ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KỸ THUẬT CÔNG NGHIỆP

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGHIÊN CỨU MỘT SỐ PHƯƠNG PHÁP BẢO MẬT MẠNG THÔNG TIN DI ĐỘNG 3G TẠI VIỆT NAM

Ngành: KỸ THUẬT ĐIỆN TỬ

Học viên: NGUYỄN AN THU

Người HD Khoa học: PGS.TS. NGUYỄN HỮU CÔNG

THÁI NGUYÊN – 2012

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC
KỸ THUẬT CÔNG NGHIỆP
----------ꕥ----------

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

LUẬN VĂN THẠC SĨ

Họ và tên học viên	**:**	Nguyễn An Thu
Ngày tháng năm sinh	**:**	Ngày 03 tháng 12 năm 1972
Nơi sinh	**:**	Bắc Ninh
Nơi công tác	**:**	Viễn thông Bắc Ninh
Cơ sở đào tạo	**:**	Trường Đại học Kỹ thuật Công nghiệp Thái Nguyên
Chuyên ngành	**:**	Kỹ thuật điện tử
Khóa học	**:**	K13- KTĐT

TÊN ĐỀ TÀI:

NGHIÊN CỨU MỘT SỐ PHƯƠNG PHÁP BẢO MẬT MẠNG THÔNG TIN DI ĐỘNG 3G TẠI VIỆT NAM

Người hướng dẫn khoa học: **PGS.TS. Nguyễn Hữu Công**
Phó Giám đốc Đại học Thái Nguyên

Ngày giao đề tài: ...../...../.....
Ngày hoàn thành: ...../...../.....

GIÁO VIÊN HƯỚNG DẪN **HỌC VIÊN**

PGS.TS. Nguyễn Hữu Công **Nguyễn An Thu**

BAN GIÁM HIỆU **KHOA SAU ĐẠI HỌC**

LỜI MỞ ĐẦU

Các mạng thông tin di động 3G đã và đang được triển khai rộng khắp ở Việt Nam cho phép người sử dụng với thiết bị đầu cuối có khả năng kết nối 3G và đăng ký sử dụng dịch vụ 3G có thể nhận được rất nhiều ứng dụng đa phương tiện như Video Call, Internet Mobile, Mobile TV, Mobile Broadband… Tuy nhiên, ở phần truy nhập vô tuyến, người sử dụng dịch vụ di động 3G thực hiện kết nối vô tuyến qua giao diện không gian, đây là một môi trường mở đồng nghĩa với việc trong môi trường này dễ dàng có các nguy cơ truy nhập trái phép so với môi trường hữu tuyến cố định. Mặt khác để cung cấp các dịch vụ và nội dung phong phú cho khách hàng, các nhà khai thác mạng di động cần thực hiện mở kết nối mạng của mình với các mạng dữ liệu, các mạng di động khác và mạng Internet công cộng.

Từ những nguyên nhân đó mà các mạng thông tin di động 3G không chỉ bị tác động bởi các tấn công trên đường truyền truy nhập vô tuyến giống như ở mạng truyền thống (Mạng 3G kế thừa đầy đủ các nguy cơ an ninh của cả công nghệ viễn thông thế hệ cũ (1G và 2G) và công nghệ truyền tải dữ liệu tốc độ cao trên nền IP) mà còn có thể bị tấn công bởi các loại Virus (Qua thống kê cho thấy có đến hơn 190 loại virus trên điện thoại di động, những con virus này có thể xóa sạch dữ liệu trên máy điện thoại hoặc làm rối loạn hoạt động của máy), các tấn công từ chối dịch vụ (DoS)…từ các Hacker hoặc các tổ chức phạm tội khác nhau. Kẻ tấn công sẽ khai thác các điểm yếu trong kiến trúc và các giao thức được sử dụng trong các mạng di động 3G để thực hiện các kiểu tấn công khác nhau, gây nguy hại có thể tới mức nghiêm trọng cho mạng của nhà khai thác cũng như khách hàng như làm tắc nghẽn mạng, từ chối dịch vụ, tràn ngập lưu lượng, gian lận cước, đánh cắp thông tin bí mật…

Các dịch vụ 3G hiện nay ở Việt Nam mới chỉ là cơ bản nên những vấn đề về an ninh bảo mật chưa bộc lộ nhiều. Nhưng trong tương lai, khi dịch vụ 3G phát triển mạnh thì những nguy cơ an ninh bảo mật như trên sẽ xuất hiện rất nhiều và gây thiệt hại rất lớn.

Với những lý do trên luận văn tiến hành phân tích, nghiên cứu mọi tấn công có thể nảy sinh gây nguy hại nghiêm trọng mà từ đó đề xuất các giải pháp về bảo mật trong mạng thông tin di động 3G. Do các vấn đề bảo mật trong hệ thống thông tin di động 3G là rất rộng và phức tạp, tác giả chưa có đủ điều kiện để nghiên cứu sâu và rộng toàn bộ mọi vấn đề (chẳng hạn: Nghiên cứu bảo mật ở miền người sử dụng, bảo mật miền ứng dụng cũng như thuật toán bí mật f8 và thuật toán toàn vẹn dữ liệu f9). Chính vì vậy luận văn gồm 3 chương như sau:

- Chương 1: Tổng quan về bảo mật và hệ thống thông tin di động 3G. Chương này nói về một số khái niệm, kiến trúc mạng 3G và kiến trúc bảo mật mạng 3G.

- Chương 2: Nghiên cứu các tính năng bảo mật. Trong chương này lần lượt nghiên cứu tính năng bảo mật ở miền truy nhập vô tuyến và tính năng bảo mật ở miền mạng. Cuối chương là nghiên cứu tìm hiểu thuật toán tạo khóa và nhận thực.

- Chương 3: Phân tích các tấn công và giải pháp bảo vệ mạng 3G tại Việt Nam: Phân tích các kiểu tấn công vào mạng di động 3G rồi từ đó đề xuất các phương pháp bảo vệ mạng mạng 3G.

Tuy nhiên các vấn đề mà luận văn đề cập trên lĩnh vực tương đối rộng, thông qua nhiều giao thức đặc biệt là các giao thức vô tuyến trong di động. Mặc dù tác giả đã nỗ lực hết sức, cố gắng vận dụng kiến thức, mọi khả năng, mọi điều kiện, nội dung luận văn chắc chắn còn nhiều thiếu sót và hạn chế. Rất mong nhận được những góp ý quý báu của người đọc để tác giả có thể hoàn thiện hơn.

Cuối cùng xin cám ơn bạn bè và người thân trong gia đình đã động viên quan tâm, giúp đỡ tôi hoàn thành khóa học và luận văn này.

Thái Nguyên, ngày tháng 11 năm 2012

CHƯƠNG I

TỔNG QUAN VỀ MẠNG DI ĐỘNG 3G VÀ BẢO MẬT

1.1TỔNG QUAN VỀ MẠNG DI ĐỘNG 3G

1.1.1. MẠNG DI ĐỘNG 3G

Hệ thống viễn thông di động toàn cầu (UMTS) được tiêu chuẩn hóa bởi 3GPP là một hệ thống di động thế hệ 3, tương thích với mạng GSM và GPRS. UMTS kết hợp các kỹ thuật đa truy nhập W-CDMA (IMT-2000 CDMA Direct Spread); CDMA 2000 (IMT-2000 CDMA Multi-Carrier) hoặc công nghệ CDMA TDD...

Hệ thống UMTS sử dụng công nghệ W-CDMA có một số đặc điểm sau: Mỗi kênh vô tuyến có độ rộng 5 MHz; tương thích ngược với GSM; chip rate 3,84 Mbps; hỗ trợ hoạt động không đồng bộ giữa các cell; truyền nhận đa mã; hỗ trợ điều chỉnh công suất dựa trên tỷ số tín hiệu/tạp âm; có thể áp dụng kỹ thuật anten thông minh để tăng dung lượng mạng và vùng phủ sóng (phiên bản HSPA từ Rel - 8 trở lên); hỗ trợ nhiều kiểu chuyển giao giữa các cell, bao gồm soft-handoff, softer-handoff và hard-handoff. UMTS cho phép tốc độ downlink là 0,384 Mbps (full mobility) và với phiên bản nâng cấp lên HSPA Release 6 hiện nay, tốc độ lên tới 14 Mbps (downlink) và 1,4 Mbps (uplink). Ở phiên bản HSPA Release 8 (thêm tính năng MIMO) thì tốc độ tương ứng sẽ là 42 Mbps & 11,6 Mbps.

Công nghệ IMT-2000 CDMA Multi-Carrier còn được gọi là IMT-MC hay CDMA2000 là công nghệ phát triển lên 3G từ họ CDMAOne (IS-95) bởi 3GPP2. CDMA2000 sử dụng các cặp sóng mang có độ rộng kênh 1,25 MHz. Phiên bản đầu tiên CDMA2000 1x (hay IS-2000) sử dụng 1 cặp kênh vô tuyến 1,25 MHz để chuyển tải 128 kênh lưu lượng, cung cấp tốc độ downlink 144 kB/s. Phiên bản CDMA2000 và CDMA2000 EV-DV sử dụng 3 kênh 1,25 MHz để tăng tốc độ. CDMA2000 EV-DV có tốc độ downlink lên đến 3,1 Mbps và uplink là 1,8 Mbps.

Họ công nghệ CDMA TDD bao gồm TD-CDMA và TD-SCDMA. TD-CDMA hay còn gọi là UMTS-TDD sử dụng chung một kênh vô tuyến 5 MHz cho

cả đường lên và đường xuống. Mỗi khung thời gian rộng 10ms chia thành 15 timeslot. Các timeslot được phân bổ cho đường lên và đường xuống theo một tỷ lệ cố định. Công nghệ truy cập CDMA được sử dụng trong mỗi timeslot để ghép kênh các dòng dữ liệu từ các tranceiver khác nhau. Công nghệ TD-CDMA chủ yếu được sử dụng để truy cập dữ liệu internet băng thông rộng, nó được dùng cho các pico-cell và micro-cell có nhu cầu dữ liệu lớn.

UMTS đã được tiêu chuẩn hóa ở một số phiên bản, bắt đầu từ phiên bản 1999 đến các phiên bản 4, phiên bản 5,….Mục tiêu chính là để cung cấp một dải rộng các ứng dụng đa phương tiện thời gian thực với các mức chất lượng dịch vụ khác nhau và các thuộc tính dịch vụ tiên tiến tới người sử dụng di động. Phiên bản UMTS Rel-4 và Rel-5 hướng tới kiến trúc mạng toàn IP, thay thế công nghệ truyền tải chuyển mạch kênh (CS) ở phiên bản 1999 bởi công nghệ truyền tải chuyển mạch gói (PS). Hơn nữa đây là một kiến trúc dịch vụ mở (OSA), cho phép các nhà khai thác mạng cung cấp cho bên thứ ba được truy nhập tới kiến trúc dịch vụ UMTS.

1.1.2. KIẾN THỨC CHUNG MẠNG THÔNG TIN DI ĐỘNG 3G

Một mạng UMTS được phân chia logic thành hai phần là mạng lõi (CN) và mạng truy nhập vô tuyến chung (GRAN). Mạng lõi tái sử dụng một số phần tử của mạng GPRS và mạng GSM, gồm 2 miền là miền kênh CS và miền gói PS. Miền CS được hình thành bởi các thực thể thực hiện phân bổ các tài nguyên dành riêng tới lưu lượng người sử dụng, điều khiển các tín hiệu khi các kết nối được thiết lập và giải phóng các kết nối khi các phiên kết thúc. Các thực thể trong miền PS thực hiện truyền tải dữ liệu người sử dụng ở dạng các gói được định tuyến độc lập nhau.

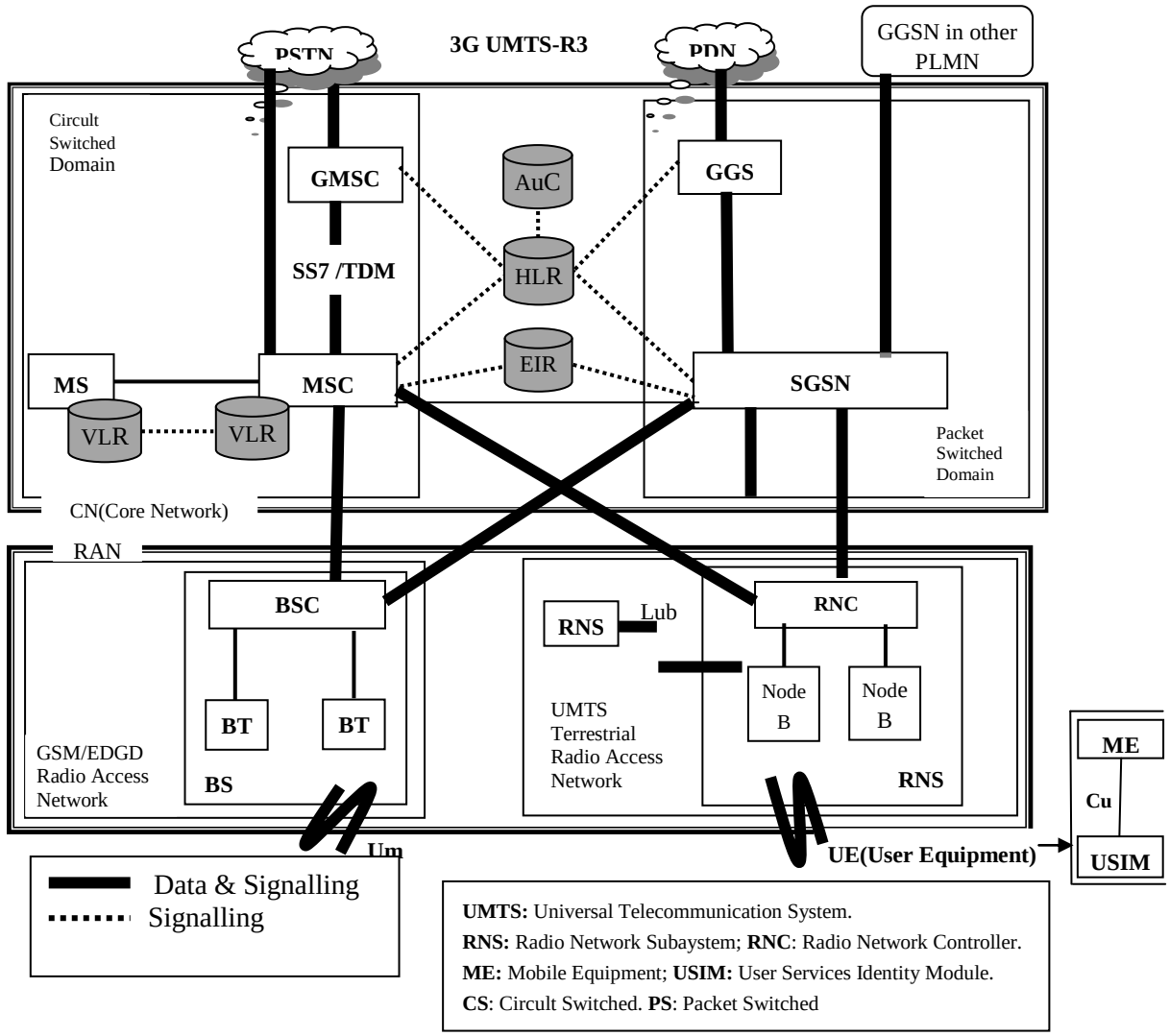
- Chuyển mạch kênh(CS): Là sơ đồ chuyển mạch trong đó thiết bị chuyển mạch thực hiện các cuộc truyền tin bằng các thiết lập kết nối chiếm một tài nguyên mạng nhất định trong toàn bộ cuộc truyền tin. Kết nối này là tạm thời, liên tục và dành riêng.

- Chuyển mạch gói (PS): Là sơ đồ chuyển mạch thực hiện phân chia số liệu của một kết nối thành các gói có độ dài nhất định và chuyển mạch các gói này theo thông tin về nơi nhận được gắn với từng gói và ở PS tài nguyên mạng chỉ bị chiếm dụng khi có gói cần truyền. Chuyển mạch gói cho phép nhóm tất cả các số liệu của

nhiều kết nối khác nhau phụ thuộc vào nội dung, kiểu hay cấu trúc số liệu thành các gói có kích thước phù hợp và truyền chúng trên một kênh chia sẻ.

Chuyển mạch gói có thể thực hiện trên cơ sở ATM hoặc IP.

+ ATM là công nghệ thực hiện phân chia thông tin cần phát thành các tế bào 53 byte để truyền dẫn và chuyển mạch. Một tế bào ATM gồm 5 byte tiêu đề và 48 byte tải tin. Thông tin định tuyến trong tiêu đề gồm đường dẫn ảo(VP) và kênh ảo(VC). Điều khiển kết nối bằng VC và VP cho phép khai thác và quản lý có khả năng mở rộng và có độ linh hoạt cao.



Hình 1.1: Kiến trúc mạng di động 3G

+ IP là một công nghệ thực hiện phân chia thông tin thành các gói được gọi là tải tin(Payload). Mỗi gói được gán một tiêu đề chứa các thông tin địa chỉ cần

thiết cho chuyển mạch. Trong thông tin di động do vị trí của đầu cuối di động nên cần phải có thêm tiêu đề bổ sung được gọi là đường hầm (Tunnel). Tunnel là một đường truyền mà tại đầu vào gói IP được đóng bao vào một tiêu đề mang địa chỉ nơi nhận và tại đầu ra gói IP được tháo bao bằng cách loại bỏ tiêu đề bọc ngoài. Có 2 cơ chế để thực hiện điều này là MIP(Mobile IP) và GTP (GPRS Tunnel Protocol).

Kiến trúc cơ bản của mạng UMTS được chi thành 3 phần (Hình 1.1) gồm: Máy di động (MS), mạng truy nhập (UTRAN) và mạng lõi (CN). Mạng truy nhập điều khiển tất cả các chức năng liên quan đến các tài nguyên vô tuyến và quản lý giao diện không gian, trong khi mạng lõi thực hiện các chức năng chuyển mạch và giao diện với các mạng bên ngoài.

1.1.2.1 Máy di động (MS)

MS được định nghĩa là một thiết bị cho phép người sử dụng truy nhập tới các dịch vụ của mạng và truy nhập tới module đặc tả thuê bao toàn cầu (USIM). MS liên quan đến bất kỳ thủ tục UMTS nào, quản lý và thiết lập cuộc gọi, các thủ tục chuyển giao và quản lý di động. Máy di động 3G có thể hoạt động một trong ba chế độ sau:

- Chế độ chuyển mạch kênh, cho phép MS chỉ được gắn với miền CS và chỉ được sử dụng các dịch vụ của miền CS.

- Chế độ chuyển mạch gói, cho phép MS chỉ được gắn với miền PS và chỉ được sử dụng các dịch vụ của miền PS, nhưng các dịch vụ của miền CS có thể được cung cấp trên miền PS.

- Chế độ PS/CS, trong đó MS được gắn với cả miền PS và CS và có khả năng sử dụng đồng thời các dịch vụ của miền PS và các dịch vụ của miền CS.

1.1.2.2 Mạng truy nhập (UTRAN)

UTRAN quản lý tất cả các chức năng liên quan đến các nguồn tài nguyên vô tuyến và quản lý giao diện không gian. UTRAN gồm 2 kiểu phần tử là các Node B và các bộ điều khiển mạng vô tuyến (RNC).

- Node B là đơn vị vật lý để thu/phát tín hiệu vô tuyến với các máy di động ở trong các tế bào của chúng. Mục tiêu chính của các Node B là thu /phát tín hiệu vô tuyến qua giao diện không gian và thực hiện mã hóa kênh vật lý CDMA. Node

B cũng đo lường chất lượng và cường độ tín hiệu của các kết nối và xác định tỷ lệ lỗi khung. Node B phát dữ liệu này tới RNC như là báo cáo kết quả đo để thực hiện chuyển giao và phân tập macro. Node B gồm các chức năng phát hiện lỗi trên các kênh truyền tải và chỉ thị tới các lớp cao hơn, điều chế/giải điều chế các kênh vật lý…

- Bộ điều khiển mạng vô tuyến (RNC): RNC quản lý các nguồn tài nguyên vô tuyến của mỗi một Node B mà nó điều khiển. RNC kết nối Node B tới mạng truyền tải. Nó đưa ra các quyết định chuyển giao yêu cầu báo hiệu tới MS. Các nguồn tài nguyên Node B được điều khiển từ RNC. Các chức năng điển hình của RNC là điều khiển tài nguyên vô tuyến, điều khiển sự nhận vào và sự phân bổ kênh, các thiết lập điều khiển công suất, điều khiển chuyển giao, phân tập macro và mật mã hóa. Một số nhiệm vụ khác của RNC bao gồm: xử lý lưu lượng tthoại và dữ liệu, chuyển giao giữa các tế bào, thiết lập và kết thúc cuộc gọi.

1.1.2.3 Mạng lõi (CN)

Mạng lõi CN đảm bảo việc truyền tải dữ liệu của người sử dụng đến đích. CN bao gồm việc sử dụng một số các thực thể chuyển mạch và các gateway (như MSC, Gateway MSC, SGSN và GGSN) tới các mạng bên ngoài (như mạng internet). CN cũng duy trì thông tin liên quan đến các đặc quyền truy nhập của người sử dụng (gồm AuC và EIR). Do đó, CN cũng gồm các cơ sở dữ liệu lưu giữ các profile người sử dụng và thông tin quản lý di động (HLR, VLR).

- Trung tâm chuyển mạch di dộng (MSC): Đây là phần tử chính miền mạng CS. MSC đóng vai trò là giao diện giữa mạng tế bào và các mạng điện thoại chuyển mạch kênh cố định bên ngoài. MSC thực hiện việc định tuyến các cuộc gọi từ mạng bên ngoài đến máy di động đơn lẻ và tất cả các chức năng chuyển mạch và báo hiệu cần thiết bởi các máy di động trong một vùng địa lý được định nghĩa như là vùng MSC.

- Bộ ghi định vị thường trú (HLR): HLR trong UMTS giống như HLR trong GSM, là một cơ sở dữ liệu lưu giữ dữ liệu liên quan đến mọi thuê bao di động sử dụng các dịch vụ được cung cấp bởi mạng di động. Có hai kiểu thông tin được lưu giữ ở HLR là các đặc tả cố định và tạm thời. Dữ liệu cố định không thay đổi trừ khi

một tham số thuê bao được yêu cầu phải biến đổi. Dữ liệu tạm thời thay đổi liên tục, nó thay đổi từ MSC điều khiển đến MSC khác, thậm chí thay đổi từ một tế bào này sang tế bào khác và từ cuộc gọi này sang cuộc gọi khác. Dữ liệu cố định gồm IMSI và một khóa nhận thực. Để định tuyến và tính cước các cuộc gọi HLR còn lưu giữ thông tin về SGSN và VLR nào hiện đang phụ trách người sử dụng.

- Bộ ghi định vị tạm trú (VLR): VLR nói chung được thực hiện trong một kết nối với MSC. VLR lưu giữ thông tin liên quan đến mọi máy di động thực hiện chuyển vùng tới một vùng mà máy di động điều khiển qua một MSC kết hợp. Do đó, VLR gồm thông tin về các thuê bao tích cực trong mạng của nó. Khi thuê bao đăng ký với các mạng khác, thông tin trong HLR của thuê bao được chép sang VLR ở mạng tạm trú và bị loại bỏ khi thuê bao rời mạng.

- Trung tâm nhận thực AuC: Lưu giữ toàn bộ số liệu cần thiết để nhận thực, mật mã hóa và bảo vệ sự toàn vẹn thông tin cho người sử dụng. AuC chỉ cung cấp thông tin về các vector nhận thực (AV) cho HLR. AuC lưu giữ khóa bí mật k cho từng thuê bao cùng với tất cả các hàm tạo khóa từ f0 đến f5. Nó tạo ra các AV cả trong thời gian thực khi SGSN/VLR yêu cầu hay khi tải xử lý thấp lẫn các AV dự trữ.

- Node hỗ trợ GPRS phục vụ (SGSN): SGSN quản lý tính di động và điều khiển các phiên gói IP. SGSN định tuyến lưu lượng gói của người sử dụng từ mạng truy nhập vô tuyến tới Node hỗ trợ GPRS Gateway ad hoc, node này cung cấp truy nhập tới các mạng dữ liệu gói bên ngoài. SGSN giúp điều khiển truy nhập tới các tài nguyên mạng, ngăn ngừa truy nhập bất hợp pháp tới mạng.

- Node hỗ trợ GPRS cổng (GGSN): GGSN là một gateway giữa mạng tế bào và các mạng dữ liệu gói như mạng Internet và các mạng Intranet.

1.2 TỔNG QUAN VỀ BẢO MẬT TRONG MẠNG 3G

1.2.1. HỆ THỐNG MẬT MÃ HOÁ

Mật mã học là khoa học về bảo mật và đảm bảo tính riêng tư của thông tin. Các kỹ thuật toán học được kiểm tra và được phát triển để cung cấp tính nhận thực, tính bí mật, tính toàn vẹn và các dịch vụ bảo mật khác cho thông tin được truyền thông, được lưu trữ hoặc được xử lý trong các hệ thống thông tin.