nhận rộng rãi là X.509 do ITU định nghĩa. Các thực thể công cộng và riêng dựa trên các dịch vụ tin tưởng do một CA chung cung cấp và tiếp nhận do CA cung cấp. Do vậy, các thành viên của PKI chỉ cần thiết lập quan hệ tin tưởng an ninh với một thành viên của PKI với CA chứ không phải với các thành viên khác. Vì thế có thể định nghĩa PKI ngắn gọn như sau: "PKI như một thực thể ảo kết hợp nhiều thực thể vật lý bởi một tập các chính sách và các quy tắc ràng buộc các khóa chung với các nhận dạng của các thực thể phát hành khóa, thông qua việc sử dụng một thẩm quyền chứng nhận CA".

PKI gồm ba chức năng chính:

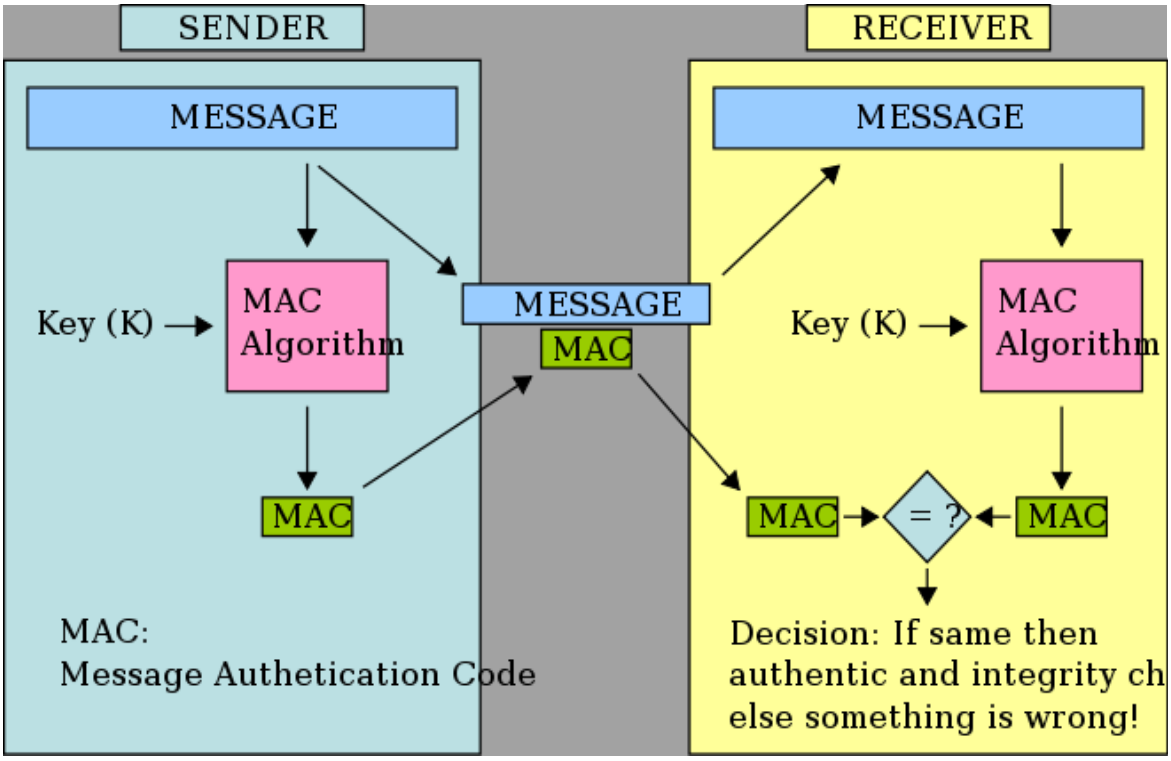
+ ***Chứng nhận:*** Chứng nhận hay ràng buộc một khóa với một nhận dạng bằng một chữ ký được thực hiện bởi một thẩm quyền chứng nhận CA. Quá trình chứng nhận bao gồm việc tạo ra một cặp khóa gồm khóa công khai và khóa riêng, do người sử dụng tạo ra và tính toán cho CA trong một phần của yêu cầu hay do CA thay mặt người sử dụng tạo ra.

+ Công nhận hợp lệ: Công nhận có hợp lệ hay chuyên môn hơn là kiểm tra nhận thực chứng nhận được thực hiện bởi một thực thể PKI bất kỳ. Quá trình công nhận hợp lệ bao gồm việc kiểm tra chữ ký do CA phát hành, đối chiếu với danh sách hủy chứng nhận (CRL) và khóa công khai của CA.

+ ***Hủy:*** Hủy một chứng nhận hiện có, trước khi nó hết hạn cũng được thực hiện bởi CA. Sau khi chứng nhận bị hủy, CA cập nhật thông tin mới cho CRL. Trong một kịch bản điển hình, khi người sử dụng cần nhận hay công nhận một chứng nhận được trình bày hợp lệ, nó sẽ gửi yêu cầu này đến CA. Sau khi chứng nhận được yêu cầu được phát đi hay tính hợp lệ của nó được kiểm tra, thông tin tương ứng được CA gửi vào một kho chứng nhận, trong đó có cả CRL.

3.1.3.8. Nhận thực bằng bản tin nhận thực

Nhận thực bằng bản tin nhận thực là một phương pháp đảm bảo toàn vẹn số liệu và nhận thực nguồn gốc số liệu. Một sơ đồ phổ biến của phương pháp này là sử dụng mã nhận thực bản tin MAC



Hình 3.4. Phương pháp nhận thực sử dụng MAC

Người gửi tin nhắn chạy nó thông qua một thuật toán MAC để sản xuất một thể dữ liệu MAC. Thông điệp và các từ khóa MAC sau đó được gửi đến người nhận. Thu lần lượt chạy phần tin nhắn của truyền thông qua các thuật toán cùng MAC bằng cách sử dụng cùng một chìa khóa, sản xuất một MAC thứ hai dữ liệu thẻ. Người nhận sau đó so sánh các từ khóa MAC đầu tiên nhận được trong truyền tải đến các từ khóa thứ hai MAC tạo ra. Nếu giống nhau, người nhận có thể thừa nhận rằng sự toàn vẹn của thông điệp không bị tổn hại, và thông điệp không bị thay đổi hoặc giả mạo trong quá trình truyền.

Một phương pháp phổ biến nhất để tạo ra MAC là sử dụng MD5. MD5 nhận bản tin có độ dài bất kỳ và tạo ra ở đầu ra 128 bit MD. Phía phát sẽ gửi bản tin gốc cùng với MD đến phía thu, phía thu tính MD từ bản tin gốc nhận được và so sánh với MD thu được để nhận định bản tin còn nguyên vẹn hay không?

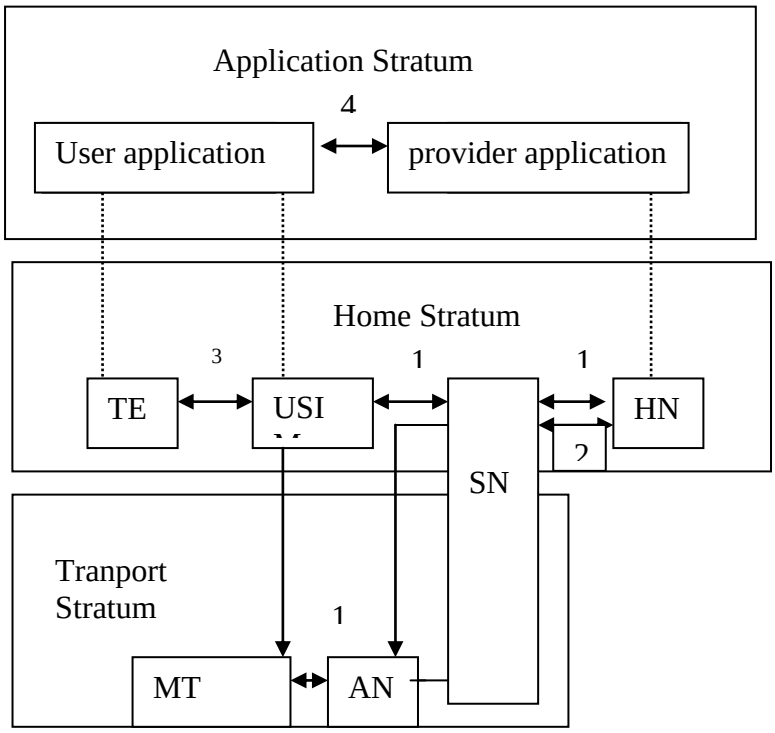
Giải thuật SHA-1 cũng có thể được sử dụng để tính toán MD giống như MD5. Tuy nhiên MD ở đầu ra của nó chỉ là 120bit.

Bằng cách sử dụng hàm làm rối (hàm Hash) một máy tính có thể nhận thực một người sử dụng mà không cần lưu trữ mật khẩu trong văn bản thô. Sau khi tạo ra một tài khoản (account) người sử dụng gõ mật khẩu, máy tính sử dụng hàm Hash một chiều với đầu vào là mật khẩu, để tạo ra giá trị làm rối (giá trị Hash) và lưu giữ giá trị này. Lần sau khi người sử dụng đăng nhập vào máy tính, máy tính sẽ sử dụng hàm Hash với đầu vào là mật khẩu mà người sử dụng gõ vào để tính ra giá trị Hash và so sánh giá trị này với giá trị được lưu. Nếu kết quả giống nhau thì người sử dụng đó được quyền đăng nhập. Do mật khẩu không được lưu trong văn bản thô nên rất khó bị lộ.

Cả MD5 và SHA-1 đều là các hàm Hash không khóa, nghĩa là không có khóa bí mật giữa các bên tham gia thông tin. Các giải thuật này không sử dụng khóa bí mật làm đầu vào hàm Hash. Giải thuật mã nhận thực bản tin rối HMAC sử dụng hàm Hash với một khóa chia sẻ bí mật để nhận thực bản tin. Mục đích chính của HMAC bao gồm:

+ Sử dụng các hàm Hash hiện có mà không cần thay đổi chúng, ví dụ có thể sử dụng các chương trình phần mềm của các hàm Hash đang được sử dụng rộng rãi và miễn phí;
+ Duy trì hoạt động nguyên gốc của hàm Hash mà không làm giảm đáng kể chất lượng

3.1.4. Mô hình an ninh tổng quát của một hệ thống thông tin di động



Hình 3.5. Kiến trúc an ninh tổng quát của một hệ thống thông tin di động

TE: Thiết bị đầu cuối

UMTS: User Identity Module Dịch vụ

SN: Phục vụ mạng

HN: Nhà mạng

MT: Điện thoại di động kết cuối

AN: Truy cập mạng

Nhìn vào hinh ve ta thấy được UMTS bao gồm năm nhóm tính năng bảo mật:

+ Nhóm 1: cho người dùng truy cập an toàn tới các dịch vụ UMTS và bảo vệ lại các cuộc tấn công vào liên kết truy nhập vô tuyến.

+ Nhóm 2: bảo vệ chống lại các cuộc tấn công mạng có dây và cho phép các nút trong lĩnh vực cung cấp dịch vụ để trao đổi dữ liệu báo hiệu an toàn.

+ Nhóm 3:cung cấp an toàn cho trạm di động.

+ nhóm 4: cho phép trao đổi an toàn thông tin giữa các ứng dụng cho người sử dụng và trong lĩnh vực cung cấp dịch vụ.

+ Nhóm 5: Bảo mật cho phép người dùng để quan sát xem là tính năng bảo mật đang hoạt động và nếu một số dịch vụ phụ thuộc vào tính năng bảo mật.

An ninh trong GSM

3.1.5. Nhận thực thuê bao GSM

Môi trường an ninh trên giao diện vô tuyến GSM được đảm bảo bởi hai quá trình: nhận thực và mật mã.

Ở GSM chỉ có mạng nhận thực MS. AuC được sử dụng để nhận thực SIM card của thuê bao, AuC tạo ra bộ ba thông số {RAND||SRES||Kc}. Trong đó, RAND (128bit); Kc (128bit); SRES (32bit). Tiếp theo, RAND được gửi xuống SIM, SRES được gửi xuống VLR đang quản lý thuê bao thông qua HLR. Các thông số này được lưu tại VLR và được sử dụng cho từng cuộc gọi. Sau khi nhận được hô lệnh mạng ngẫu nhiên (RAND), SIM sử dụng nó cùng với khóa nhận thực thuê bao Ki được lưu tại đây làm đầu vào cho giải thuật A3 để tạo ra giá trị trả lời được ký (SRES). Sau đó SIM gửi giá trị này trở lại mạng (VLR) để mạng kiểm tra bằng cách so sánh nó với SRES

tương ứng được tạo ra ở AuC, nếu chúng trùng nhau thì nhận thực thành công và MS đó hợp lệ.

3.1.6. Mật mã hóa ở GSM

Mục đích của mật mã hóa là đảm bảo tính riêng tư cho thông tin người sử dụng trên đường truyền vô tuyến. Sau khi nhận thực người sử dụng thành công, tại SIM giải thuật A8 sử dụng khóa nhận thực Ki cùng với hô lệnh ngẫu nhiên (RAND) để tạo ra khóa mật mã Kc (64bit). Tiếp theo giải thuật A5 được sử dụng với đầu vào là văn bản thô, số khung Count (24bit) và khóa mật mã Kc, để cho ra vản bản đã được mật mã, và gửi chúng lên giao diện vô tuyến để truyền đi. Tại phía mạng phục vụ khóa Kc tương ứng được tạo ra ở AuC bằng giải thuật A8 và được gửi đến BTS thông qua VLR, tại đây bằng cách sử dụng giải thuật A5 với đầu vào là Kc, số khung count (24bit) để chống phát lại và văn bản đã được mã hóa nhận được từ MS gửi đến. Cho ra văn bản thô ở đầu ra. Có thể nói hai quá trình này là quá trình mật mã và giải mật mã hóa số liệu. Luồng mật mã tại đầu này phải được đồng bộ với luồng giải mật mã ở đầu kia để luồng bit mật mã hóa và luồng bit giải mật mã trùng khớp với nhau.

3.1.7. Các hạn chế trong an ninh GSM

An ninh GSM dựa trên nhận thực và bảo mật đã thể hiện ưu điểm vượt trội so với hệ thống thông tin di động tương tự (1G). Tuy nhiên, nó cũng tồn tại không ít các hạn chế:

+Cả hai giải thuật A3 và A8 đều được sử dụng để nhận thực người sử dụng và tạo ra các khóa phiên đều được thực hiện bởi các nhà cung cấp dịch vụ bằng giải thuật COMP128. COMP128 đã được tính toán đảo tại Berkeley vào năm 1998 và các phân tích về mật mã học của các nhà nghiên cứu Berkeley chỉ ra rằng, giải thuật này có thể bị phá vỡ sau 219 lần hỏi từ một BTS giả mạo đến SIM card trong vòng 8 giờ. Phân tích kỹ hơn về ứng dụng COMP128 của GSM cũng phát hiện rằng bản thân giải thuật này cũng bị thực hiện yếu. Giải thuật đòi hỏi khóa 64bit, nhưng 10bit trong số đó luôn được đặt bằng 0, vì thế giảm đáng kể tính an ninh của ứng dụng A8. Nếu khóa Kc bị tổn hại, kẻ xâm phạm có thể đóng giả VLR hợp pháp mà không cần định kỳ nhận thực. Ngoài ra việc lưu giữ bộ tam {RAND, SRES và Kc} trong VLR để

đợi sử dụng sẽ tăng thêm khả năng bị lộ nhất là đối với xâm phạm từ bên trong.

+ Dưới sự điều khiển của giao thức nhận thực GSM, BTS nhận thực MS yêu cầu phiên thông tin. Tuy nhiên không có nhận thực ngược lại từ MS đến mạng, nên MS không được đảm bảo rằng nó không bị thông tin với một BTS giả mạo. Điều này lại trở nên tồi tệ hơn khi chính hô lệnh ngẫu nhiên (RAND) được dùng để nhận thực lại là hạt giống để tạo ra mã phiên khi sử dụng làm đầu vào cho giải thuật A8. Ngoài ra giao thức bản tin hô lệnh-trả lời lại không chứa nhãn thời gian. Vì thế nếu một BTS giả mạo thành công nó có thể tìm được một khóa phiên để giải mã mọi bản tin sử dụng cùng khóa trong thời gian khá dài.

+ Nhận thực GSM nói riêng và an ninh GSM nói chung bảo vệ đường truyền vô tuyến giữa MS và BTS phục vụ nó. Cơ chế an ninh này không bảo vệ truyền dẫn thông tin giữa AuC và mạng phục vụ. Việc thiếu an ninh trong mạng hữu tuyến là khả năng chính để lộ ở GSM, nhất là hiện trạng truyền dẫn giữa các BTS và mạng hữu tuyến thường là các đường viba số dẫn đến thông tin dễ bị chặn.

+ Trong số hai phương án của giải thuật mật mã hóa số liệu (A5/1 và A5/2), giải thuật yếu hơn là A5/2 và có thể được xuất khẩu trên toàn thế giới không hạn chế. Theo Bruce Schneier, A5/2 được phát triển với sự hỗ trợ của NSA và có thể bị phá vỡ trong thời gian thực với hệ số phá vỡ là khoảng 2_{16}. A5/1 mạnh hơn và có khả năng chịu đựng tấn công với hệ số phá vỡ là 2_{20}. Nghĩa là nếu kẻ tấn công sử dụng phần cứng đặc biệt có thể gây tổn hại gần như ở thời gian thực

3.2. Giải pháp an ninh trong 3G UMTS

3.2.1. Mô hình kiến trúc an ninh 3G UMTS

- **Nhận thực**

Nhận thực để xác nhận nhận dạng câu một thực thể. Một nút muốn nhận thực đến một người (A) thì phải trình diện số nhận dạng của mình. Quá trình này được thực hiện bằng cách chỉ ra được mọt bí mật mà chỉ có hai nút mạng mới biết hoặc một nút trung gian được cả hai nút tin tưởng giao cho để xác nhận các nhận dạng của chúng. Nhận thực trong 3G UMTS được chia thành 2 phần:

+ Mạng nhận thực người

+ Người nhận thực mạng

Thử tục mạng nhận thực người và người nhận thực mạng , trong quá trình trao đổi bản tin xẩy ra cùng một lúc. Thủ tục này gọi là "nhận thực một lần gửi" để giảm các bản tin cần truyền.Sau các thủ tục này, người sử dụng sẽ tin tưởng mạng được cung cấp đến.Đồng thời, mạng cũng tin tưởng nhận dạng của người sử dụng là hợp lệ.

- **Bảo mật**

Bảo mật để bảm bảo an ninh thông tin không bị rò rỉ ra bên ngoài.Khi mà số lượng thuê bao không ngừng tăng cho cả các cuộc gọi cá nhận lẫn doanh nghiệp(ví dụ trực tuyến như trao đổi ngân hàng) thì nhu cầu bảo mật thông tin ngày càng trở nên bức thiết.

Bảo mật trong 3G UMTS đạt được bằng cách mật mã hóa các cuộc truyền hông giữa thuê bao và mạng, bằng cách sử dụng nhận thực tạm thời TMSI thay cho sử dụng nhận dạng toàn cầu IMSI. Mật mã hóa được thực hiện giữa USIM và RNC, bảo mật người sử dụng được thực hiện giữa USIM và VLR/SGSN. Các thuộc tính cần bảo mật:

+ Nhận dạng thuê bao
+ Vị trí hiện thời của thuê bao
+ Số liệu người sử dụng
+ Số liệu báo hiệu

Nếu mạng phục vụ không hỗ trợ bảo mật số liệu người sử dụng thì thuê bao cần được thông báo về khả năng này bị từ chối

- **Toàn vẹn**

Đôi khi bản tin mà chúng ta có thể nhận được từ từ một phía nhận thực tin cậy,nhưng co thể bị giả mạo.Bởi vậy để tránh vấn đề này cần có bảo vệ toàn vẹn, với mục đích không chỉ bảo mật bản tin mà cần bảo đảm đây là bản tin chính thống. Tạo ra các con dấu bổ sung cho các bản tin là phương pháp tối ưu nhất để bảo vệ toàn vẹn trong 3G UMTS.Từ một khóa chủ biết trước (K), các con dấu có thể được tạo ra tại các nút biết được các khóa.Bảo vệ toàn vẹn đặc biệt cần thiết, vì mạng phục vụ thường được khai thác bởi

một nhà khai thác khác với nhà khai thác của thuê bao. Thuộc tính cần được bảo vệ toàn vẹn là các bản tin báo hiệu.

Cần lưu ý rằng tại lớp vật lý, các bit được kiểm tra tính toàn vẹn bằng cách kiểm tra tổng CRC (kiểm tra vòng dư). Xong các biện pháp này chỉ được thực hiện để đạt được các cuộc truyền thông số liệu không mắc lỗi trên giao diện vô tuyến, chứ không giống như toàn vẹn mức truyền tải.

3.2.2. Các hàm mật mã

3.2.2.1. Yêu cầu đối với các giải thuật và các hàm mật mã

Các giải thuật và các hàm mật mã phải đáp ứng các yêu cầu chặt chẽ. Các hàm này phải được thiết kế để có thể tiếp tục được sử dụng ít nhất 20 năm. Các UE chứa các hàm này không bị giới hạn về xuất khẩu và sử dụng. Các thiết bị mạng như RNC và AuC có thể phải chịu các hạn chế. Việc xuất khẩu các nút này phải tuân thủ thỏa thuận Wassenaar. Như vậy nhà khai thác có thể thiết lập thiết bị và giải thuật theo luật và giấy phép địa phương và người sử dụng có thể chuyển mạng bằng thiết bị của mình mỗi khi chuyển đến một mạng hay một nước khác. Khi không biết các khóa đầu vào, ta không thể phân biệt các hàm này với các hàm ngẫu nhiên độc lập của các đầu vào của chúng. Thay đổi một thông số đầu vào mỗi lần không thể phát hiện bất kỳ thông tin nào về khóa chủ (K) hay trường cầu hình của nhà khai thác

3.2.2.2. Các hàm mật mã

Các tính năng an ninh của 3G UMTS được thực hiện bởi tập các hàm và các giải thuật mật mã. Tất cả có mười hàm mật mã để thực hiện tính năng này : f0, f1, f2, f3, f4, f5, f1*, f5*, f8 và f9. Trong đó, f0 để tạo ra hô lệnh ngẫu nhiên (RAND), bẩy hàm tiếp theo là các hàm tạo khóa. Chúng đều là đặc thù nhà khai thác, vì các khóa được sử dụng để nhận thực chỉ được tạo ra ở USIM và AuC. Đây là hai miền mà cùng một nhà khai thác phải chịu trách nhiệm. Các hàm để tạo ra các thông số AKA là: f1, f2, f3, f4, f5, f1* và f5*. Việc lựa chọn các hàm này về nguyên tắc là tùy thuộc vào nhà khai thác. Do việc thiết kế giải thuật mật mã mạnh cho các hàm này rất khó, nên 3GPP đã cung cấp một tập mẫu các giải thuật AKA với tên gọi là MILENAGE. Việc cấu trúc các giải thuật này dựa trên một giải thuật mật mã mạnh 128bit được gọi là hàm lõi cùng với trường cấu trúc bổ sung do nhà khai thác lựa chọn. Tiêu chuẩn mật mã hóa tiên tiến (AES) được khuyến nghị sử dụng cho hàm

lõi của các hàm f1, f2, f3, f4 và f5. Hàm f1* và f5* được sử dụng để tạo khóa phục vụ quá trình đồng bộ lại. Các hàm f8 và f9 sử dụng hàm lõi là bộ mật mã khối KASUMI. Các hàm f8 và f9 được sử dụng trong USIM và RNC, vì hai miền này có thể thuộc hai nhà khai thác khác nhau, nên chúng không thể đặc thù nhà khai thác. Các hàm này sử dụng khóa chủ (K). Lý do là để tránh phân bổ khóa này trên mạng và để giữ nó an toàn trong USIM và AuC

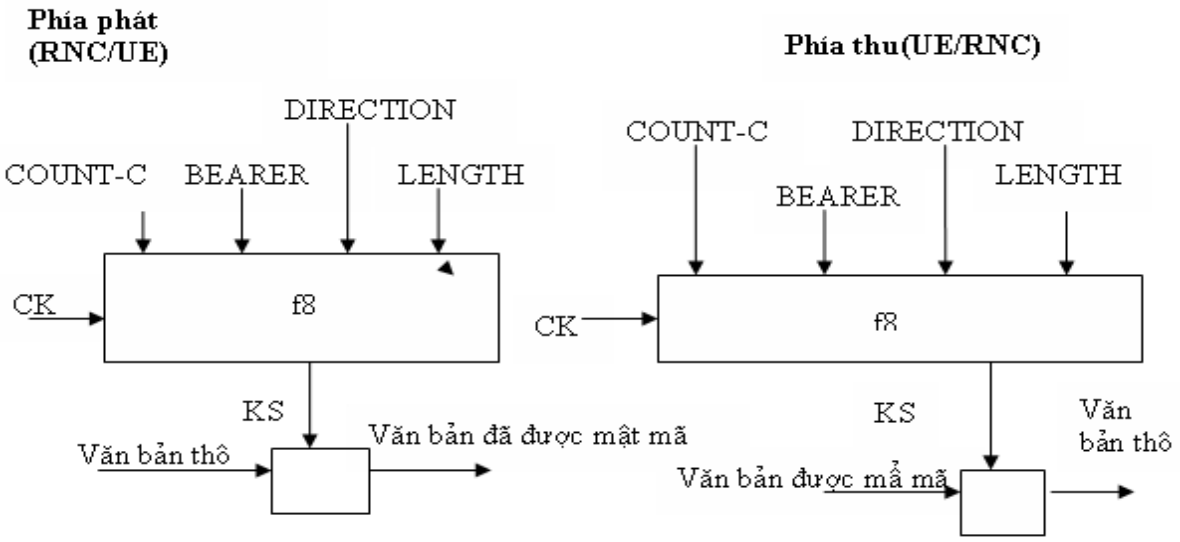
Bảng 4. Các hàm mật mã.

Hàm	**Đầu vào**	**Đầu ra**	**Chức năng**
f0		RAND	Tạo hô lệnh ngẫu nhiên cho mạng
f1	K, SQN, AMF, RAND,	MAC-A/XMAC-A	Nhận thực mạng
f2	K, RAND	XRES VÀ RES	Nhận thực người dử dụng
f 3	K, RAND	CK	Tạo khóa mật mã
f 4	K, RAND	IK	Tạo khóa toàn vẹn
f 5	K, RAND	AK	Tạo khóa dấu tên
f 1*	K, RAND,	MAC-S	Nhận thực bản tin đồng bộ lại
f 5*	K,RAND	AK	Tạo khóa dấu tên cho bản tin đồng bộ lại
f 8	CK, COUNT-C, BEARER, DICRECTION, LENGTH	KS	Tạo luồng khóa để mật mã hóa và giải mật mã hóa số liệu
f 9	Bản tin báo hiệu phát/ thu, DICRECTION, IK, COUNT-I, FREESH	MAC-I VÀ XMAC-I	Tạo mã nhận thực toàn vẹn bản tin

- ***Hàm f8***

Số liệu người sử dụng và một số phần tử thông tin báo hiệu được coi là nhậy cảm và phải được bảo mật. Để bảo mật nhận dạng, số nhận dạng thuê bao di động tạm thời gói (P-TMSI) phải được truyền trong chế độ bảo mật tại thời điểm cấp phát và tại các thời điểm khác, khi các thủ tục báo hiệu cho

phép nó. Hàm mật mã đảm bảo chế độ truyền dẫn có bảo vệ trên các kênh truy nhập vô tuyến giữa UE và RNC. Chúng ta dùng hàm mật mã f8 để tiến hành mật mã hóa và giải mật mã hóa số liệu (hình 3.6)



Hình 3.6. Quá trình mật mã hóa và giải mật mã hóa bằng hàm f8

Các thông số đầu vào của hàm f8 bao gồm: Số trình tự mật mã hóa (COUNT-C) (32bit), số này tăng mỗi khi gửi đi hoặc thu về một bản tin được bảo mật. Có hai bộ đếm cho đường lên và đường xuống. Khóa mật mã (CK) (128bit) được tạo ra ở AuC và được gửi đến VLR/SGSN trong các vec-tơ nhận thực (AV). Sau khi quá trình nhận thực thành công, khóa này được gửi đến RNC. USIM tạo ra các khóa này trong thời gian nhận thực, khi thực hiện chuyển giao khóa mật mã (CK) được truyền từ RNC hiện thời đến RNC mới để đảm bảo tiếp tục truyền thông. CK không thay đổi khi chuyển giao. Sẽ có hai khóa CK, một CK_{cs} được thiết lập giữa miền dịch vụ chuyển mạch kênh với người sử dụng và CK_{ps} được thiết lập giữa miền dịch vụ chuyển mạch gói với người sử dụng.

Nhận dạng kênh mang (BEARER) (5bit) được sử dụng để phân biệt các kênh mang vô tuyến logic khác nhau liên kết với cùng một người sử dụng trên cùng một kênh vật lý. Điều này được thực hiện để tránh xảy ra cùng một thông số đầu vào dẫn đến cùng một luồng khóa cho các kênh mang vô tuyến khác nhau.

Nhận dạng hướng (DIRECTION) (1bit) được sử dụng để phân biệt các bản tin phát với các bản tin thu nhằm tránh sử dụng cùng một thông số đầu vào cho hàm.

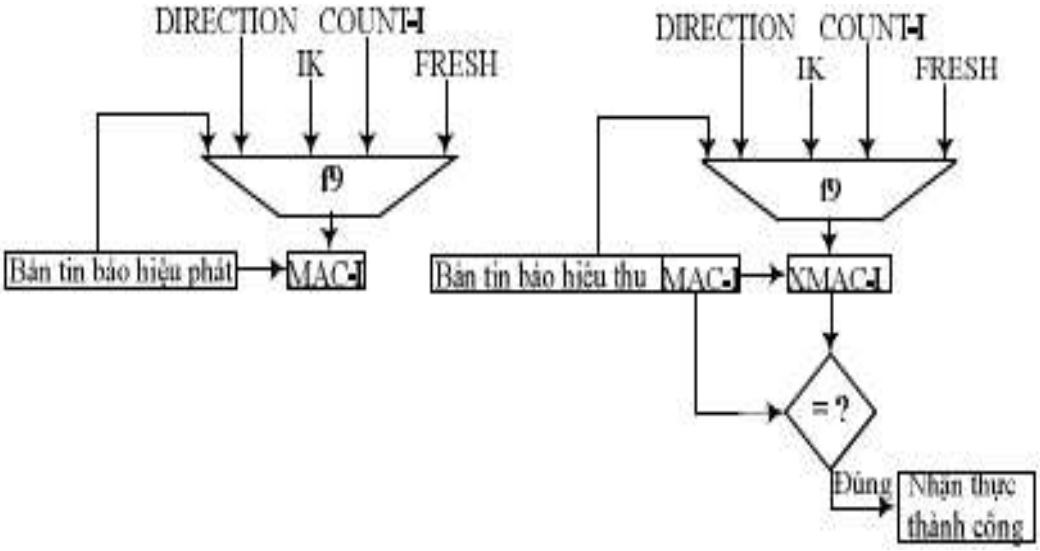
Nhận dạng hướng có kích cỡ 1bit, với "0" cho các bản tin ở đường lên (xuất phát từ USIM) và "1" cho các bản tin ở đường xuống (xuất phát từ RNC). Thông số này cùng với COUNT-C đảm bảo rằng các thông số đầu vào thay đổi trong một kết nối. Thông số chiều dài (LENGTH) (16bit) được sử dụng để đặt độ dài cho luồng khóa (KS). Bản thân thông số này không làm thay đổi các bit trong KS, nhưng nó ảnh hưởng tới số bit trong luồng này.

Thông số ở đầu ra của hàm là luồng khóa KS, luồng khóa này được thực hiện XOR với văn bản thô rồi phát lên giao diện vô tuyến. Luồng khóa KS của bộ mật mã hóa là duy nhất đối với từng khối. Với các thông số đầu vào khác nhau ta sẽ thu được ở đầu ra các KS khác nhau. Vì thế cả phía phát lẫn phía thu phải đồng bộ bằng cùng một bộ đếm tại mọi thời điểm để tạo ra cùng một COUNT-C, bằng không không thể giải mật mã hóa được. Đồng thời, cả USIM và RNC phải sử dụng đồng thời cùng một giải thuật mật mã. USIM thông báo cho RNC về các giải thuật mật mã mà nó hỗ trợ, RNC sau đó chọn giải thuật mật mã sẽ sử dụng theo ưu tiên của nhà khai thác và quy định địa phương. Quá trình này được gọi là nhận dạng giải thuật mật mã (UEA).

Khi cần bảo vệ toàn vẹn, bảo mật chỉ là tùy chọn, tuy nhiên người sử dụng phải được thông báo về việc có cho phép mật mã hóa hay không.

- **Hàm f9**

Hầu hết các thông tin báo hiệu điều khiển được gửi giữa UE và mạng đều được coi là nhậy cảm và cần được bảo vệ toàn vẹn. Hàm toàn vẹn (f9) được sử dụng để bảo vệ toàn vẹn các bản tin đó. Trái lại số liệu của người sử dụng không được bảo vệ toàn vẹn và nó chỉ được bổ sung ở các giao thức bậc cao hơn nếu cần. Bảo vệ toàn vẹn là bắt buộc trong 3G UMTS cho các bản tin báo hiệu, hàm f9 được sử dụng giống như AUTN và AUTS. Nó bổ sung "các dấu ấn" vào các bản tin để đảm bảo rằng các bản tin này được tạo ra tại nhận dạng hợp lệ. Nó cũng đảm bảo rằng bản tin không phải là giả mạo. Quá trình kiểm tra toàn vẹn bản tin bằng hàm toàn vẹn f9 được mô tả trong hình 3.7.



Hình 3.7. Lưu đồ thuật toán hàm f9

Các thông số đầu vào của hàm f9 bao gồm:

Số trình tự toàn vẹn (COUNT-I) (32bit), số này tăng mỗi khi gửi đi hoặc thu về một bản tin được bảo vệ toàn vẹn. Có hai bộ đếm cho đường lên và đường xuống.

Khóa toàn vẹn (IK) (128bit) được tạo ra ở cả AuC lẫn USIM. VLR/SGSN nhận IK trong AV từ AuC gửi đến, sau quá trình nhận thực thành công nó được gửi đến RNC. Khi xảy ra chuyển giao, khóa toàn vẹn IK được chuyển từ RNC hiện thời đến RNC mới, khóa này không đổi khi chuyển giao. Số nhận dạng hướng (DIRECTION) (1bit) được sử dụng để phân biệt bản tin phát và bản tin thu. Điều này cần thiết để tránh việc hàm sử dụng cùng một thông số cho các bản tin phát đi và thu về. Số nhận dạng hướng là 1bit, với "0" cho bản tin ở đường lên (xuất phát từ USIM) và "1" cho bản tin ở đường xuống (xuất phát từ RNC). Thông số làm tươi (FRESH) được sử dụng để chống các tấn công phát lại. Một giá trị FRESH được ấn định cho từng người sử dụng, RNC tạo ra thông số này khi thiết lập kết nối. Sau đó, nó gửi thông số này đến người sử dụng bằng "lệnh chế độ an ninh". Thời hạn hiệu lực của thông số này là một kết nối và giá trị FRESH mới sẽ được tạo ra tại kết nối sau. Ngoài ra, khi chuyển giao, FRESH sẽ được đặt lại vào giá trị mới.

Một thông số quan trọng nhất cho hàm là "bản tin báo hiệu". Nhờ hàm

này mà bản tin báo hiệu được bảo vệ toàn vẹn. Nếu trong quá trình truyền thông mà bản tin này bị thay đổi thì sẽ không có các giá trị ở đầu ra (MAC-I và XMAC-I) trùng nhau, vì thế nơi nhận sẽ từ chối bản tin này.

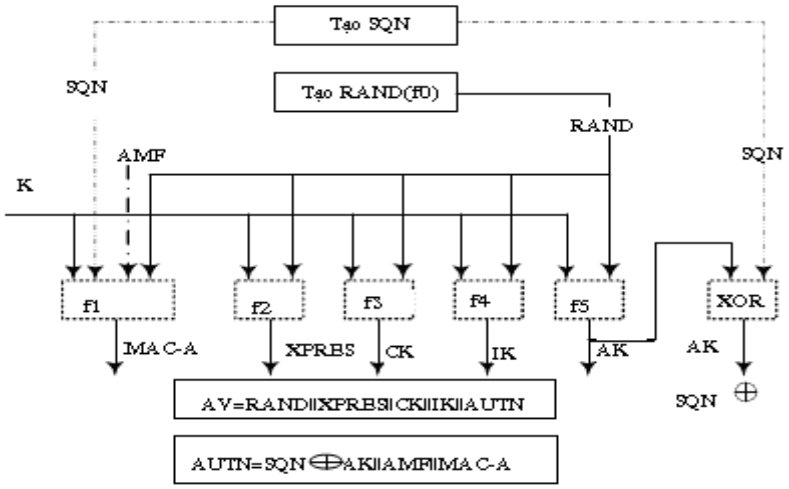
Thông số ở đầu ra của hàm f9 là mã nhận thực bản tin toàn vẹn số liệu (MAC-I) và XMAC-I (giá trị kỳ vọng) được sử dụng sau khi kết thúc các thủ tục AKA, MAC-I được tạo ra ở phía phát (USIM hoặc RNC) và được so sánh với XMAC-I tại phía thu (RNC hoặc USIM). Phía phát tạo ra MAC-I với bản tin đầu vào và phía thu sử dụng chính bản tin đi kèm cho hàm của chính nó để tạo ra XMAC-I. Nếu chúng trùng nhau chứng tỏ rằng bản tin không bị thay đổi và gốc của nó được nhận thực. Nếu không trùng nhau thì bản tin sẽ bị từ chối.

Cũng tương tự như ở hàm f8 cả phía phát lẫn phía thu phải đồng bộ bằng cùng một bộ đếm tại mọi thời điểm để tạo ra cùng một COUNT-I. Đồng thời, do giải thuật toàn vẹn UMTS xảy ra ở cả USIM và RNC, nên chúng có thể ở các miền của các nhà khai thác khác nhau. Vì thế, các nút có thể hỗ trợ các giải thuật khác nhau. Để nhận dạng các giải thuật khác nhau được sử dụng, mỗi giải thuật toàn vẹn UMTS (UIA) có một nhận dạng riêng 4bit. USIM sẽ cung cấp cho RNC thông tin về các UIA mà nó hỗ trợ, sau đó RNC quyết định sẽ sử dụng UIA nào.

3.2.2.3. Sử dụng các hàm mật mã để tạo AV trong AuC

Vec-tơ nhận thực (AV) bao gồm các thông số: hô lệnh ngẫu nhiên (RAND); trả lời kỳ vọng từ người sử dụng (XRES); khóa mật mã (CK); khóa toàn vẹn (IK); và thẻ nhận thực mạng (AUTN). Hình 3.8. mô tả quá trình sử dụng các hàm mật mã để tạo ra các AV trong AuC

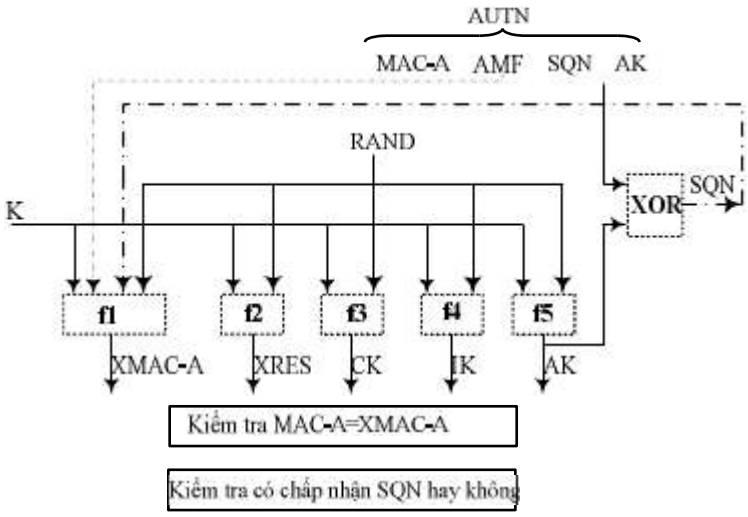
Như trên ta đã biết chức năng của các hàm mật mã. Hàm f0 tạo ra hô lệnh ngẫu nhiên (RAND). Hàm f1 với các thông số đầu vào là: RAND; trường quản lý nhận thực (AMF); số trình tự SQN và khóa chủ (K) được lưu sẵn trong AuC sẽ cho ra ở đầu ra mã nhận thực bản tin dành cho nhận thực (MAC-A), các hàm tiếp theo từ f2 đến f5 với cùng các thông số đầu vào là RAND và K sẽ cho ra ở đầu ra các thông số lần lượt như sau: XRES; CK; IK; AK. AK được tạo ra sau đó được XOR với SQN để tạo ra SQN $\oplus$ AK. Đến đây ta đã được đầy đủ các thông số của AV.



Hình 3.8. Quy trình tạo các AC trong AuC

3.2.2.4. Sử dụng các hàm mật mã để tạo các thông số an ninh trong USIM

Để tạo ra các khóa đầu ra trong USIM, nó chỉ có một trong số bốn thống số mà AuC có, đó là khóa chủ (K).Các thông số còn lại phải nhận từ AuC. Hình 3.9. mô tả quá trình tạo các thông số an ninh trong USIM.



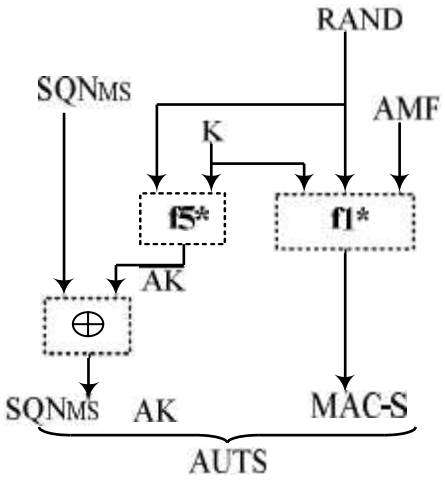
Hình3.9. Quy trình tạo các thông số trong USIM

Khi USIM nhận được cặp (RAND||AUTN), nó bắt đầu tạo ra khóa dấu tên (AK) bằng hàm f5 dựa trên số ngẫu nhiên RAND thu được. Bằng cách XOR AK với SQN ⊕ AK có được từ thẻ nhận thực AUTN ta thu được SQN_{HE} của AuC. Sau đó, hàm f1 được sử dụng với các đầu vào là K, RAND, AMF, SQN cho ra ở đầu ra mã nhận thực bản tin kỳ vọng (XMAC-A). Nó tiến hành

so sánh số này với MAC-A có trong AUTN. Nếu hai số này trùng nhau, USIM nhận thực rằng bản tin (cặp RAND||AUTN) nhận được từ chính HE đang quản lý nó. Quá trình được tiếp tục bằng các hàm tạo khóa khác. Nếu hai số này không trùng nhau thì bản tin "từ chối nhận thực của người sử dụng kèm theo nguyên nhân" được gửi trở lại VLR/SGSN. Nếu nhận thực thành công, USIM tiến hành kiểm tra SQN_{HE} có nằm trong dải của SQN_{MS}. Nếu số trình tự này nằm trong dải quy định, USIM sẽ tiến hành tạo ra các thông số tiếp theo bằng cách sử dụng các hàm f2 (tạo ra RES), f3 (tạo ra CK), f4 (tạo ra IK), f5 (tạo ra AK).

3.2.2.5. Sử dụng các hàm để đồng bộ lại tại USIM

Khi USIM nhận thấy chuỗi trình tự SQN_{HE} nhận được nằm ngoài dải của SQN_{MS}, các chức năng tạo khóa bình thường bị hủy và USIM bắt đầu tạo ra thẻ đồng bộ lại AUTS. Quá trình được miêu tả cụ thể trong hình 3.10.

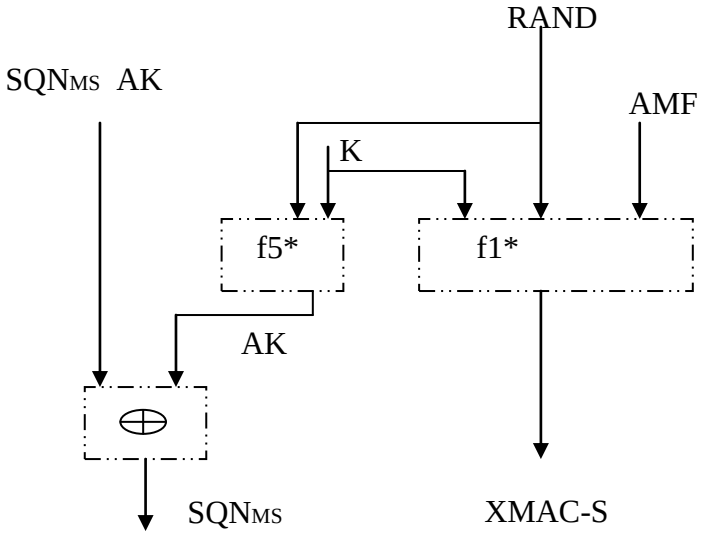


Hình 3.10. Tạo các AuTS trong USIM

Bằng hàm f1* với các thông số đầu vào là hô lệnh ngẫu nhiên (RAND), khóa chủ (K) và trường quản lý nhận thực (AMF, đặt bằng 0). Ta được ở đầu ra của hàm mã nhận thực bản tin đồng bộ lại (MAC-S). Tiếp theo hàm f5* được sử dụng với hai thông số đầu vào là K và RAND ta được thông số đầu ra là AK. AK được XOR với SQN_{MS} để tạo thành $SQN_{MS} \oplus AK$. Sau đó, $SQN_{MS} \oplus AK$ và MAC-S được ghép vào thẻ đồng bộ lại AUTS. Cuối cùng bản tin "sự cố đồng bộ" cùng với thông số AUTS được gửi tới VLR/SGSN. Các hàm f1* và f5* chỉ được sử dụng cho thủ tục đồng bộ lại. Các hàm này

được xây dựng sao cho các giá trị của chúng không làm lộ các hàm khác.

3.2.2.6 Sử dụng các hàm để đồng bộ lại tại AuC



Hình 3.11. Thủ tục đồng bộ tại AuCc

AuC nhận thực cặp RAND||AUTS từ VLR/SGSN và thực hiện thử tục đồng bộ lại. Quá trình được miêu tả trong hình 3.11.

Hàm f1* sử dụng các thông số đầu vào là K, AMF và RAND để tạo ra mã nhận thực đồng bộ lại kỳ vọng (XMAC-S). Sau đó, XMAC-S được so sánh với MAC-S, nếu trùng nhau thì thủ tục được tiếp tục diễn ra.

Hàm f5* sử dụng các thông số đầu vào là K và RAND để tạo ra khóa dấu tên (AK) và giá trị này được XOR với $SQN_{MS} \oplus AK$ ta thu được SQN_{MS} của USIM. AuC tiến hành so sánh hai số trình tự (SQN_{MS} với SQN_{HE}). Nếu nó nhận thấy AV được tạo ra tiếp theo sẽ được USIM tiếp nhận, nó sẽ gửi các AV này trở lại VLR/SGSN. Nếu không có AV nào nằm trong dải được USIM tiếp nhận, AuC phải đặt $SQN_{HE}=SQN_{MS}$. VLR/SGSN sẽ tạo ra XMAC-S và so sánh nó với MAC-S nhận được từ AUTS (thẻ nhận thực đồng bộ lại). Quá trình này được thực hiện để nhận thực thuê bao, nếu thành công số trình tự của AuC (SQN_{HE}) sẽ được đặt lại bằng giá trị SQN_{MS}. Sau đó, AuC tạo ra một tập các AV mới. Như đã nói ở trên, việc tạo ra nhiều AV trong thời gian thực có thể làm AuC quá tải. Vì thế có thể AuC chỉ gửi đến VLR/SGSN một AV trong lần gửi đầu tiên.

3.2.2.7 Thứ tự tạo khóa

Thứ tự tạo khóa có thể không được thực hiện như đã mô tả ở trên. Thứ tự được mô tả ở trên là logic, nhưng thực hiện có thể khác, nếu việc thực hiện này hiệu quả hơn. Điều quan trọng là các khóa phải sẵn sàng theo thứ tự trình bày ở trên.

3.2.3 Các thông số nhận thực

Các thông số được sử dụng trong thủ tục AKA bao gồm:

3.2.3.1 Các thông số của vec-tơ nhận thực (AV)

Các AV được tạo ra ở AuC và được tập trung gửi đến mạng phục vụ (SN), nơi chúng sẽ được sử dụng cho nhận thực. Khi nhận thực được thực hiện, các khóa mật mã và nhận thực của AV được lưu tại RNC. Các thông số của AV bao gồm: RAND, XRES, AUTN, CK, IK.

3.2.3.2 Thẻ nhận thực mạng (AUTN)

Thẻ nhận thực mạng được tạo ra tại AuC và được gửi cùng với RAND từ VLR/SGSN đến USIM. AUTN bao gồm: $SQN_{HE} \oplus AK||AMF||MAC\text{-}A$.

3.2.3.3 Trả lời của người sử dụng và giá trị kỳ vọng (RES&XRES)

RES được mạng sử dụng để nhận thực thuê bao. Trước hết XRES được tạo ra ở AuC và được gửi đến VLR/SGSN trong AV. Sau đó, USIM tạo ra RES (bằng hàm f2) và gửi nó đến VLR/SGSN, tại đây chúng được so sánh với nhau. Nếu chúng trùng nhau thì người sử dụng được nhận thực.

3.2.3.4 Mã nhận thực bản tin dành cho nhận thực và giá trị kỳ vọng (MAC-A&XMAC-A)

Hai thông số này được sử dụng trong AKA để USIM nhận thực mạng. USIM nhận được MAC-A trong AV và so sánh với XMAC-A do nó tạo ra bằng hàm f1. Nếu hai mã này trùng nhau thì mạng được USIM nhận thực.

3.2.3.5 Thẻ đồng bộ lại (AUTS)

AUTS được tạo ra ở USIM (bằng hàm f1*&f5*) khi SQN_{HN} không nằm trong dải của SQN_{MS}. Sau đó nó gửi AUTS (có kèm theo SQN_{MS}) đến AuC để tiến hành thủ tục đồng bộ lại.

3.2.3.6 Mã nhận thực bản tin dành cho đồng bộ lại và giá trị kỳ vọng (MAC-S&XMAC-S)

Hai thông số này được sử dụng để nhận thực USIM trước khi đặt lại số

trình tự của AuC. Khi USIM nhận ra sự cố đồng bộ, nó tạo ra MAC-S và gửi nó trong AUTS đến AuC. AuC tự tạo ra giá trị kỳ vọng XMAC-S và so sánh hai thông số này với nhau. Hai thông số này được tạo ra bằng hàm f1*. Nếu chúng trùng nhau, bản tin sự cố đồng bộ được nhận thực và SQN_{HE} được đặt vào vị trí của SQN_{MS}.

3.2.3.7 Kích cỡ của các thông số nhận thực

Dưới đây là bảng thống kê các thông số nhận thực với các kích cỡ kèm theo.

Thông số	Định nghĩa	Số bit
K	Khóa chủ (Master Key)	128
RAND	Hô lệnh ngẫu nhiên	128
SQN	Số trình tự	48
AK	Khóa nặc danh	48
AMF	Trường quản lý nhận thực	16
MAC	Mã nhận thực bản tin	64
CK	Khóa mật mã	128
IK	Khóa toàn vẹn	128
RES	Trả lời của người sử dụng	32-128
X-RES	Trả lời kỳ vọng của người sử dụng	32-128
AUTN	Thẻ nhận thực mạng	128
AUTS	Thẻ đồng bộ lại	96-128
MAC-I	Mã nhận thực bản tin cho toàn vẹn số liệu	32

Bảng 5. Bảng kích cỡ các thông số nhận thực

3.2.4. Mô hình an ninh cho giao diện vô tuyến 3G UMTS

Nhận thực ở 3G UMTS được thực hiện ở cả hai chiều: mạng nhận thực người sử dụng và ngược lại. Để làm được điều đó, mạng phải gửi đến UE một bản tin yêu cầu nhận thực có chứa mã nhận thực MAC-A. Sau đó, USIM sẽ tính toán con dấu kiểm tra nhận thực XMAC-A và so sánh hai mã này nếu trùng nhau thì quá trình nhận thực thành công.

Mật mã bản tin được thực hiện ở cả hai chiều bằng luồng khóa (KS). Tại RNC, KS được tạo ra từ khóa mật mã (CK)

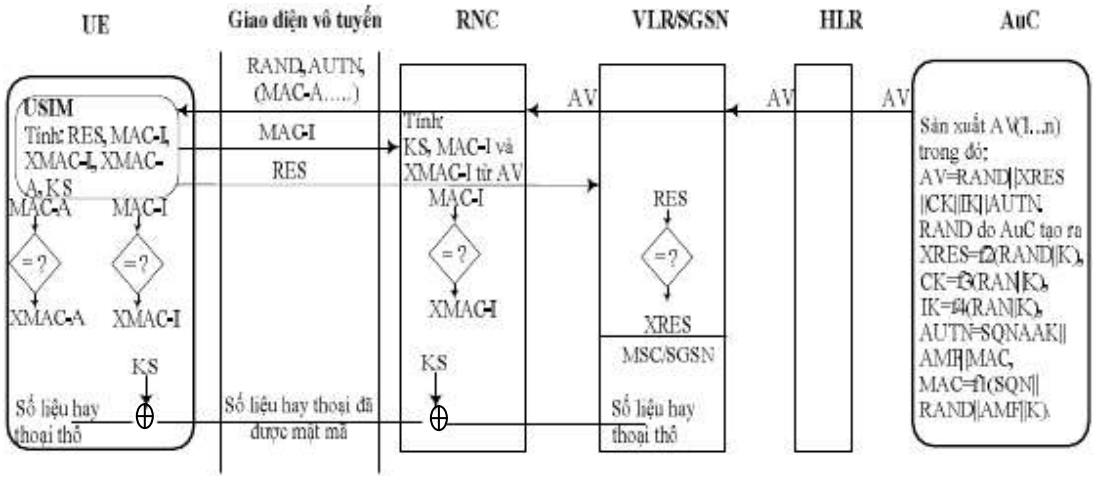
trong AV do AuC gửi xuống. Còn trong USIM, KS được tạo ra từ CK

mà CK lại được tính toán từ RAND và AUTN (do mạng gửi đến).

Bảo vệ toàn vẹn cũng được thực hiện ở cả hai chiều bằng nhận thực bản tin toàn vẹn, được truyền giữa RNC và UE. Để được nhận thực bản tin phát (từ UE hoặc RNC) phải được đóng dấu bằng mã nhận thực bản tin dành cho toàn vẹn (MAC-I). Phía thu (RNC hoặc UE) tính toán ra XMAC-I để kiểm tra.

Các thành phần quan trọng nhất liên quan đến an ninh là khóa chủ biết trước (K) và một số thông số khác được lưu trong USIM và AuC, chúng không bao giờ được truyền ra ngoài khỏi hai vị trí này. Cũng cần đảm bảo rằng các thông số nói trên đồng bộ với nhau ở cả hai phía.

Mô hình an ninh tổng quát cho giao diện vô tuyến ở 3G UMTS được minh họa ở hình 3.12.



Hình 3.12. Mô hình an ninh cho giao diện vô tuyến 3G UMTS

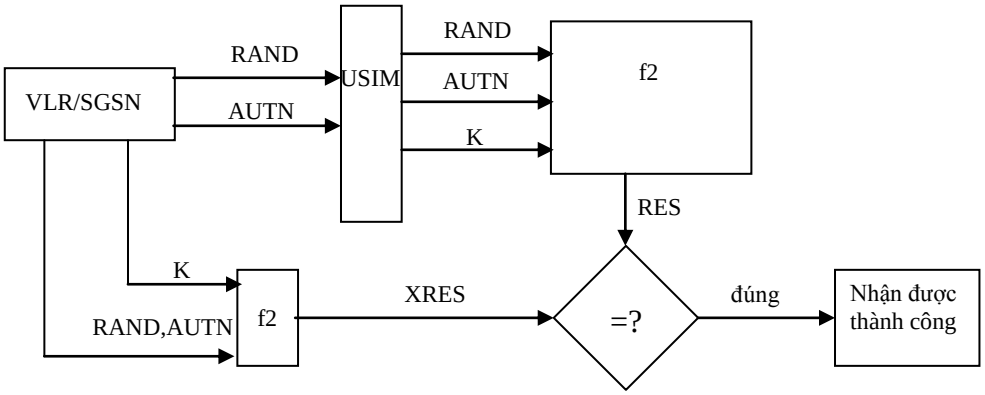
3.2.4.1 Mạng nhận thực người sử dụng

Để đảm bảo nhận thực mạng UMTS ta cần xét đến ba thực thể: VLR/SGSN; USIM; HE. VLR/SGSN kiểm tra nhận dạng thuê bao giống như ở GSM, còn USIM đảm bảo rằng VLR/SGSN được HE quản lý nó cho phép thực hiện điều này.

Nhận thực được thực hiện ngay sau khi mạng phục vụ (SN) nhận dạng thuê bao. Quá trình này được thực hiện khi VLR (trong miền CS) hoặc SGSN (trong miền PS) gửi yêu cầu nhận thực đến AuC. Tiếp đến VLR/SGSN gửi

bản tin yêu cầu nhận
thực người sử dụng đến UE. Trong bản tin này có chứa RAND và AUTN.

Khóa chủ (K) trong USIM sẽ được sử dụng kết hợp với hai thông số (RAND&AUTN) để tính toán ra thông số trả lời của người sử dụng (RES) bằng cách sử dụng hàm mật mã f2. RES có độ dài (32-128bit), sau khi được tạo ra ở USIM nó được gửi ngược trở lại VLR/SGSN. Tại đây nó được so sánh với giá trị kỳ vọng XRES do AuC tạo ra và gửi đến. Nếu hai thông số này trùng nhau, thì nhận thực thành công. Quá trình được mô tả ở hình 3.13.

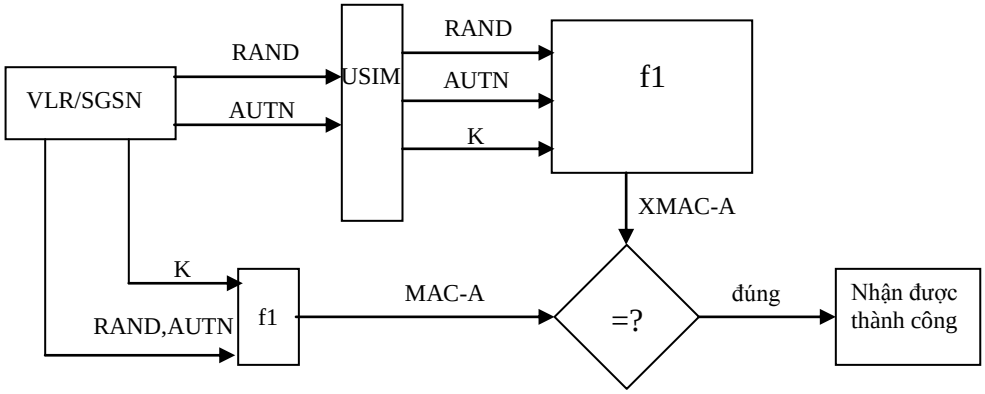


Hình 3.13. Nhận thực người sử dụng tại VLR/SGSN

3.2.4.2. USIM nhận thực mạng

Như trên đã nêu, để được nhận thực bởi USIM, mạng phải gửi đến USIM mã nhận thực bản tin dành cho nhận thực (MAC-A). Mã này có trong thẻ nhận thực mạng AUTN cùng với RAND mà mạng gửi đến. Sau đó USIM sẽ sử dụng hàm f1 với đầu vào là khóa chủ K cùng với AUTN và RAND để tính ra XMAC-A (giá trị kỳ vọng).

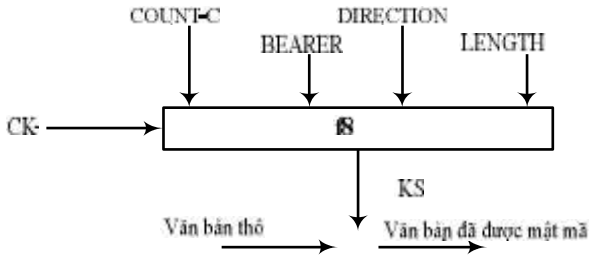
Tiếp đến nó tiến hành so sánh XMAC-A và MAC-A, nếu chúng giống nhau thì nhận thực thành công. Quá trình được minh họa ở hình 3.14.



Hình 3.14. Nhận thực tại mạng USIM

3.2.4.3. Mật mã hóa UTRAN

Sau khi nhận thực cả người sử dụng lẫn mạng (nhận thực qua lại) thành công, quá trình thông tin an ninh bắt đầu. Để cóthể thực hiện mật mã, cả hai phía phải thỏa thuận với nhau về giải thuật mật mã sẽ được sử dụng. Quá trình mật mã được thựchiện tại UE và RNC. Để thực hiện mật mã cả USIM lẫn RNC phải tạo ra các luồngkhóa (KS). Quá trình này được minh họa trong hình 3.15.



Hình 3.15. Bộ mật mã luồng khóa trong UMTS

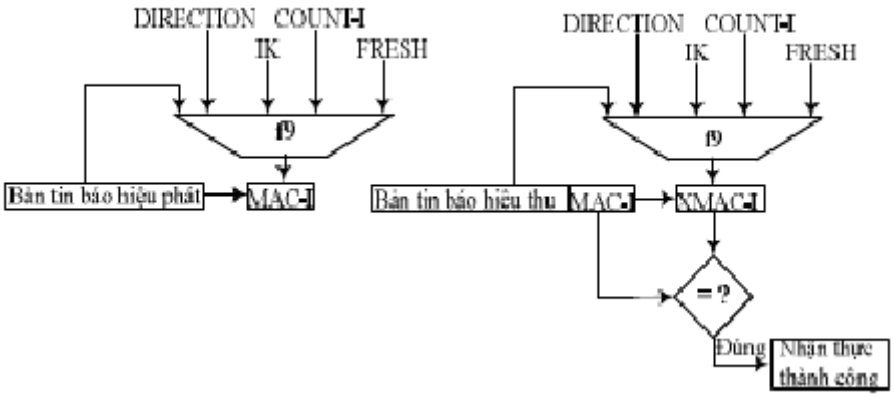
Theo đó ta thấy các thông số đầu vào của hàm f8 là: khóa mật mã (CK); số trình tự mật mã hóa (COUNT-C); nhận dạng kênh mang vô tuyến (BEARER); phương truyền (DIRECTION) và độ dài thực tế của luồng khóa (LENGTH). RNC nhận được CK trong vec-tơ nhận thực (AV) được gửi tới từ AuC. Còn tại USIM, CK được tính toán bằng hàm f3 với đầu vào là K và RAND nhận được từ mạng. Sau khi có được CK ở cả hai phía, RNC chuyển

vào chế độ mật mã bằng cách gửi đi lệnh an ninh RRC (kết nối tài nguyên vô tuyến) đến UE.

Trong quá trình mật mã UMTS, số liệu văn bản gốc được cộng từng bit với số liệu mặt nạ giả ngẫu nhiên của KS (hình 3.14). Ưu điểm lớn nhất của phương pháp này là có thể tạo ra số liệu mặt nạ trước khi nhận được văn bản thô. Vì thế quá trình mật mã hóa được tiến hành nhanh hơn. Quá trình giải mật mã được tiến hành theo cách tương tự như mật mã hóa, xong theo chiều ngược lại.

3.2.4.4. Bảo vệ toàn vẹn báo hiệu RRC

Mục đích của bảo vệ toàn vẹn là để nhận thực các bản tin điều khiển. Quá trình này được thực hiện trên lớp kết nối tài nguyên vô tuyến (RRC) giữa UE và RNC. Để nhận thực toàn vẹn bản tin, phía phát (USIM hoặc RNC) phải tạo ra mã nhận thực bản tin dành cho toàn vẹn (MAC-I), gắn vào bản tin đã được mật mã và gửi tới phía thu (RNC hoặc USIM). Tại phía thu mã XMAC-I được tính toán và so sánh với MAC-I nhận được. Nếu hai mã này trùng nhau thì bản tin được coi là toàn vẹn. Quá trình tạo ra MAC-I và XMAC-I được thực hiện bằng hàm f9 và được minh họa ở hình 3.16.



Hình 3.16. Nhận thực toàn vẹn bản tin.

Theo đó ta thấy các thông số đầu vào của hàm f9 bao gồm: bản tin báo hiệu thu/phát; phương truyền (DIRECTION); khóa toàn vẹn (IK); số trình tự mật mã (COUNT-I) và làm tươi (FRESH). Trong đó, thông số COUNT-I giống như bộ đếm được sử dụng để mật mã hóa, thông số FRESH được sử dụng để chống lại kẻ xấu chọn giá trị khởi đầu cho COUNT-I. RNC nhận

được IK và CK trong lệnh chế độ an ninh. Còn trong USIM, IK được tính bằng hàm f4 với thông số đầu vào là K và RAND do mạng gửi đến.

3.2.5. Nhận thực và thỏa thuận khóa AKA

Thủ tục nhận thực và thỏa thận khóa AKA được thực hiện khi:

Đăng ký người sử dụng trong mạng phục vụ: khi một thuê bao lần đầu tiên nối đến mạng phục vụ (mới bật máy hay di chuyển sang nước khác) nó phải tiến hành đăng ký với mạng phục vụ.

Sau mỗi yêu cầu dịch vụ: là khả năng để thuê bao ứng dụng các giao thức cao hơn vì thế phải thực hiện AKA.

Yêu cầu cập nhật vị trí: khi đầu cuối thay đổi vùng định vị nó cần cập nhật vị trí của mình vào HLR và VLR.

Yêu cầu đăng nhập và hủy đăng nhập: đây là các thủ tục kết nối và hủy kết nối thuê bao đến mạng phục vụ.

Yêu cầu thiết lập lại kết nối: yêu cầu này được thực hiện khi số lượng các nhận thực địa phương được thực hiện cực đại.

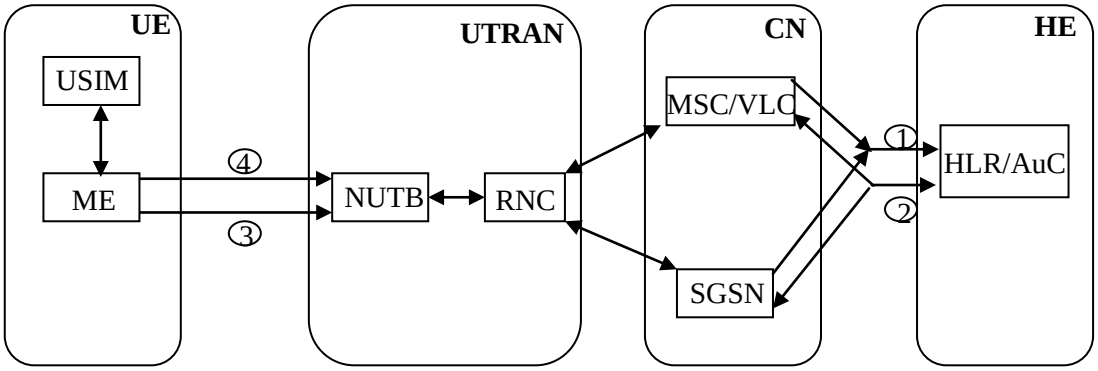
Yêu cầu thiết lập lại kết nối: yêu cầu này được thực hiện khi số lượng các nhận thực địa phương được thực hiện cực đại.

3.2.5.1. Tổng quan về AKA

Nhận thực và thỏa thuận khóa (AKA) là một trong các tính năng quan trọng của hệ thống 3G UMTS. Tất cả các dịch vụ khác đều phụ thuộc vào AKA, vì không thể sử dụng bất cứ dịch vụ nào cao hơn mà không phải nhận thực người sử dụng. Để thực hiện các quá trình này trong 3G UMTS, AuC phải tạo ra các vec-tơ nhận thực (AV) dựa trên bốn thông số: số ngẫu nhiên (RAND); khóa chủ (K); số trình tự (SQN) và trường quản lý nhận thực (AMF). AV nhận được sẽ bao gồm: mã nhận thực bản tin để nhận thực mạng (MAC-A); chữ ký kỳ vọng từ người sử dụng để nhận thực người này (X-RES), khóa mật mã (CK); khóa toàn vẹn (IK); khóa dấu tên (AK) và một số thông số khác được sử dụng để chống phát lại. Mạng cũng sẽ phát các thông số RAND và AUTN=(SQN $\oplus$ AK, AMF, MAC-A) đến USIM để nó tạo ra mã nhận thực bản tin kỳ vọng để nhận thực mạng(X-MACA), chữ ký để nhận thực nó với mạng (RES), CK, IK, AK và SQN.

3.2.5.2. Các thủ tục AKA

Hình 3.16 đã miêu tả cụ thể các quá trình nhận thực thỏa thuận khóa AKA.



Hình 3.17. Tổng quan quá trình nhận thực và thỏa thuận khóa AKA

Các thủ tục AKA xảy ra tại USIM, SGSN/VLR và HLR/AuC. Vì mạng phục vụ được chia thành các miền CS và PS. Các thủ tục được nhận thực giống nhau và độc lập trong cả hai miền.Tiếp theo chúng ta sẽ đi tìm hiểu quá trình nhận thực AKA được minh họa ở hình 3.17.

Nhận thực và thỏa thuận khóa AKA được quản lý bởi LR/SGSN mà thuê bao nối tới. Trước hết VLR/SGSN phụ trách máy di động gửi bản tin "yêu cầu số liệu nhận thực IMSI" đến HLR (1). Sau khi nhận được bản tin này HLR sẽ định vị tới AuC (nơi chứa số liệu thuê bao) và yêu cầu các AV từ trung tâm này. Nếu AuC đã lưu các AV cho thuê bao nó sẽ trả lời bằng cách gửi một hay nhiều AV trở lại VLR/SGSN (2). Thông thường nhiều AV được gửi đi một lần (có tới 5AV), nhờ vậy giảm bớt được số lần yêu cầu AuC và giảm thiểu lưu lượng mạng. Tuy nhiên, nếu tải AuC cao nó có thể chỉ gửi đi một AV. Nếu chưa có sẵn AV trong cơ sở dữ liệu của mình AuC sẽ tiến hành tạo ra các AV mới.

Sau khi đã nhận được các AV từ HLR gửi đến, VLR/SGSN sẽ lưu chúng trong cơ sở dữ liệu của mình và chọn một trong số chúng kèm theo hai thông số RAND và AUTN để gửi tới USIM trong bản tin gọi là "yêu cầu nhận thực RAND(i)||AUTN(i)" (3) thông qua UTRAN.

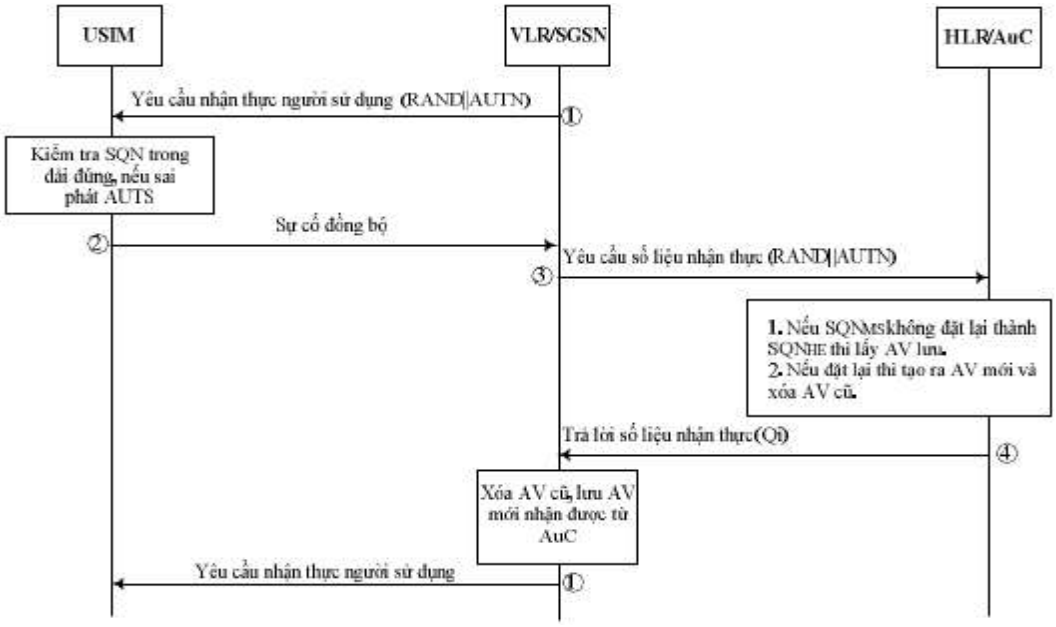
Sau khi nhận được bản tin này, USIM tiến hành kiểm tra thẻ nhận thực mạng AUTN để nhận thực mạng. Bằng cách mở thẻ AUTN ra và tiến hành so sánh MAC-A với XMAC-A do nó tạo ra. Nếu hai thông số này không trùng

nhau thì nhận thực mạng bị từ chối. Điều này có nghĩa là khóa chủ (K) ở cả hai miền không giống nhau. Vì thế bản tin này không bắt nguồn từ môi trường nhà (HE) của thuê bao. Khi đó, nó hủy thủ tục nhận thực mạng và gửi đi bản tin "từ chối nhận thực của người sử dụng, kèm theo lý do" về phía VLR/SGSN. Nhận được bản tin này VLR/SGSN gửi "báo cáo nhận thực thất bại kèm lý do" tới HLR. Và có thể khởi đầu lại các thủ tục AKA. Quá trình này được gọi là USIM từ chối trả lời. Nếu MAC-A và XMAC-A trùng nhau thì quá trình nhận thực mạng thành công.

Tiếp theo USIM tiến hành tạo ra các trả lời từ người sử dụng để nhận thực mạng (RES) và gửi nó ngược trở lại VLR/SGSN (4). Tại đây RES sẽ được so sánh với X-RES (có trong AV do HLR gửi đến). Nếu chúng giống nhau thì thuê bao được nhận thực. Như vậy hai nửa nhận thực đã hoàn tất. Khi đó VLR/SGSN nhận các khóa mật mã và toàn vẹn (CK, IK) từ AV và gửi chúng đến HE đang quản lý thuê bao. Các khóa này được sử dụng để mật mã hóa truyền thông và kiểm tra sự toàn vẹn của bản tin.

Tương tự như thế, USIM cũng đồng thời tạo ra các khóa này.

3.2.6. Thủ tục đồng bộ lại AK



Hình 3. 18. Thủ tục đồng bộ lại

VLR/SGSN gửi đi "yêu cầu nhận thực người sử dụng RAND(i)||AUTN(i)" đến USIM (1). Sau khi nhận được bản tin này USIM tiến hành kiểm tra tính xác thực của bản tin. Nếu đây là bản tin được tạo ra tại HE quản lý nó thì hai số trình tự SQN_{HE} và SQN_{MS} phải nằm trong một giải, nếu SQN_{HE} nằm ngoài dải của SQN_{MS} thì thủ tục đồng bộ lại được tiến hành. Khi đó USIM sẽ tạo ra một thẻ đồng bộ lại (AUTS) và gửi nó đến VLR/SGSN (2). Sau khi nhận được sự cố đồng bộ VLR/SGSN tìm một hô lệnh ngẫu nhiên thích hợp từ bộ nhớ của mình và bổ sung nó vào bản tin "yêu cầu số liệu nhận thực" và gửi bản tin này ("yêu cầu số liệu nhận thực RAND(i)||AUTS") đến HLR/AuC đang quản lý thuê bao (3). Khi AuC nhận được AUTS từ bản tin trên, nó tiến hành so sánh hai số trình tự. Nếu thấy rằng AV tạo ra tiếp theo có thể tiếp nhận được, nó sẽ gửi AV này đến VLR/SGSN (4). Nếu không có AV nào trong số các AV được lưu nằm trong dải được USIM tiếp nhận, AuC sẽ tiến hành kiểm tra sự toàn vẹn của bản tin. Quá trình này để đảm bảo rằng chính USIM muốn thủ tục đồng bộ lại, nếu nhận thực này thành công, chuỗi SQN_{HE} được đặt vào SQNMS. Sau đó, AuC sẽ xóa các AV cũ đồng thời tạo ra các AV mới. Vì việc tạo ra nhiều AV trong thời gian thực có thể chiếm tải lớn đối với AuC, nên có thể chỉ một AV được gửi đi trong lần trả lời đầu tiên. Khi đó, AV mới được gửi đến từ AuC sẽ được gắn thêm thông số Qi.

Khi VLR/SGSN nhận được các AV mới được gửi đến từ AuC, nó sẽ xóa tất cả các AV cũ để đảm bảo rằng các AV này không dẫn đến sự cố đồng bộ lại khác. Sau đó, VLR/SGSN lại thực hiện lại từ đầu thủ tục AKA bằng cách gửi "yêu cầu nhận thực người sử dụng RAND(i)||AUTN(i)" đến USIM (1)…..

Tiếp theo ta đi tìm hiểu về sử dụng lại các AV do USIM từ chối do kiểm tra số trình tự. Việc sử dụng lại các AV này cản trở mạng thực hiện AKA với sử dụng lặp lại một AV.

Tuy nhiên, việc sử dụng lại Av lại cần thiết, ví dụ khi VLR/SGSN gửi bản tin "yêu cầu nhận thực người sử dụng" đến USIM, nhưng lại không nhận được trả lời của USIM do mạng bị sự cố. Khi vượt quá thời gian tạm dừng để chờ trả lời, VLR/SGSN sẽ tìm cách gửi lại USIM cặp (RAND(i)||AUTN(i)) một lần nữa. Nếu thực chất USIM đã nhận được AV này lần đầu, nó coi rằng số trình tự nhận được nằm ngoài dải. Trong trường hợp này để khởi đầu thủ

tục đồng bộ lại, USIM khởi đầu bằng cách so sánh hô lệnh ngẫu nhiên vừa nhận được (RAND) với RAND nhận được trước đó. Nếu chúng trùng nhau, nó chỉ cần gửi đi trả lời của người sử dụng (RES) được lưu lại lần cuối cùng. Vì thế cần lưu tất cả các thông số được đặt ra tại USIM.

Trong 3G UMTS ngay cả khi thực hiện cuộc gọi khẩn cũng cần thực hiện thủ tục nhận thực. Nhưng nếu nhận thực bị sự cố (do không có USIM hoặc do không có thỏa thuận chuyển mạng) kết nối vẫn sẽ được thiết lập. Cuộc gọi sẽ chỉ bị hủy nếu bảo mật và toàn vẹn thất bại.

KẾT LUẬN

Hiện nay, thuật ngữ 3G đã không còn xa lạ với những tổ chức liên quan đến lĩnh vực viễn thông và cả những người sử dụng dịch vụ viễn thông trên toàn thế giới. Với những ưu điểm vượt trội về công nghệ và những dịch vụ tiện ích phong phú, phù hợp với nhu cầu người dùng, công nghệ 3G đã được đón nhận một cách nhanh chóng.

Sau một thời gian nghiên cứu, tìm hiểu em đã hoàn thành xong Đồ án "Công nghệ 3G và vấn đề an ninh bao mật". Nội dung được đề cập trong Đồ án là:

Chương 1. Tổng quát về các hệ thống thông tin di động nói về vấn đề lịch sử phát triển của hệ thông thông tin di động, các đặc điểm cơ bản của hệ thông thông tin di động, các đặc điểm truyền sóng, hệ thông thông tin di động thế hệ thư ba

Chương 2. Hệ thông thông tin di động thế hệ thứ ba nói về xu thế chung của công nghệ di động là phải đáp ứng nhu cầu ngày càng cao về chất lượng, dung lượng, tính tiện lợi, giá cả, tính đa dạng về dịch vụ của người sử dụng. Vì vậy sau khi tồn tại một thời gian thì các công nghệ 2G đã bộc lộ các điểm yếu là không thể đáp ứng được yêu cầu trên mà phải đợi đến công nghệ 3G.

Chương 3. Vấn đề bảo mật trong 3G. Phần 1 trình bày về năm yêu tố để thiết lập một môi trương an ninh, các đe dọa an ninh, các công nghệ an ninh.Phần 2 trinh bày về mô hình kiến trúc an ninh 3G UMTS, các hàm mật mã, các thông số nhận thực,nhận thực và thỏa thuận khóa AKA, thủ tục đồng bộ lại AKA

Cuối cùng, em xin gửi lời cảm ơn chân thành đến toàn thể các Thầy – Cô, các bạn và gia đình đã giúp đỡ, ủng hộ em rất nhiều trong suốt thời gian qua.

Đặc biệt, lời cảm ơn chân thành và sâu sắc nhất em xin được gửi tới thầy giáo ThS. Mai Văn Lập – người đã định hướng đề tài, cung cấp các tài liệu quan trọng và tận tình hướng dẫn, chỉ bảo em trong suốt quá trình hoàn thành Đồ án tốt nghiệp.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 25 tháng 10 năm 2010

NGÔ THỊ PHƯƠNG HOA

TÀI LIỆU THAM KHẢO

1. Vũ Đức Thọ(2001), tính toán mạng thông tin di động số, Nhà xuất bản giáo dục.
2. TS. Nguyễn Phạm Anh Dũng, Giáo trình thông tin di động thế hệ ba, Học viện Bưu chính viễn thông, Nhà xuất bản bưu điện.
3. Các tài liệu khác trên mạng.