PHẠM TUẤN MINH

CÔNG NGHỆ THÔNG TIN

2005-2007

Hà Nội
2006

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

LUẬN VĂN THẠC SỸ KHOA HỌC

NGÀNH: CÔNG NGHỆ THÔNG TIN

NGHIÊN CỨU VẤN ĐỀ CHẤT LƯỢNG DỊCH VỤ VÀ AN TOÀN BẢO MẬT TRONG MẠNG WiMAX

PHẠM TUẤN MINH

HÀ NỘI 2006

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG

CÁC THUẬT NGỮ VÀ TỪ VIẾT TẮT

STT	Thuật ngữ	Giải nghĩa
1.	Access Service Network (ASN)	Mạng dịch vụ truy cập
2.	Access Service Network Gateway (ASN-GW)	Cổng mạng dịch vụ truy cập
3.	Admission Control (AC)	Kiểm soát cho phép
4.	Authentication, Authorization and Accounting (AAA)	Xác thực, uỷ quyền và kế toán
5.	Authentication Key (AK)	Khoá xác thực
6.	Base Station (BS)	Trạm cơ sở
7.	Best Effort Services (BE)	Dịch vụ cố gắng tốt nhất
8.	Common Part Sublayer (CPS)	Lớp con phần chung
9.	Connection Identifier (CID)	Định danh kết nối
10.	Connectivity Service Network (CSN)	Mạng dịch vụ kết nối
11.	Convergence Sublayer (CS)	Lớp con hội tụ
12.	Key Encryption Key (KEK)	Khoá mã hoá khoá
13.	Medium Access Control (MAC)	Lớp điều khiển truy cập phương tiện

STT	Thuật ngữ	Giải nghĩa
14.	Network Access Provider (NAP)	Nhà cung cấp truy cập mạng
15.	Network Access Server (NAS)	Server truy cập mạng
16.	Network Service Provider (NSP)	Nhà cung cấp dịch vụ mạng
17.	Non-Real-Time Polling Services (nrtPS)	Dịch vụ thăm dò không phải thời gian thực
18.	Real-Time Polling Services (rtPS)	Dịch vụ thăm dò thời gian thực
19.	Physical (PHY)	Lớp vật lý
20.	Policy Function (PF)	Chức năng chính sách
21.	Protocol Data Unit (PDU)	Đơn vị dữ liệu giao thức
22.	Reference Point (RP)	Điểm tham chiếu
23.	Security Sublayer	Lớp con bảo mật
24.	Service Access Point (SAP)	Điểm truy cập dịch vụ
25.	Service Data Unit (SDU)	Đơn vị dữ liệu dịch vụ
26.	Service Flow ID (SFID)	Định danh luồng dịch vụ
27.	Subscriber Station	Trạm thuê bao
28.	Traffic Encryption Key (TEK)	Khoá mã hoá lưu lượng
29.	Unsolicited Grant Services (UGS)	Dịch vụ cấp không phải yêu cầu

LỜI CẢM ƠN

Con xin bày tỏ lòng biết ơn sâu sắc đến cha mẹ và gia đình đã nuôi dưỡng, giáo dục và tạo điều kiện tốt nhất để cho con thực hiện đề tài này.

Em xin chân thành cảm ơn khoa Công nghệ Thông tin, quý Thầy, Cô trong Khoa, Trung tâm Đào tạo và Bồi dưỡng sau đại học, trường Đại học Bách Khoa Hà Nội đã tạo điều kiện cho chúng em học tập và thực hiện luận văn tốt nghiệp này.

Đặc biệt, em xin chân thành cảm ơn thầy giáo Nguyễn Thúc Hải, người đã trực tiếp tận tình hướng dẫn, giúp đỡ em hoàn thành đề tài này.

Em xin gửi lời cảm ơn chân thành tới các anh chị, bạn bè, đồng nghiệp đã động viên, giúp đỡ em trong quá trình thực hiện luận văn tốt nghiệp này.

Phạm Tuấn Minh

Tháng 11/2006

LỜI MỞ ĐẦU

Xu thế phát triển viễn thông hiện nay trên thế giới mang tính chất hội tụ, đáp ứng các nhu cầu thiết yếu và đòi hỏi của xã hội về tốc độ truyền tin, độ chính xác và sự đa dạng hoá các dịch vụ. Để đáp ứng các yêu cầu đó, nhiều công nghệ mới đã được nghiên cứu và ra đời như 3G, Wi-Fi, WiMAX,... Công nghệ đang được chú trọng quan tâm là WiMAX.

Công nghệ WiMAX (Worldwide Interoperability for Microwave Access) là công nghệ truy nhập vô tuyến băng rộng cho một vùng rộng dựa trên chuẩn IEEE 802.16 sử dụng băng tần thấp hơn 66 GHz bao gồm các phiên bản đòi hỏi và không đòi hỏi tầm nhìn thẳng. Mạng truy cập không dây băng thông rộng dựa trên công nghệ WiMAX (gọi tắt là mạng WiMAX) cung cấp các dịch vụ đa phương tiện trên nền IP như điện thoại có hình ảnh, điện thoại di động, truyền dữ liệu tốc độ cao, truyền hình theo yêu cầu,... WiMAX có ưu thế vượt trội so với các công nghệ cung cấp dịch vụ băng thông rộng hiện nay về tốc độ truyền dữ liệu và giá cả thấp do cung cấp các dịch vụ trên nền IP.

Trên thế giới, mạng WiMAX đang được tiến hành thử nghiệm tại nhiều nước, tập trung cho vùng thưa dân cư, dịch vụ cung cấp chủ yếu là truy cập Internet băng rộng cố định. Theo đánh giá của Maravedis Inc, thị trường viễn thông băng rộng có tốc độ tăng trưởng bình quân hàng năm 30%. Việc xuất hiện một công nghệ mới như WiMAX cho phép triển khai nhanh dịch vụ với giá cả thấp sẽ làm bùng nổ thị trường trong những năm tới.

Tại Việt Nam, hiện tại có 4 doanh nghiệp được cấp phép thử nghiệm mạng WiMAX. Việc cấp phép thiết lập mạng WiMAX cung cấp dịch vụ viễn thông sẽ được xem xét sau khi đánh giá các báo cáo kết quả thử nghiệm.

WiMAX là một công nghệ hoàn toàn mới mẻ và chưa được triển khai rộng rãi. Các chuẩn vẫn đang được xây dựng, hoàn thiện và vẫn còn nhiều vấn đề được các nhà nghiên cứu, triển khai quan tâm. Hai vấn đề được chú trọng là chất lượng dịch vụ và an toàn bảo mật của mạng WiMAX.

Nhiệm vụ của luận văn là nghiên cứu vấn đề chất lượng dịch vụ và an toàn bảo mật trong mạng WiMAX. WiMAX định nghĩa hai chế độ hoạt động là PMP và Mesh. Các nghiên cứu trong phạm vi đề tài tập trung nghiên cứu chế độ PMP, chế độ được ứng dụng phổ biến. Nội dung chủ yếu của đề tài được tóm tắt trong 4 chương:

- Chương 1: Tổng quan về mạng WiMAX

Trong chương này, đầu tiên chúng ta sẽ tìm hiểu về khái niệm, ứng dụng của WiMAX, các phiên bản WiMAX, chứng nhận sản phẩm WiMAX và sự phát triển của công nghệ WiMAX. Sau đó, chúng ta sẽ tìm hiểu về bộ chuẩn 802.16. Các nghiên cứu về chuẩn 802.16 nếu không chỉ rõ thì đó là chuẩn 802.16-2004. Cuối cùng, chúng ta sẽ tìm hiểu về xu hướng phát triển mạng không dây băng thông rộng.

- Chương 2: Kiến trúc mạng WiMAX

Trong chương này, chúng ta sẽ nghiên cứu mô hình lý thuyết của kiến trúc mạng WiMAX mà diễn đàn WiMAX đưa ra, các đặc điểm khi triển khai và cấu trúc của bản tin điều khiển giữa các thực thể chức năng trong mô hình.

- Chương 3: Vấn đề chất lượng dịch vụ

Chúng ta sẽ tìm hiểu về mô hình các thực thể chức năng đảm bảo chất lượng dịch vụ do diễn đàn WiMAX đưa ra. Sau đó, nghiên cứu về cơ chế đảm bảo chất lượng dịch vụ mà IEEE 802.16-2004 hỗ trợ. Cuối cùng, chúng ta tập trung phân tích hoàn thiện cơ chế đảm bảo chất lượng dịch vụ của IEEE 802.16 với chế độ hoạt động PMP và sử dụng ghép kênh theo thời gian, đề xuất cơ chế kiểm soát cho phép và đề xuất phương pháp để áp dụng thuật toán

DRR vào việc lập lịch gói tin đường lên.

- Chương 4: Vấn đề an toàn bảo mật

Chúng ta sẽ tìm hiểu về mô hình các thực thể chức năng đảm bảo an toàn bảo mật do diễn đàn WiMAX đưa ra. Sau đó, nghiên cứu về cơ chế đảm bảo an toàn bảo mật mà IEEE 802.16-2004 hỗ trợ. Cuối cùng, chúng ta tập trung phân tích những ưu điểm mà IEEE 802.16-2004 đã khắc phục từ những hạn chế an toàn bảo mật của IEEE 802.11, những điểm yếu còn tồn tại của IEEE 802.16-2004, những đề xuất khắc phục hạn chế, cũng như xem xét những cải tiến mới nhất mà IEEE 802.16e-2005 đã bổ sung hoàn thiện.

Chương 1.
TỔNG QUAN VỀ MẠNG WiMAX

1.1 Công nghệ WiMAX

1.1.1 Khái niệm và ứng dụng của WiMAX

Khái niệm về WiMAX được diễn đàn WiMAX đưa ra là: WiMAX là một công nghệ dựa trên các chuẩn cho phép chuyển truy cập băng thông rộng không dây thay thế cho băng thông rộng có dây như cáp và DSL. WiMAX cho phép cung cấp kết nối băng thông rộng không dây cố định và di động.

Hệ thống WiMAX có khả năng cung cấp băng thông lớn (134,4 Mbp/s trong kênh 28 MHz), khoảng cách truyền xa (50 km), không đòi hỏi tầm nhìn thẳng, làm việc bình thường khi thiết bị người dùng di chuyển với tốc độ 120km/h, hiệu quả sử dụng phổ cao và chi phí thấp. ([12], trang 21)

Công nghệ WiMAX sử dụng các dạng của kỹ thuật điều chế OFDM. OFDM được đánh giá là một công nghệ dẫn đầu cho việc cung cấp kết nối không dây băng thông rộng. Do tốc độ của các dịch vụ không dây tăng vì thế đòi hỏi nhiều phổ sóng vô tuyến. Điều này dẫn tới việc xin cấp dải phổ sẽ khó khăn và sẽ phải trả chi phí cao. Vì vậy hiệu quả phổ, số lượng bít được mã thành một chu kỳ sóng vô tuyến đơn, trở nên rất quan trọng. Các công nghệ dựa trên OFDM, bao gồm WiMAX, có hiệu quả sử dụng phổ cao khoảng 4bps/Hz so với 802.11d dưới 2bps/Hz. ([8], trang 29)

OFDM thực hiện cắt đoạn phổ khả dụng bởi tần số và mang một phần dữ liệu trên mỗi tần số đó. Mỗi tần số đó là duy nhất và không chồng nhau. Điều này đảm bảo không có giao nhau giữa các âm. Kỹ thuật này đi cùng với các cải tiến phức tạp khác trong xử lý tín hiệu số đã đưa ra một công nghệ mạng nhanh và hiệu quả.

Công nghệ WiMAX là giải pháp cho nhiều kiểu ứng dụng băng thông rộng tại cùng thời điểm bao gồm các dịch vụ dữ liệu, tiếng nói và truyền hình. WiMAX hỗ trợ đảm bảo chất lượng dịch vụ, truyền khoảng cách xa, tốc độ

cao thích hợp với các ứng dụng truy cập băng thông rộng cố định trong các vùng nông thôn, đặc biệt khi khoảng cách xa mà DSL và cáp không tới được cũng như các vùng thành phố, ngoại ô ở các nước đang phát triển. Bên cạnh các dịch vụ cho hộ gia đình như Internet tốc độ cao, điện thoại VoIP, truyền hình là các dịch vụ cho các doanh nghiệp như hội nghị truyền hình, giám sát truyền hình, mạng riêng ảo,...

1.1.2 Các phiên bản WiMAX

Tổ chức thực hiện đẩy nhanh sự triển khai WiMAX và xây dựng chứng chỉ WiMAX nhằm đảm bảo sự tương thích, khả năng phối hợp hoạt động của các sản phẩm sử dụng chuẩn IEEE 802.16 với sản phẩm khác là diễn đàn WiMAX. Diễn đàn được thành lập vào tháng 6 năm 2001. Hiện tại diễn đàn có hơn 350 thành viên là các nhà sản xuất thiết bị, nhà cung cấp dịch vụ, nhà tích hợp hệ thống hàng đầu trên thế giới. Diễn đàn làm việc chặt chẽ với các nhà cung cấp dịch vụ và nhà sản xuất để đảm bảo rằng các hệ thống chứng chỉ của diễn đàn WiMAX thỏa mãn các yêu cầu của người sử dụng và tổ chức chính phủ. ([19], WiMAX Forum Overview)

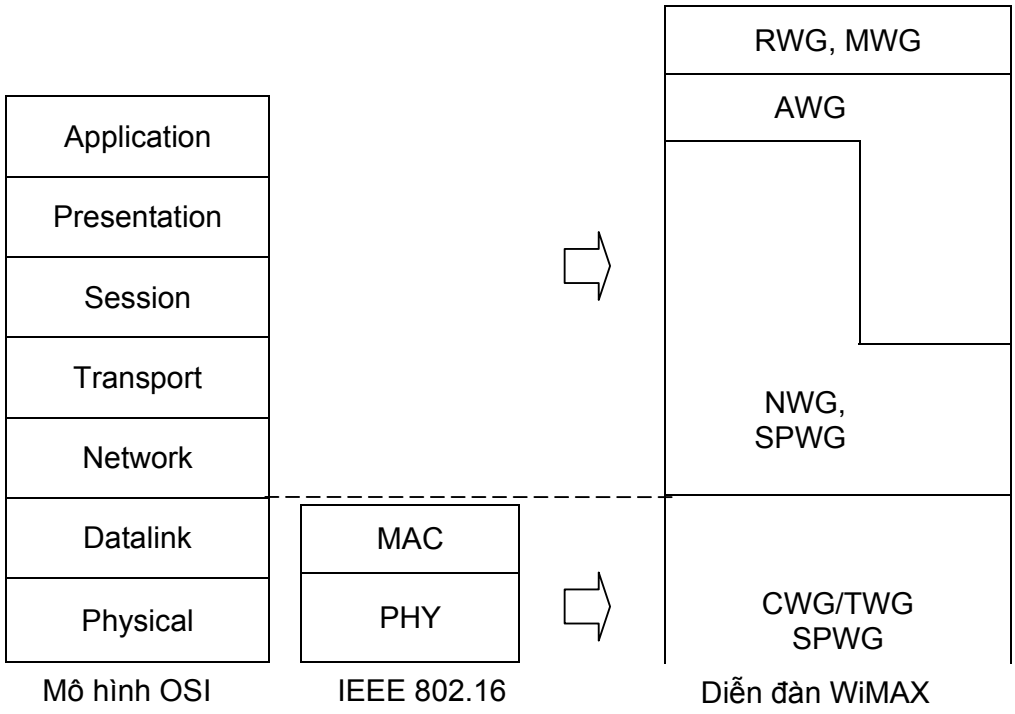
Diễn đàn WiMAX có 7 nhóm làm việc: RWG, MWG, AWG, NWG, SPWG, CWG, TWG. Nhiệm vụ các nhóm là:

- RWG (Regulatory Working Group): Đảm bảo khả năng cung cấp và sự hài hoà về dải phổ hoạt động trên thế giới, khuyến khích sự chấp nhận một băng tần duy nhất. Làm việc với các nhà cung cấp băng tần để phát triển khung các băng tần. Điều này cho phép các nhà cung cấp dịch vụ triển khai hầu hết các giải pháp trên các thị trường.
- MWG (Marketing Working Group): Cung cấp các thông tin về truy

cập băng thông rộng, tạo dựng hình ảnh cho các sản phẩm được chứng nhận bởi diễn đàn WiMAX, quảng bá chương trình chứng nhận của diễn đàn WiMAX, tạo dựng hình ảnh diễn đàn WiMAX là tổ chức hàng đầu về công nghệ không dây băng thông rộng..

- AWG (Application Working Group): Mô tả và chứng minh các giải pháp khả thi nhất đối với người sử dụng và đảm bảo các ứng dụng đó tương thích với công nghệ đã có cũng như khai thác khả năng của WiMAX.
- NWG (Networking Working Group): Xây dựng đặc tả mạng cho hệ thống WiMAX dựa trên chuẩn 802.16, xây dựng mô hình kiến trúc tham chiếu dựa theo các đặc tả yêu cầu từ SPWG.
- SPWG (Service Provider Working Group): Thiết lập một khung cho các nhà cung cấp dịch vụ cung cấp các phản hồi tới tất cả các nhóm làm việc khác trong diễn đàn WiMAX. Nhóm này có vai trò: Định nghĩa các yêu cầu cho kiến trúc mạng dựa trên chuẩn IEEE 802.16, phát triển các mô hình kinh doanh cho các sản phẩm được chứng nhận bởi diễn đàn WiMAX, định nghĩa các đặc tả chức năng cho các chuẩn IEEE 802.16 trong tương lai.
- CWG (Certification Working Group): Đánh giá kiểm tra, lựa chọn các test lab, quản lý sự liên hệ giữa các test lab, quản lý chương trình chứng nhận của diễn đàn WiMAX. Nhóm này có liên hệ chặt chẽ với TWG.
- TWG (Technical Working Group): Thống nhất sự tương thích và phối hợp hoạt động của các sản phẩm được chứng nhận bởi diễn đàn WiMAX. Phát triển các đặc tả đảm bảo sự tương thích và khả năng phối hợp hoạt động dựa trên các chuẩn quốc tế. Xây dựng các hệ thống chứng nhận và kiểm tra.

Hình 1.1 minh hoạ phạm vi hoạt động của các nhóm làm việc trong diễn đàn WiMAX.



Hình 1.1 Phạm vi của hoạt động của IEEE 802.16 và diễn đàn WiMAX

Diễn đàn WiMAX cam kết sẽ cung cấp giải pháp tối ưu cho truy cập không dây băng thông rộng cố định, có khả năng di chuyển và di động. Hai phiên bản của WiMAX giải quyết các yêu cầu truy cập khác nhau ([10], trang 2):

- WiMAX cố định. Phiên bản này dựa trên chuẩn 802.16-2004 của chuẩn IEEE 802.16 và dựa trên ETSI HiperMAN. Nó sử dụng OFDM và hỗ trợ truy cập cố định và di chuyển trong môi trường LOS và NLOS. LOS là chế độ truyền đòi hỏi tầm nhìn thẳng nghĩa là điểm thu và điểm phát nhìn thấy nhau theo đường thẳng. NLOS là chế độ truyền không đòi hỏi tầm nhìn thẳng. Bảng mô tả ban đầu diễn đàn xây dựng là cho băng tần 3,5 GHz và 5,8 GHz.

- WiMAX di động. Phiên bản này dựa trên bản bổ sung 802.16e, hỗ trợ thêm tính di động. Nó sử dụng OFDMA, một kỹ thuật điều chế đa mang sử dụng sự tạo kênh con. Các nhà cung cấp dịch vụ triển khai WiMAX di động cũng có thể sử dụng phiên bản này để cung cấp các dịch vụ cố định.

Hai phiên bản này cùng tồn tại và đáp ứng yêu cầu phát triển truy cập băng thông rộng không dây trong thị trường cố định và di động. Khi chọn một giải pháp, nhà cung cấp cần đánh giá các yếu tố như thị trường cung cấp, phổ khả dụng và thời gian triển khai. Các sản phẩm WiMAX cố định ít phức tạp hơn các phẩm WiMAX di động. Sản phẩm WiMAX cố định có thể sử dụng với dải băng tần không đăng ký rộng, thời gian triển khai nhanh và thường có thông lượng cao hơn các thiết bị dựa trên WiMAX di động. Ngược lại, các sản phẩm WiMAX di động hỗ trợ di động, cải tiến độ bao phủ và quản lý linh hoạt tài nguyên phổ.

1.1.3 Chứng nhận sản phẩm WiMAX

Diễn đàn WiMAX xây dựng các bản mô tả hệ thống (system profile) cho mỗi phiên bản WiMAX. Trong khi 802.16 hỗ trợ một dải tần số rộng (tới 66 GHz), độ rộng của kênh từ 1,25 MHz tới 20 MHz, các bản mô tả hệ thống thu hẹp phạm vi của 802.16 tập trung vào các cấu hình cụ thể. Sự lựa chọn một số giới hạn các bản mô tả nhằm đảm bảo khả năng phối hợp giữa các sản phẩm của các nhà sản xuất khác nhau, tiết kiệm số lượng cấu hình làm giảm chi phí, công nghệ dễ đi vào thực tiễn hơn. Sự lựa chọn này được xác định dựa vào yêu cầu thị trường, phổ khả dụng, các dịch vụ được yêu cầu và phụ thuộc vào lựa chọn của nhà cung cấp. Ví dụ, sự khả dụng của phổ cho các dịch vụ truy cập không dây băng thông rộng trong nhiều nước thúc đẩy việc xây dựng bản

mô tả đầu tiên trong băng tần 3,5 GHz.

Bản mô tả chứng nhận (certification profile) là một tập con của các bản mô tả hệ thống. Diễn đàn WiMAX xây dựng các giấy chứng nhận dựa trên từng bản mô tả chứng nhận cho các sản phẩm được kiểm tra. Các bản mô tả chứng nhận này được đưa ra bởi nhóm làm việc chứng nhận (Certification Working Group) và được phê chuẩn bởi diễn đàn WiMAX. Chi tiết về các bản mô tả chứng nhận cho WiMAX cố định mô tả trong bảng 1.1 và cho WiMAX di động mô tả trong bảng 1.2.

Bảng 1.1 Các bản mô tả chứng nhận cho WiMAX cố định

Băng tần (MHz)	Độ rộng kênh (MHz)	Phương pháp ghép kênh
3400-3600	3,5	TDD
3400-3600	3,5	FDD
3400-3600	7	TDD
3400-3600	7	FDD
5725-5859	10	TDD

(Nguồn: [10], trang 6)

Bảng 1.2 Các bản mô tả chứng nhận cho WiMAX di động

Băng tần (GHz)	Độ rộng kênh (MHz)	Phương pháp ghép kênh
2,3-2,4	8,75	TDD
2,3-2,4	5 10	TDD
2,305-2,320 2,345-2,360	3,5	TDD
2,305-2,320 2,345-2,360	5	TDD
2,305-2,320 2,345-2,360	10	TDD
2,496-2,69	5 10	TDD
3,3-3,4	5	TDD
3,3-3,4	7	TDD

(Nguồn: [17], trang 6)

Quá trình chứng nhận bao gồm việc kiểm tra khả năng hoạt động phối hợp với các sản phẩm từ các nhà sản xuất khác và kiểm tra tính tương thích với các bản mô tả chứng nhận WiMAX. Sản phẩm đầu tiên của WiMAX di động đạt chứng nhận của diễn đàn WiMAX dự kiến sẽ có vào khoảng đầu năm 2007.

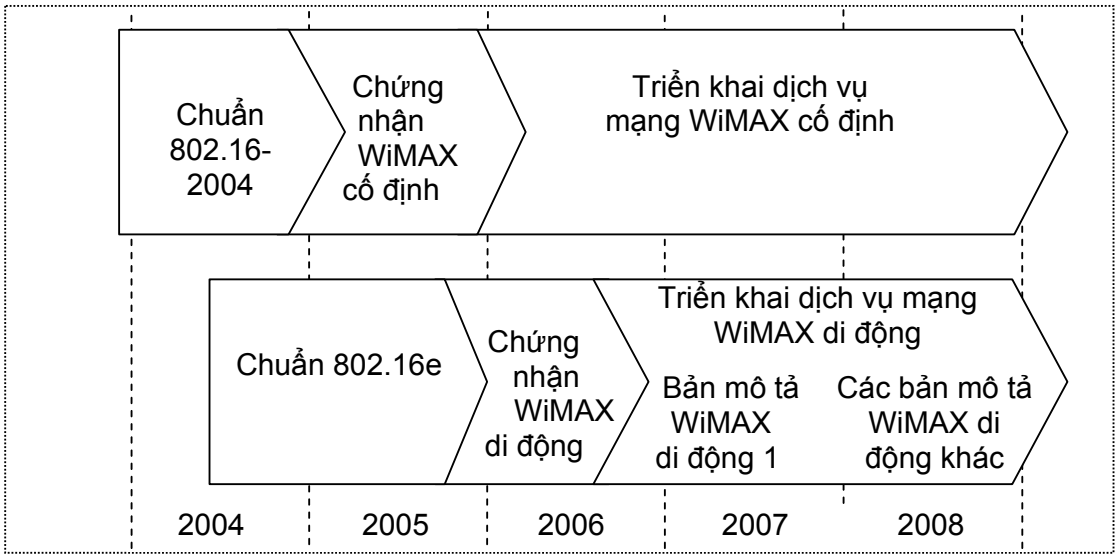
1.1.4 Sự phát triển của công nghệ WiMAX

Một dải các công nghệ được đặt tên WiMAX bao gồm các công nghệ tương tự như chuẩn IEEE 802.16. Trong khi chuẩn 802.16 và các mở rộng của nó vẫn tiếp tục được hoàn thành, một số nhà sản xuất đã đưa ra các công nghệ được thiết kế cho thị trường băng thông rộng.

Samsung và LG Electronics của Hàn Quốc đã phát triển một công nghệ kiểu WiMAX gọi là WiBro cho truy cập băng thông rộng không dây. Công nghệ này được thiết kế cho băng tần 2,3GHz, cung cấp tốc độ từ 512Kbp/s tới 1024Kbp/s và cho phép người sử dụng di chuyển tốc độ phương tiện giao thông (khoảng 60 km/h). Hệ thống này được hỗ trợ của chính phủ Hàn Quốc, là công nghệ ứng dụng riêng cho Hàn Quốc. WiBro không được các nhà đầu tư chấp nhận như một chuẩn công nghệ. Tại thời điểm này, Hàn Quốc hướng tới việc phát triển WiBro dựa trên 802.16e. ([8], trang 29)

Viện tiêu chuẩn Truyền thông Châu Âu (ETSI) cũng phát triển chuẩn cho truy cập không dây băng thông rộng có tên gọi là HiperMAN. Giống WiBro và các công nghệ khác, hệ thống này cho phép truyền với khoảng cách xa và băng thông rộng (280 Mbp/s trên một BS). ([8], trang 29)

Diễn đàn WiMAX làm việc với HiperMAN, WiBro, IEEE 802.16 để đảm bảo khả năng phối hợp hoạt động giữa các hệ thống này. Chi tiết về kế hoạch thời gian phát triển dự kiến của công nghệ WiMAX như trong hình 1.2.



Hình 1.2 Con đường phát triển của công nghệ WiMAX

(Nguồn: [11], trang 50)

Tóm lại, trong phần này chúng ta đã tìm hiểu chung về các vấn đề liên quan tới công nghệ WiMAX như khái niệm công nghệ WiMAX, ứng dụng của công nghệ WiMAX, hệ thống chứng nhận WiMAX,... Trong các phần tiếp theo của chương này, chúng ta sẽ tìm hiểu về chuẩn 802.16 và về các công nghệ mạng không dây băng thông rộng khác cùng xu hướng phát triển công nghệ mạng không dây băng thông rộng.

1.2 Chuẩn 802.16

1.2.1 Bộ chuẩn 802.16

Chuẩn 802.16 bao gồm các đặc tả truy cập không dây băng thông rộng, do IEEE phát triển, còn gọi là WirelessMAN. Chuẩn 802.16 đầu tiên được chấp nhận vào tháng 12 năm 2001 và được công bố vào năm 2002 là IEEE Std 802.16-2001. Sau đó, chuẩn có hai bổ sung là 802.16a và 802.16c. Chuẩn 802.16a bổ sung đặc tả cho lớp vật lý dải tần 2-11GHz, chuẩn 802.16c mô tả

chi tiết bảng mô tả hệ thống 10-66 GHz. Vào tháng 9 năm 2003, dự án 802.16d rà soát lại các chuẩn trên, điều chỉnh thống nhất với chuẩn ETSI HIPERMAN và quy định các đặc tả cho việc kiểm tra. Dự án kết thúc vào tháng 10 năm 2004, chuẩn 802.16 được công bố là IEEE Std 802.16-2004 thay thế cho IEEE Std 802.16-2001 và hai chuẩn bổ sung của nó 802.16a, 802.16c. Chuẩn 802.16-2004 quy định chuẩn truy cập không dây cố định.

Sau đó, vào tháng 2 năm 2006, chuẩn bổ sung 802.16e-2005 (còn được gọi là WiMAX di động) được công bố và cuối tháng 8 năm 2006 thì IEEE cho phép mọi người có thể lấy về. Chuẩn này bổ sung tính di động trong truy cập không dây băng thông rộng. Kết quả của dự án sửa các lỗi trong chuẩn 802.16-2004 là 802.16-2004/Cor1-2005 công bố ghép cùng với chuẩn 802.16e-2005.

Ngoài ra, chuẩn 802.16 còn có chuẩn bổ sung 802.16f quy định cơ sở thông tin quản trị được công bố vào tháng 12 năm 2005. Các chuẩn bổ sung đang được xây dựng bao gồm 802.16g, 802.16h, 802.16i, 802.16j, 802.16k. Chuẩn bổ sung 802.16g quy định các dịch vụ và thủ tục. Chuẩn bổ sung 802.16h quy định các cơ chế cùng tồn tại hoạt động của phổ không đăng ký, chuẩn bổ sung 802.16i quy định cơ sở thông tin quản lý di động, chuẩn bổ sung 802.16j quy định chuyển tiếp giữa nhiều trạm di động, chuẩn bổ sung 802.16k quy định về cầu nối. ([18], IEEE 802.16 Project Development Milestones)

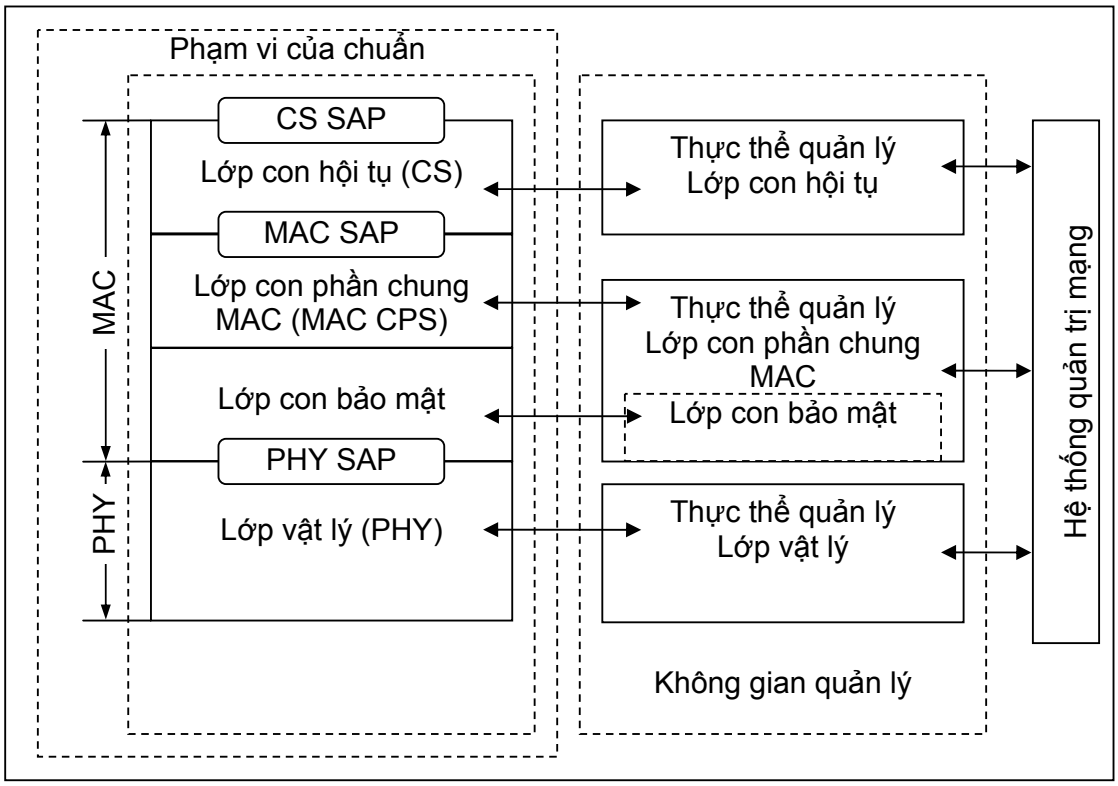
1.2.2 Chuẩn 802.16-2004

1.2.2.1 Mô hình chuẩn 802.16-2004

Chuẩn 802.16-2004 định nghĩa lớp điều khiển truy cập (MAC) và lớp vật lý (PHY). Trong đó lớp MAC được tách thành 3 lớp con: Lớp con hội tụ

(Convergence Sublayer - CS), lớp con phần chung (Common Part Sublayer - CPS) và lớp con bảo mật (Security Sublayer). Lớp MAC của WiMAX khác với Wi-Fi về thuật toán phân phối băng thông và truy cập, quản lý các kiểu lưu lượng bởi các tham số chất lượng dịch vụ. Lớp MAC của IEEE 802.16 là hướng kết nối và bao gồm một chuỗi các máy trạng thái. Mỗi máy trạng thái xác định thao tác của các quá trình riêng lẻ trong cấu trúc MAC. Có các máy trạng thái cho quá trình khởi đầu vào mạng, uỷ quyền và quản lý khoá,... Máy trạng thái là một khái niệm quan trọng khi xem xét sâu bên trong của các cơ chế hoạt động của lớp MAC.

Mô hình tham chiếu định nghĩa phạm vi của chuẩn IEEE 802.16 như mô tả trong hình 1.3. Trong phần sau, chúng ta sẽ tìm hiểu chi tiết về các lớp trên.



Hình 1.3 Mô hình tham chiếu của IEEE 802.16

(Nguồn: [6], trang 3)

1.2.2.2 Lớp con hội tụ

Chuẩn WiMAX định nghĩa hai lớp con hội tụ ([6], trang 17-21):

- Lớp con hội tụ ATM cho các dịch vụ dựa trên ATM.
- Lớp con hội tụ cho các dịch vụ dựa trên IPv4 hoặc IPv6, Ethernet và VLAN.

Lớp con hội tụ cung cấp các chức năng sau:

- Chuyển đổi hay ánh xạ của dữ liệu nhận qua điểm truy cập dịch vụ CS (CS SAP) thành đơn vị dữ liệu MAC (MAC SDU) nhận bởi lớp con phần chung qua điểm truy cập dịch vụ MAC (MAC SAP). Sự ánh xạ phụ thuộc vào kiểu của dịch vụ.
- Phân loại các SDU và liên kết chúng với định danh luồng dịch vụ MAC, định danh kết nối thích hợp.

Đơn vị dữ liệu dịch vụ (SDU) là dữ liệu trao đổi giữa hai lớp giao thức kề nhau. Theo hướng xuống, SDU là các đơn vị dữ liệu đã nhận từ lớp cao hơn trước đó. Theo hướng lên, SDU là các đơn vị dữ liệu được gửi tới lớp cao hơn tiếp theo. Phân biệt đơn vị dữ liệu dịch vụ với đơn vị dữ liệu giao thức (PDU). PDU là đơn vị dữ liệu trao đổi giữa các thực thể của cùng một lớp giao thức. Theo hướng xuống, PDU là đơn vị dữ liệu sinh cho lớp thấp hơn. Theo hướng lên PDU là đơn vị dữ liệu nhận từ lớp thấp hơn.

Định dạng bên trong của dữ liệu lớp con hội tụ thống nhất với kiểu lớp con hội tụ đó (ví dụ lớp con hội tụ ATM thì định dạng dữ liệu lớp con hội tụ sẽ là định dạng tế bào ATM) và lớp con phần chung không phải hiểu định dạng hoặc phân tích bất kỳ thông tin nào từ dữ liệu của lớp con hội tụ.

1.2.2.3 Lớp con phần chung

Lớp con phần chung cung cấp chức năng chính của MAC bao gồm truy cập hệ thống, phân phối băng thông, thiết lập kết nối, duy trì kết nối. Lớp này

nhận dữ liệu từ các lớp con hội tụ qua điểm truy cập dịch vụ MAC, phân loại tới các kết nối MAC cụ thể. Ở lớp này, chất lượng dịch vụ được áp dụng trong việc lập lịch và truyền dữ liệu. Chi tiết về vấn đề đảm bảo chất lượng dịch vụ của IEEE 802.16 chúng ta sẽ nghiên cứu trong phần 3.3.

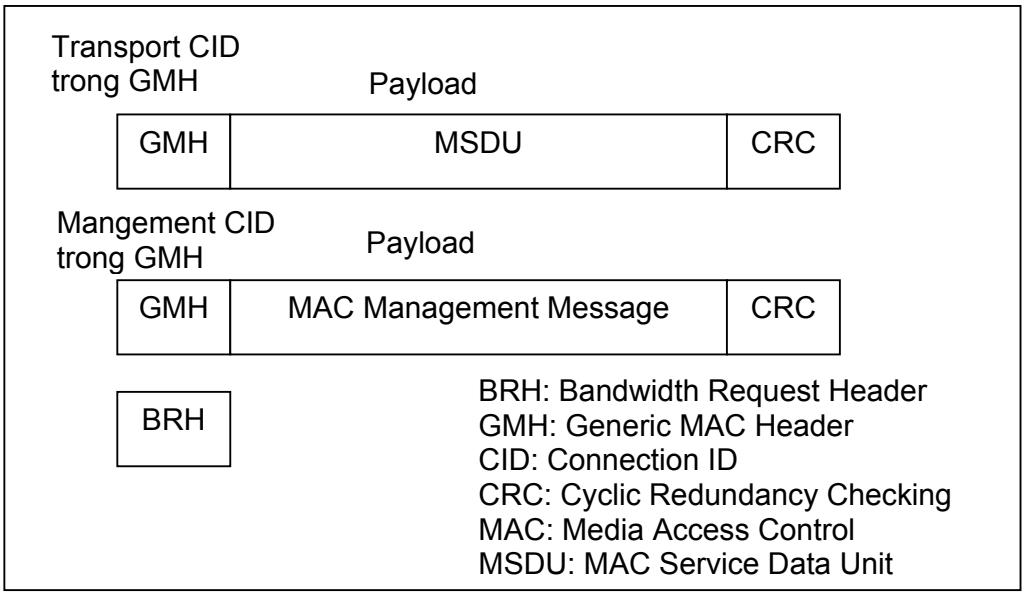
Việc quản lý kết nối, đánh địa chỉ phụ thuộc vào 2 chế độ hoạt động mà chuẩn IEEE 802.16 định nghĩa. Chuẩn 802.16 định nghĩa 2 chế độ chia sẻ phương tiện không dây là Point-to-Multipoint (PMP) và mesh. Với PMP, trạm cơ sở (BS) phục vụ một tập các trạm thuê bao (SS) trong một sector của ăng-ten truyền quảng bá, với tất cả SS nhận cùng thông tin từ BS. Việc truyền từ các SS được điều khiển bởi BS. Trong chế độ mesh, lưu lượng có thể được truyền giữa các SS với nhau, điều khiển truy cập được phân bố giữa các SS. Chế độ hoạt động PMP thích hợp với kịch bản nhiều thuê bao dịch vụ được phục vụ bởi một nhà cung cấp dịch vụ trung tâm. Mục đích để các thuê bao có thể truy cập mạng bên ngoài (ví dụ Internet) hoặc các dịch vụ như truyền hình số. PMP là mô hình hoạt động được ứng dụng phổ biến và các nghiên cứu của chúng ta chỉ tập trung nghiên cứu trong chế độ hoạt động này.

MAC là hướng kết nối. Mọi dịch vụ được ánh xạ tới một kết nối và mọi kết nối được tham chiếu tới một định danh kết nối (CID) 16 bít và có thể liên tục yêu cầu giành băng thông theo nhu cầu. Các kết nối lớp MAC có thể hình dung như kết nối TCP. Giống các kết nối TCP, trong đó một máy tính có đồng thời nhiều kết nối trong các cổng khác nhau, trong kết nối MAC, SS có thể có nhiều kết nối tới BS cho các dịch vụ khác nhau như quản trị mạng, truyền dữ liệu người sử dụng. Sự khác nhau quan trọng là trong kết nối MAC, mọi kết nối có các tham số khác nhau về băng thông, an toàn bảo mật và độ ưu tiên. Mọi kết nối được xác định bởi CID của nó, CID được gán bởi BS. Khi một SS tham gia và mạng, có 3 CID được gán cho nó và mỗi CID có yêu cầu chất lượng dịch vụ khác nhau sử dụng bởi các mức độ quản lý khác nhau:

Basic, Primary Management và Secondary Management connection.

Basic connection sử dụng để truyền ngắn, truyền các bản tin cần truyền độ trễ thấp. Primary Management connection được sử dụng để truyền dài hơn, truyền các bản tin chấp nhận trễ như các yêu cầu đăng ký và các bản tin xác thực. Secondary Management connection được sử dụng để truyền các bản tin quản lý dựa trên các chuẩn như DHCP, TFTP, SNMP. MAC dành thêm các kết nối cho các mục đích khác như truyền các lịch truyền đường lên và đường xuống.

Đơn vị dữ liệu của lớp con phần chung là các MAC PDU. MAC PDU bao gồm một MAC header có chiều dài cố định, phần dữ liệu tải có chiều dài thay đổi và kiểm tra CRC. Có hai kiểu header là kiểu header chung (GMH) và kiểu header yêu cầu băng thông (BRH). Các MAC PDU bắt đầu với kiểu header chung sẽ chứa bản tin quản lý MAC hoặc dữ liệu của lớp con hội tụ. MAC PDU có kiểu header là header yêu cầu băng thông sử dụng để yêu cầu băng thông và không chứa trường dữ liệu tải. Chi tiết định dạng của từng kiểu xem trong phần 6.3.2 tài liệu [6].



Hình 1.4 Cấu trúc của MAC PDU

MAC subheader có thể được chèn vào MAC PDU ngay sau kiểu header chung. Có 5 kiểu MAC subheader là: Mesh, Fragmentation, Fast-Feedback Allocation, Grant Management, Packing. Nếu cả Fragmentation subheader và Grant Management subheader tồn tại Grant Management subheader sẽ đứng trước. Nếu Mesh subheader tồn tại thì nó trước các subheader khác. Fast-Feedback Allocation subheader luôn nằm ở vị trí cuối. Packing subheader có thể đứng trước MAC SDU được chỉ ra bởi trường Type. Packing và Fragmentation subheader không tồn tại trong cùng MAC PDU.

Vai trò các kiểu MAC subheader là:

- Grant management subheader: sử dụng bởi SS để truyền yêu cầu quản lý băng thông tới BS của nó.
- Fragmentation subheader: chứa thông tin chỉ định sự có mặt và sự định hướng trong dữ liệu tải của fragment của các SDU.
- Packing subheader: chỉ định sự đóng gói nhiều SDU vào một PDU.
- Mesh subheader: chứa định danh của nút, sử dụng trong chế độ mesh.
- Fast-Feedback subheader: sử dụng để cho phép SS truyền các thông tin liên quan tới PHY đòi hỏi trả lời nhanh.

1.2.2.4 Lớp con bảo mật

Lớp con bảo mật đảm bảo sự riêng tư của các thuê bao khi truyền thông tin qua mạng, chống truy cập không xác thực tới các dịch vụ truyền dữ liệu. Kiến trúc bảo mật của lớp con bảo mật đảm bảo các yêu cầu trên. Chi tiết hơn về các cơ chế bảo mật của IEEE 802.16 chúng ta sẽ nghiên cứu trong phần 4.3. Kiến trúc bao gồm hai thành phần giao thức ([6], trang 271):

- Giao thức đóng gói để mã hóa gói dữ liệu qua mạng. Giao thức này định nghĩa một tập bộ mật mã hỗ trợ (cặp mã hóa dữ liệu, thuật toán

xác thực và các quy tắc để áp dụng các thuật toán đó tới dữ liệu tải của MAC PDU).

- Giao thức quản lý khóa riêng (PKM) và uỷ quyền quản lý khoá cung cấp bảo mật cho việc phân phối dữ liệu khóa từ BS tới SS. Qua giao thức quản lý khóa này, SS và BS đồng bộ dữ liệu khóa, ngoài ra BS sử dụng giao thức này để thực hiện điều kiện truy cập tới các dịch vụ mạng.

Mã hoá gói dữ liệu

Các dịch vụ mã hóa được định nghĩa như một tập các khả năng trong lớp con bảo mật của MAC. Thông tin MAC header chỉ ra sự mã hóa được chứa trong định dạng của MAC header kiểu chung. Sự mã hóa luôn được áp dung cho dữ liệu tải của MAC PDU, MAC header kiểu chung không được mã hóa. Tất cả các bản tin quản lý MAC sẽ được gửi không mã hóa để thuận tiện cho việc đăng ký và các thao tác khác của MAC.

Giao thức quản lý khoá và uỷ quyền quản lý khoá

SS sử dụng giao thức PKM để giành xác thực và khóa từ BS và để hỗ trợ xác thực lại theo chu kỳ và tạo mới khóa. Giao thức quản lý khóa sử dụng chứng chỉ số X.509, thuật toán mã hóa khóa công khai RSA để thực hiện trao đổi khóa giữa SS và BS.

Giao thức PKM gắn với mô hình client/server trong đó SS yêu cầu khóa và BS (PKM server) trả lời các yêu cầu đó. Giao thức này đảm bảo rằng các SS riêng biệt chỉ nhận khóa chúng được xác thực. Giao thức PKM sử dụng bản tin quản lý MAC là PKM-REQ và PKM-RSP.

Giao thức PKM sử dụng mật mã khóa công khai để giành khoá AK giữa SS và BS. Sau đó, khóa AK được sử dụng để bảo đảm an toàn việc trao đổi

PKM sau đó của các khóa TEK. Khoá TEK (Traffic Encryption Key) dùng để mã hoá dữ liệu trong các bản tin.

BS xác thực SS trong quá trình trao đổi xác thực ban đầu. Mỗi SS mang một chứng chỉ số X.509 duy nhất phát hành bởi nhà sản suất. Chứng chỉ số chứa một khóa công khai của SS và địa chỉ MAC. Khi yêu cầu một AK, SS đưa chứng chỉ số của nó cho BS. BS kiểm tra chứng chỉ số này rồi sử dụng khóa công khai đã được kiểm tra để mã hóa khoá AK gửi trả lời SS đã yêu cầu.

BS liên kết một định danh xác thực của SS với một chi phí của người sử dụng, với dịch vụ dữ liệu (voide, video, dữ liệu) mà người sử dụng được xác thực để truy cập. Vì vậy, với sự trao đổi AK, BS thiết lập định danh được xác thực của SS và các dịch vụ SS được xác thực để truy cập.

1.2.2.5 Lớp vật lý

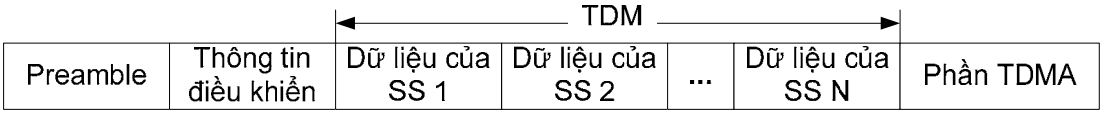
WiMAX có 5 dạng, chúng được xác định bởi lớp vật lý của chúng. Các dạng này được tách thành các băng tần bao gồm: 2-11 GHz và 10-66 GHz. Bảng 1.3 mô tả tổng quan về các dạng này. ([6], mục 8)

Bảng 1.3 Các dạng PHY

Tên	**Hoạt động**	**LOS/ NLOS**	**Tần số**	**Ghép kênh**
WirelessMAN-SC	Point-to-point	LOS	10-66 GHz	TDD, FDD
WirelessMAN-SCa	Point-to-point	NLOS	2-11 GHz	TDD, FDD
WirelessMAN-OFDM	Point-to-multipoint	NLOS	2-11 GHz	TDD, FDD
WirelessMAN-OFDMA	Point-to-multipoint	NLOS	2-11 GHz	TDD, FDD
WirelessHUMAN	Point-to-multipoint	NLOS	2-11 GHz	TDD

Lớp vật lý hoạt động tại 10-66 GHz và 2-11 GHz với tốc độ dữ liệu từ 32-130 Mbps phụ thuộc vào độ rộng băng tần và kỹ thuật điều chế. Kiến trúc IEEE 802.16 bao gồm hai kiểu trạm: SS và BS. Trong chế độ PMP, BS điều khiển mọi hoạt động truyền thông trong mạng, không có truyền thông trực tiếp giữa các SS. Đường truyền thông giữa SS và BS có hai hướng: hướng lên (từ SS tới BS) và hướng xuống (từ BS tới SS). WiMAX hỗ trợ cả ghép kênh theo thời gian (TDD) và ghép kênh theo tần số (FDD).

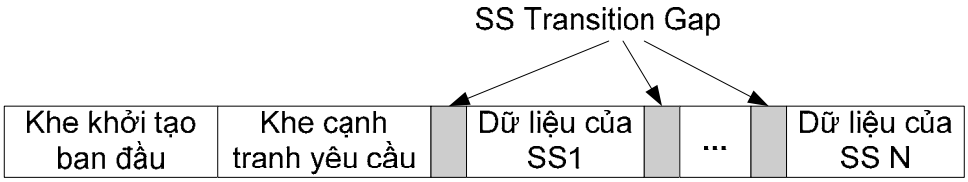
Các kênh được chia theo thời gian thông qua các khung. Một khung lại chia nhỏ theo thời gian thành các khe vật lý. Mỗi khung chia thành hai kênh lôgíc, kênh đường xuống và kênh đường lên. Khung con đường xuống tương ứng với kênh đường xuống và khung con đường lên tương ứng với kênh đường lên. Độ dài của các khung con đó thay đổi động và do BS quy định.



Hình 1.5 Cấu trúc của khung con đường xuống

Khung con đường xuống minh hoạ như trên hình 1.5. Bắt đầu khung con đường xuống là Preamble. Lớp vật lý sử dụng Preamble để đồng bộ. Phần thông tin điều khiển chứa DL-MAP cho khung đường xuống hiện tại và UL-MAP cho kênh đường lên ở một thời gian cụ thể trong tương lai. Bản tin DL-MAP mô tả khoảng thời gian của khung, số khung, định danh của kênh đường xuống,... Bản tin UL-MAP mô tả định danh kênh đường lên, thời gian bắt đầu của khung con đường lên tính tương đối so với thời gian bắt đầu của khung, băng thông giành cho SS,... Sau phần thông tin điều khiển là phần TDM. Phần TDM mang dữ liệu, được tổ chức thành các burst với các burst profile khác nau. Dữ liệu được truyền tới mỗi SS sử dụng burst profile đã thoả thuận. Trong hệ thống FDD, phần TDM có thể theo sau bởi phần TDMA để hỗ trợ

tốt hơn cho các SS bán song công.



Hình 1.6 Cấu trúc của khung con đường lên

Khung con đường lên minh hoạ trong hình 1.6. Khung con đường lên chứa ba loại burst được truyền bởi SS. Đó là burst truyền trong khe cạnh tranh dành cho quá trình điều chỉnh ban đầu, burst truyền trong các khe cạnh tranh hoặc khe unicast dành cho việc yêu cầu băng thông, burst được truyền trong các khe unicast dành cho SS để truyền dữ liệu đường lên. SS truyền theo sự cấp phát dành cho chúng sử dụng burst profile đã chỉ ra trong UL-MAP. SS Transition Gap tách việc truyền của các SS khác nhau trong suốt khung con đường lên.

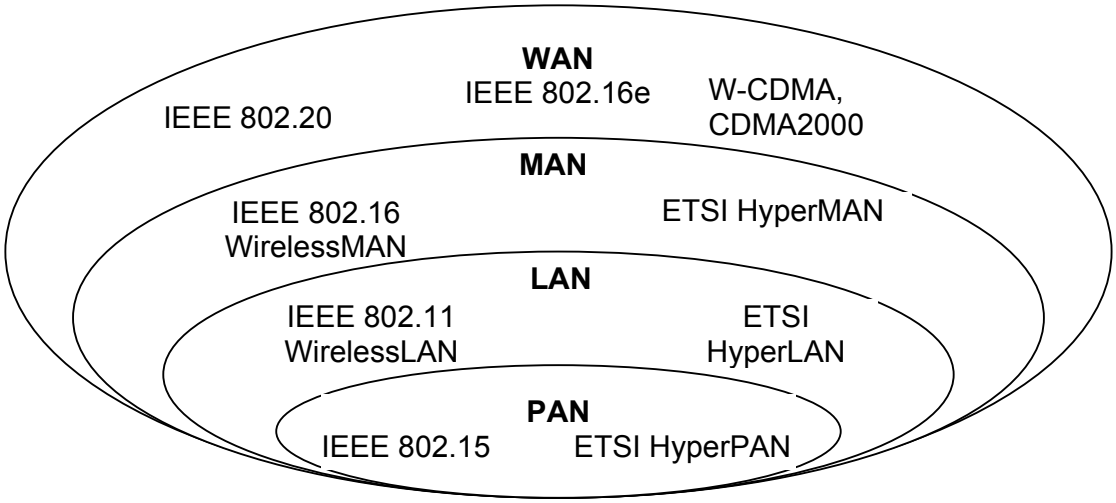
1.3 Xu hướng phát triển của mạng không dây băng thông rộng

1.3.1 Các công nghệ mạng không dây băng thông rộng

Theo tiêu chí phạm vi của mạng, người ta phân loại các công nghệ mạng không dây như sau:

- Mạng PAN: IEEE 802.15, ETSI HiperPAN
- Mạng LAN: IEEE 802.11, ETSI HiperLAN
- Mạng MAN: IEEE 802.16, ETSI HiperMAN
- Mạng WAN: IEEE 802.16e, IEEE 802.20, W-CDMA, CDMA2000

Hình 1.7 minh họa phân loại các công nghệ mạng này.



Hình 1.7 Phân loại các công nghệ mạng không dây

Trong đó, các giải pháp truy cập không dây băng thông rộng cho mạng WAN có thể chia thành 4 nhóm chính. Hai trong số đó là hệ thống GSM thế hệ ba là W-CDMA và hệ thống CDMA thế hệ ba là CDMA2000. Hai nhóm còn lại là WiMAX và 802.20 đang phát triển, hoàn thiện. Công nghệ WiMAX chúng ta đã tìm hiểu ở trên, trong phần này chúng ta sẽ tìm hiểu về 3 công nghệ mạng không dây băng thông rộng còn lại.

GSM (Global System for Mobile Communications) là công nghệ chiếm ưu thế trên thế giới và ở Châu Âu. Công nghệ này cũng được sử dụng trong nhiều quốc gia Châu Phi, Châu Á, Trung Đông và một số nước ở Châu Mỹ. Hệ thống GSM ban đầu chỉ hỗ trợ khả năng dữ liệu rất giới hạn nên chưa được gọi là băng thông rộng. GPRS và EDGE được coi là mạng GSM thế hệ 2,5G. GPRS cung cấp tốc độ tối đa 171,2 Kbp/s trong khi EDGE có thể cung cấp tốc độ cao gấp 3 lần tốc độ đó. Hệ thống W-CDMA là thế hệ ba nâng cấp lên từ mạng GSM 2,5G. Các mạng này còn gọi là UMTS, triển khai đầu tiên tại Châu Âu và Nhật Bản. Hệ thống chuẩn W-CDMA có thể hỗ trợ 2 Mbp/s.

Phiên bản nâng cao của W-CDMA là HSDPA, cho phép tốc độ đường xuống lên tới 14 Mbp/s.

Ngoài ra, chúng ta có thể biết đến chuẩn TD-SCDMA (Time Division Synchronous Code Division Multiple Access) được ứng dụng tại Trung Quốc. Đây là một chuẩn 3G được tạo bởi Học viện công nghệ truyền thông của Trung Quốc. Chuẩn TD-SCDMA là một phát triển từ chuẩn GSM theo cùng cách của W-CDMA.

CDMA (Code Division Multiple Access) là công nghệ sử dụng chuẩn IS-136. Số lượng thuê bao CDMA lớn nhất ở Châu Mỹ, tiếp theo là khu vực Châu Á Thái Bình Dương. CDMA không được ưu chuộng tại Châu Âu, các nước Ả Rập và Châu Phi. Thế hệ 3G cho mạng CDMA gọi là CDMA2000. Nó bao gồm các hệ thống CDMA 2000 1x hỗ trợ tốc độ dữ liệu lên tới 307 Kbp/s. Thực tế, người ta cho rằng thế hệ 3G thực sự của CDMA là CDMA2000 1xEV (Evolution), phiên bản cao hơn của phiên bản 1x. Phiên bản CDMA2000 1xEV bao gồm CDMA2000 1xEV-DO (data only) và CDMA2000EV-DV (data/voice). Các phiên bản này hỗ trợ tốc độ lý thuyết đường xuống 3,1 Mbp/s và đường lên 1,8 Mbp/s.

Hiệu năng và sự chấp nhận của thị trường mạng 3G (cả CDMA2000 và W-CDMA) cho tới hiện tại chưa đáp ứng được yêu cầu thực tế. Đối với các tổng đài, lý do là chi phí nâng cấp mạng cao, chi phí phải trả cho phổ 3G trong một số nước (hầu hết là Châu Âu) quá cao và thiếu các ứng dụng để thuyết phục thuê bao chấp nhận nâng cấp thiết bị cầm tay.

Chuẩn 802.20 khác WiMAX là WiMAX bắt đầu với công nghệ không dây băng thông rộng cố định và phát triển để hỗ trợ tính di động, 802.20 ngay ban đầu được thiết cho cho công nghệ băng thông rộng di động. Các yêu cầu ngay ban đầu này thể hiện ưu điểm hơn so với việc thêm hỗ trợ tính di động vào trong chuẩn không dây cố định đã có. Tuy vậy, ưu điểm của 802.16 là

chuẩn đầu tiên hội tụ các ưu điểm mạng không dây băng thông rộng và hiện tại được sự hỗ trợ của hầu hết các nhà công nghiệp truyền thông lớn.

1.3.2 Xu hướng tích hợp các công nghệ mạng

Chúng ta thấy rằng có một số sự bổ sung và cạnh tranh giữa các chuẩn, giữa các vùng, các tính năng và nhà sản xuất. Nhiều môi trường khác nhau sẽ cài đặt một tập không đồng nhất các mạng không dây mà chức năng của các hệ thống này gần như thống nhất. Do đó, một xu hướng phát triển là cung cấp khả năng phối hợp hoạt động và kết hợp của các hệ thống khác nhau.

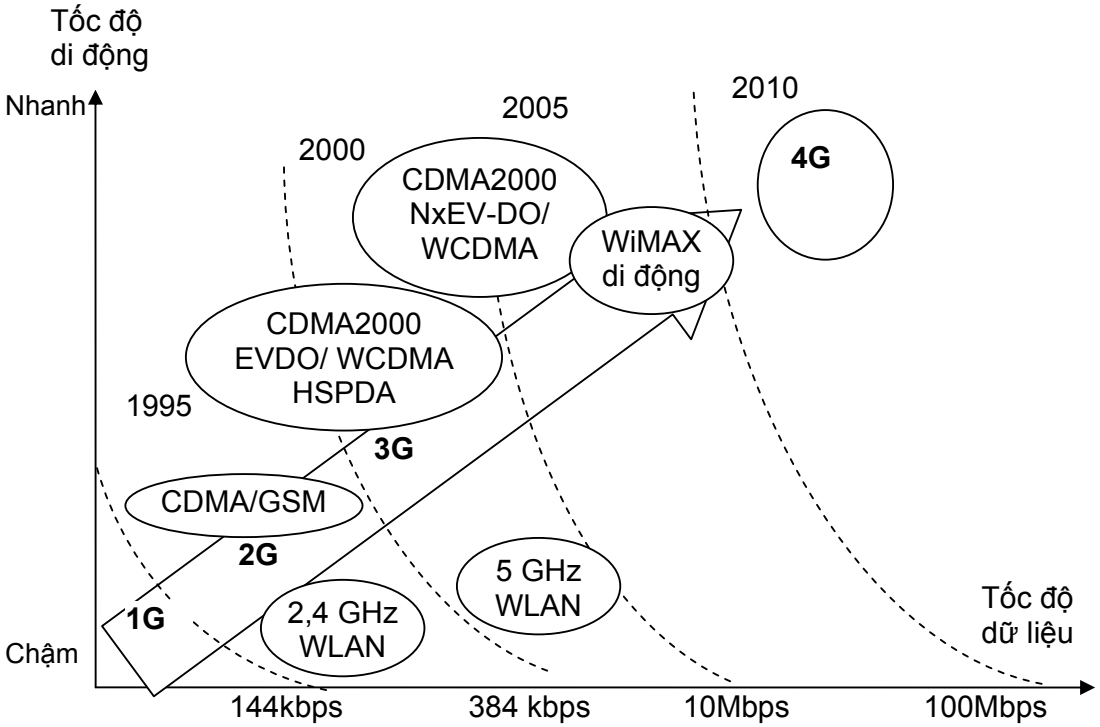
Công việc nghiên cứu tiếp tục được tiến hành là cách tích hợp các công nghệ mạng khác nhau. Ví dụ, dự án hiệp hội thế hệ ba (3GPP) đã nghiên cứu các hệ thống để phối hợp giữa các hệ thống 3G với mạng WiMAX hoặc Wi-Fi. Các vấn đề bao gồm chất lượng dịch vụ, chuyển vùng, xác thực, uỷ quyền và kế toán.

Hiện nay, không chỉ có một công nghệ băng thông rộng tối ưu duy nhất. Mỗi dòng công nghệ chính có một số điểm mạnh và một số điểm yếu. Dưới đây là một số tiêu chí chính giúp lựa chọn giữa các công nghệ. Mặc dù sự khác nhau của các công nghệ, có một chuỗi hội tụ chính giữa các đặc điểm cho ý tưởng mạng không dây băng thông rộng bao gồm:

- Băng thông rộng
- Đảm bảo chất lượng dịch vụ phía người dùng
- Hỗ trợ đa phương tiện
- Tốc độ di chuyển 60-120km/h
- Quản lý phiên liền mạch khi di chuyển
- Hỗ trợ an toàn bảo mật
- Hỗ trợ quản lý phổ động linh hoạt

- Giao thức xác thực, uỷ quyền và kế toán ưu việt.

Các mục đích trên khó thực hiện đồng thời. Công nghệ 3G và không dây cố định hội tụ các ưu điểm khác nhau. Ưu điểm mạng 3G là khả năng di động, tính toán khắp mọi nơi, đảm bảo chất lượng dịch vụ nhưng có hạn chế về tốc độ truyền dữ liệu và khả năng cung cấp dịch vụ đa phương tiện. Trong khi các công nghệ mạng như WiMAX thì chi phí vừa phải, truyền dữ liệu lớn, tốc độ truyền cao, đảm bảo chất lượng dịch vụ nhưng tính di động vẫn còn hạn chế. Hai vấn đề quan trọng mà các công nghệ cạnh tranh đó là tốc độ và khả năng di động. So sánh hai vấn đề này giữa các công nghệ như minh họa trên hình 1.8. Theo phân tích, 4G sẽ không phải là một công nghệ mới mà là sự tích hợp các công nghệ đã có để hội tụ một thiết kế mạng với đầy đủ tính năng trên.



Hình 1.8 So sánh khả năng của các công nghệ mạng không dây

1.4 Kết chương

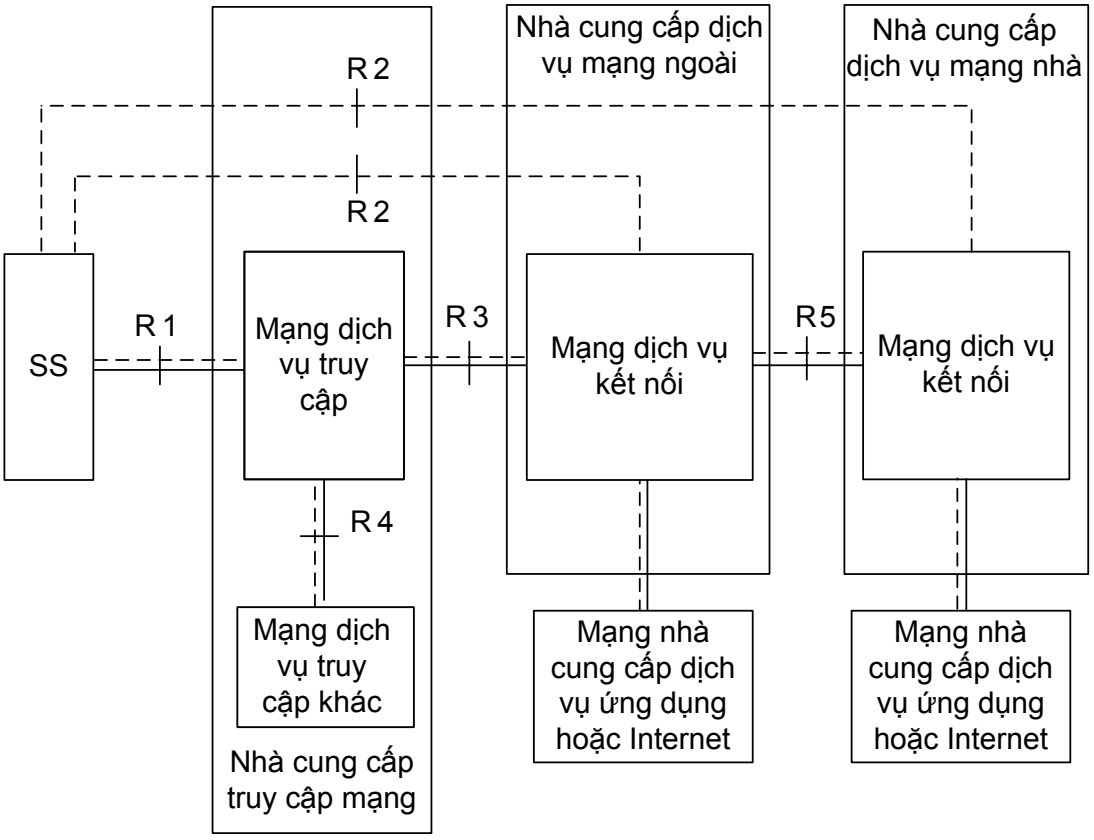
Trong chương này, chúng ta đã tìm hiểu về các vấn đề chung của công nghệ WiMAX như khái niệm, ứng dụng của WiMAX, các phiên bản WiMAX, chứng nhận sản phẩm WiMAX và sự phát triển của công nghệ WiMAX. Sau đó, chúng ta tìm hiểu về bộ chuẩn 802.16. Trong phần tìm hiểu về chuẩn 802.16, chúng ta đã biết được hai chế độ hoạt động là PMP và Mesh mà chuẩn 802.16 định nghĩa. Phạm vi nghiên cứu trong phần vấn đề chất lượng dịch vụ và an toàn bảo mật của chúng ta sẽ tập trung vào chế độ hoạt động PMP. Trong phần nghiên cứu về xu hướng phát triển của mạng không dây băng thông rộng, chúng ta biết được vị trí tương quan của WiMAX so với các chuẩn công nghệ không dây băng thông rộng khác và xu hướng phát triển tích hợp các công nghệ mạng. Trong chương tiếp theo, chúng ta sẽ nghiên cứu chi tiết về kiến trúc của mạng WiMAX.

Chương 2.
KIẾN TRÚC MẠNG WiMAX

2.1 Mô hình lý thuyết

2.1.1 Mô hình tổng thể

Kiến trúc mạng WiMAX được biểu diễn lôgic thông qua mô hình tham chiếu mạng (Network Reference Model – NRM), bao gồm các thực thể chức năng và các điểm tham chiếu. Mô hình có các thực thể lôgic là SS, mạng dịch vụ truy cập và mạng dịch vụ kết nối. Mỗi thực thể SS, mạng dịch vụ truy cập và mạng dịch vụ kết nối biểu diễn một nhóm các thực thể chức năng. Hình 2.1 minh họa mô hình tham chiếu của mạng WiMAX.



Hình 2.1 Mô hình tham chiếu mạng WiMAX

(Nguồn: [13], trang 26)

Việc nhóm và phân bố các chức năng vào các thiết bị vật lý trong mạng dịch vụ truy cập là tùy chọn. Đặc tả NWG phát hành lần thứ nhất định nghĩa 3 bảng mô tả A, B và C mô tả tính phối hợp hoạt động của mạng dịch vụ truy cập. Các nhà sản xuất hạ tầng có thể chọn một hoặc nhiều bảng thông tin mạng dịch vụ truy cập trong việc thực hiện vật lý của mạng dịch vụ truy cập để thỏa mãn yêu cầu tính phối hợp hoạt động mạng.

Trong mô hình tham chiếu mạng, chúng ta phân biệt các nhà cung cấp sau:

- Nhà cung cấp truy cập mạng là đơn vị cung cấp hạ tầng truy cập sóng vô tuyến tới một hoặc nhiều nhà cung cấp dịch vụ mạng.
- Nhà cung cấp dịch vụ mạng là đơn vị cung cấp kết nối IP và dịch vụ WiMAX tới các thuê bao theo hợp đồng cung cấp dịch vụ với các thuê bao. Đối với thuê bao sẽ phân biệt nhà cung cấp dịch vụ mạng nhà và nhà cung cấp dịch vụ mạng ngoài. Nhà cung cấp dịch vụ mạng nhà là đơn vị có hợp đồng với thuê bao đó, thực hiện xác thực, uỷ quyền và tính cước đối với thuê bao. Khi thuê bao di chuyển vào vùng của nhà cung cấp dịch vụ mạng khác, thì nhà cung cấp dịch vụ mạng đó gọi là nhà cung cấp dịch vụ mạng ngoài đối với thuê bao. Nhà cung cấp dịch vụ mạng có thể ký hợp đồng với các đơn vị thứ ba (ví dụ nhà cung cấp dịch vụ ứng dụng, nhà cung cấp dịch vụ Internet) để cung cấp các dịch vụ WiMAX cho thuê bao.

Các thực thể lôgic trong mô hình tham chiếu mạng WiMAX là mạng dịch vụ truy cập, mạng dịch vụ kết nối và SS. Chúng ta phân biệt các thực thể lôgic trên như sau:

- Mạng dịch vụ truy cập có chức năng cung cấp sự truy cập sóng vô tuyến tới một thuê bao WiMAX. Nó bao gồm một hoặc nhiều BS, một hoặc nhiều cổng mạng dịch vụ truy cập. Chúng ta trình bày chi

tiết về mạng dịch vụ truy cập trong phần 2.1.2.

- Mạng dịch vụ kết nối có chức năng mạng cung cấp các dịch vụ kết nối IP tới các thuê bao WiMAX. Chúng ta trình bày chi tiết về mạng dịch vụ kết nối trong phần 2.1.3.
- SS là thiết bị cung cấp kết nối giữa thuê bao và BS.

Mô hình tham chiếu mạng WiMAX chứa các điểm tham chiếu chuẩn là R1, R2, R3, R4, R5. Điểm tham chiếu là một điểm khái niệm giữa hai nhóm các chức năng mà nhóm chức năng này tồn tại ở các thực thể chức năng khác nhau. Các chức năng này đưa ra các giao thức khác nhau cho các điểm tham chiếu. Cụ thể nhiệm vụ của các điểm tham chiếu trên như sau:

- Điểm tham chiếu R1 chứa các giao thức và thủ tục giữa SS và mạng dịch vụ truy cập liên quan đến đặc tả giao diện không khí (đặc tả PHY và MAC theo IEEE 802.16).
- Điểm tham chiếu R2 chứa các giao thức và các thủ tục giữa SS và mạng dịch vụ kết nối liên quan tới việc xác thực, uỷ quyền dịch vụ và quản lý cấu hình trạm IP. Điểm tham chiếu này là lôgic, không phản ánh trực tiếp giao thức giao tiếp giữa SS và mạng dịch vụ kết nối. Phần xác thực của điểm tham chiếu R2 chạy giữa SS và mạng dịch vụ kết nối của nhà cung cấp dịch vụ mạng nhà. Tuy vậy, mạng dịch vụ truy cập và mạng dịch vụ kết nối của nhà cung cấp dịch vụ mạng ngoài có thể xử lý một phần trước đó.
- Điểm tham chiếu R3 chứa một tập các giao thức không gian điều khiển giữa mạng dịch vụ truy cập và mạng dịch vụ kết nối để hỗ trợ xác thực, uỷ quyền và kế toán, thực hiện các chính sách và khả năng quản lý di động. Nó cũng bao gồm các phương thức thuộc không gian vận chuyển (ví dụ, tạo đường hầm theo RFC2003, RFC2004,...) để truyền dữ liệu của người sử dụng giữa mạng dịch

vụ truy cập và mạng dịch vụ kết nối.

- Điểm tham chiếu R4 chứa một tập các giao thức không gian vận chuyển và không gian điều khiển bắt đầu/kết thúc trong các thực thể chức năng khác nhau của một mạng dịch vụ truy cập thực hiện phối hợp tính di động của SS giữa các mạng dịch vụ truy cập và các cổng mạng dịch vụ truy cập.
- Điểm tham chiếu R5 chứa một tập các giao thức không gian vận chuyển và không gian điều khiển cho hoạt động giữa mạng dịch vụ kết nối của nhà cung cấp dịch vụ mạng nhà và mạng dịch vụ kết nối của nhà cung cấp dịch vụ mạng ngoài.

2.1.2 Mô hình tham chiếu mạng dịch vụ truy cập

Mạng dịch vụ truy cập bao gồm các thực thể chức năng và các luồng bản tin tương ứng được liên kết với các dịch vụ truy cập. Mạng dịch vụ truy cập biểu diễn một đường bao cho sự phối hợp giữa các phần chức năng trong các WiMAX client, các chức năng dịch vụ kết nối WiMAX và các chức năng cung cấp bởi các nhà sản xuất thiết bị khác nhau.

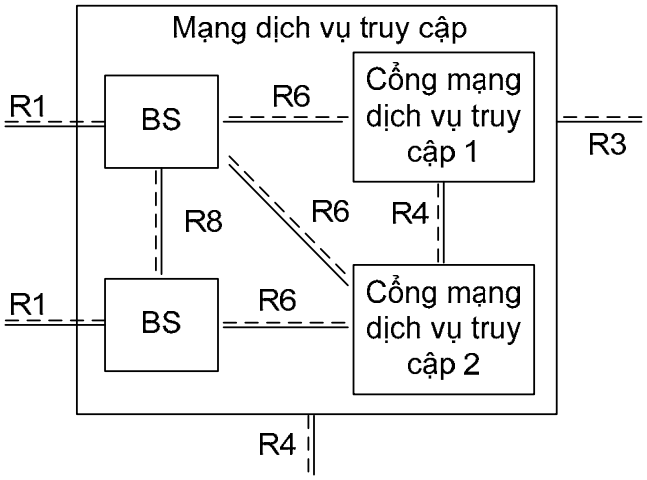
Như đã nói trong phần 2.1.1, mạng dịch vụ truy cập có chức năng cung cấp sự truy cập sóng vô tuyến tới một thuê bao WiMAX. Cụ thể, mạng truy cập dịch vụ cung cấp các chức năng bắt buộc sau:

- Kết nối lớp 2 mạng WiMAX với SS.
- Truyền các bản tin xác thực, uỷ quyền, kế toán tới nhà cung cấp dịch vụ mạng nhà của thuê bao WiMAX phục vụ việc xác thực, uỷ quyền và kế toán.
- Tìm và chọn nhà cung cấp dịch vụ mạng ưu thích của các thuê bao WiMAX.

- Chức năng chuyển tiếp để giành kết nối lớp 3 với SS (ví dụ, vị trí địa chỉ IP).
- Quản lý tài nguyên sóng vô tuyến.

Mạng dịch vụ truy cập bao gồm ít nhất một BS và ít nhất một cổng mạng dịch vụ truy cập.

- BS là thực thể lôgic thực hiện đầy đủ chức năng của WiMAX MAC và WiMAX PHY tương thích với IEEE 802.16. Một BS được gán một tần số và phạm vi bao phủ là một hình quạt. BS kết hợp chặt chẽ với các chức năng lập lịch cho tài nguyên đường lên và đường xuống. BS mô tả trong mô hình là thực thể lôgic và thực hiện vật lý của nó có thể bao gồm nhiều BS.
- Cổng mạng dịch vụ truy cập là thực thể lôgic biểu diễn sự kết tập của các thực thể chức năng của không gian điều khiển ghép cặp với một chức năng tương ứng trong mạng dịch vụ truy cập hoặc một chức năng trong mạng dịch vụ kết nối hoặc một chức năng trong mạng dịch vụ truy cập khác. Cổng mạng dịch vụ truy cập thực hiện chức năng cầu nối hoặc định tuyến của không gian vận chuyển.

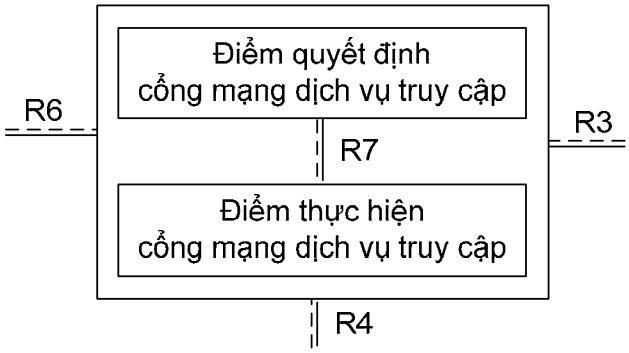


Hình 2.2 Mô hình tham chiếu mạng dịch vụ truy cập

(Nguồn: [13], trang 28)

Mạng dịch vụ truy cập giao tiếp với SS sử dụng điểm tham chiếu R1, với mạng dịch vụ kết nối sử dụng điểm tham chiếu R3 và với mạng dịch vụ truy cập khác sử dụng điểm tham chiếu R4. BS kết nối tới một hoặc nhiều cổng mạng dịch vụ truy cập sử dụng điểm tham chiếu R6. Trong các điểm tham chiếu trên, điểm tham chiếu R4 là điểm tham chiếu duy nhất cho không gian vận chuyển và không gian điều khiển để phối hợp hoạt động giữa các mạng dịch vụ truy cập tương tự hoặc khác nhau.

Các chức năng mạng dịch vụ truy cập trong cổng mạng dịch vụ truy cập có thể phân tách thành hai nhóm chức năng là điểm quyết định và điểm thi hành như minh họa trên hình 2.3. Điểm thi hành bao gồm các chức năng không gian vận chuyển và điểm quyết định bao gồm các chức năng không thuộc không gian vận chuyển. Khi thực hiện, sự phân rã thành hai nhóm trên là không bắt buộc.



Hình 2.3 Mô hình tham chiếu cổng mạng dịch vụ truy cập

Ngoài các điểm tham chiếu chuẩn R1, R2, R3, R4, R5, các điểm tham chiếu trong mạng dịch vụ truy cập bao gồm R6, R7 và R8 (như mô tả trên hình 2.2 và 2.3).

Điểm tham chiếu R6 bao gồm một tập các giao thức của không gian vận chuyển và không gian điều khiển để giao tiếp giữa BS và cổng mạng dịch vụ truy cập. Không gian vận chuyển bao gồm đường dữ liệu trong mạng dịch vụ

truy cập giữa SS và cổng mạng dịch vụ truy cập. Không gian điều khiển bao gồm các giao thức cho việc điều khiển thiết lập, thay đổi và giải phóng đường dữ liệu phù hợp với sự kiện di động của SS. R6 kết hợp với R4 có thể sử dụng như một đường dẫn để trao đổi thông tin trạng thái MAC giữa các BS khi các trạm này không thể phối hợp qua R8 (xem hình 2.2).

Điểm tham chiếu R7 bao gồm tập các giao thức tùy chọn của không gian điều khiển, ví dụ giao thức phối hợp đăng ký, xác thực, uỷ quyền với chính sách trong cổng mạng dịch vụ truy cập cũng như các giao thức khác cho sự phối hợp giữa hai nhóm các chức năng định nghĩa trong R6. Sự phân rã của các chức năng mạng dịch vụ truy cập sử dụng các giao thức R7 là tùy chọn.

Điểm tham chiếu R8 bao gồm tập các luồng bản tin của không gian điều khiển và các luồng dữ liệu của không gian vận chuyển giữa các BS để đảm bảo việc di chuyển giữa các BS nhanh và liền mạch. Không gian vận chuyển bao gồm các giao thức cho phép dữ liệu truyền giữa các BS liên quan tới việc di chuyển của một SS nào đó. Không gian điều khiển bao gồm giao thức truyền thông giữa các BS phù hợp với IEEE 802.16 và tập các giao thức cho phép điều khiển truyền dữ liệu giữa các BS liên quan tới SS nào đó.

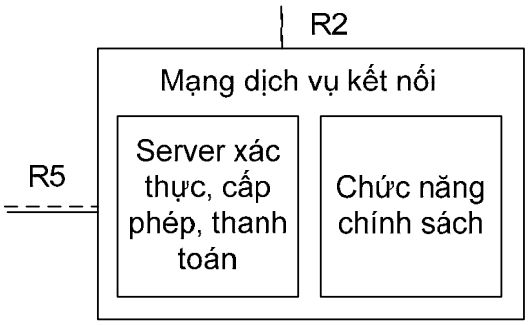
2.1.3 Mô hình tham chiếu mạng dịch vụ kết nối

Mạng dịch vụ kết nối bao gồm các phần tử mạng như bộ định tuyến, server xác thực, uỷ quyền và kế toán, cơ sở dữ liệu người dùng, thực hiện các chính sách. Mạng dịch vụ kết nối thực hiện chức năng cụ thể như sau:

- Cấp phát địa chỉ IP của SS và cấp tham số điểm cuối cho các phiên người sử dụng.
- Truy cập Internet.
- Server xác thực, uỷ quyền và kế toán.

- Điều khiển chính sách hoặc kiểm soát cho phép dựa trên các bảng thông tin thuê bao người sử dụng.
- Sự hỗ trợ tạo đường hầm giữa mạng dịch vụ truy cập và mạng dịch vụ kết nối.
- Tính cước thuê bao và đối soát giữa các tổng đài.
- Tạo đường hầm giữa các mạng dịch vụ kết nối phục vụ cho việc chuyển vùng.
- Hỗ trợ tính di động giữa các mạng dịch vụ truy cập.
- Các dịch vụ WiMAX như các dịch vụ dựa vào vị trí thuê bao, xác thực hoặc kết nối tới các dịch vụ đa phương tiện IP.

Trong phiên bản lần 1, diễn đàn WiMAX chưa định nghĩa các điểm tham chiếu giữa các thực thể chức năng trong mạng dịch vụ kết nối. Mô hình mạng dịch vụ kết nối diễn đàn WiMAX cung cấp hiện tại như hình 2.4.

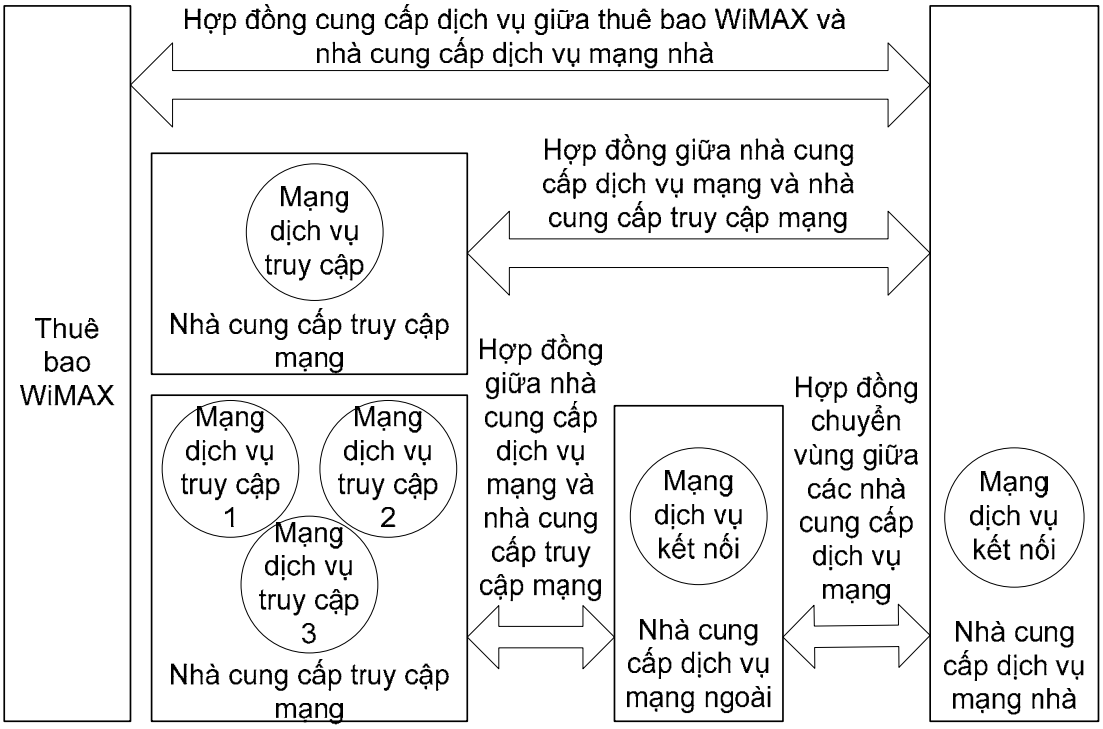


Hình 2.4 Mô hình tham chiếu mạng dịch vụ kết nối

2.2 Các đặc điểm khi triển khai

Trên thực tế, các thành phần tham gia vào mạng bao gồm:

- Thuê bao WiMAX
- Nhà cung cấp truy cập mạng
- Nhà cung cấp dịch vụ mạng



Hình 2.5 Quan hệ kinh tế giữa các thành phần khi triển khai

(Nguồn: [15], trang 1)

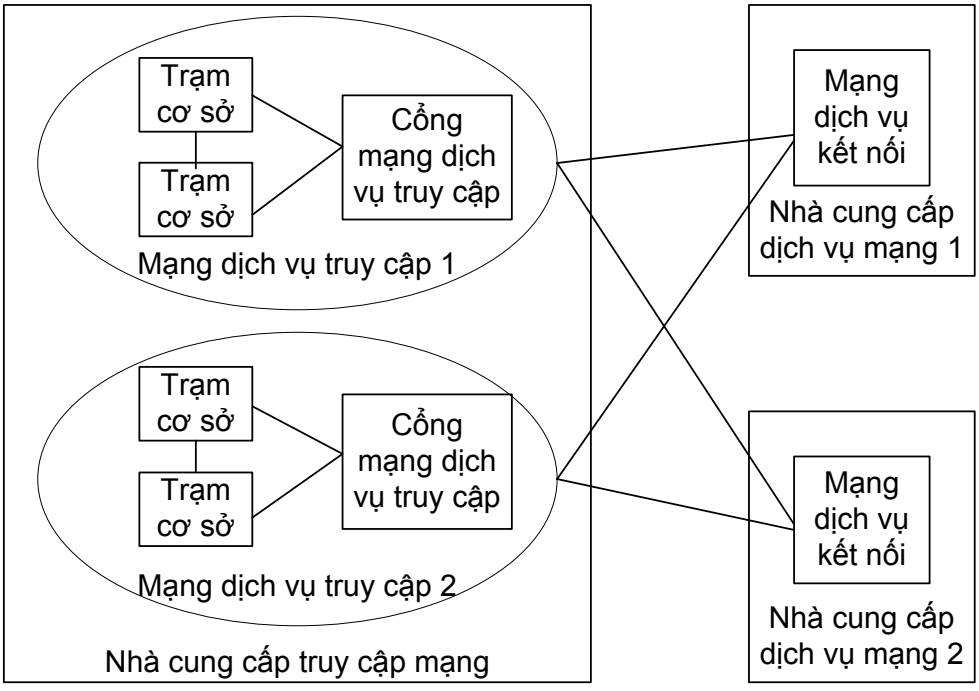
Hình vẽ 2.5 minh hoạ các quan hệ kinh tế giữa các thành phần. Quan hệ kinh tế giữa các thành phần này thể hiện dưới hình thức các hợp đồng sau:

- Hợp đồng cung cấp dịch vụ giữa thuê bao WiMAX và nhà cung cấp dịch vụ mạng nhà: Hợp đồng này cho phép thuê bao WiMAX truy cập tới tập các dịch vụ WiMAX và cho phép tính cước chính xác cho các dịch vụ bởi nhà cung cấp dịch vụ mạng nhà.
- Hợp đồng giữa nhà cung cấp dịch vụ mạng và nhà cung cấp truy cập mạng: Hợp đồng này cấp phép nhà cung cấp dịch vụ mạng sử dụng vùng bao phủ của nhà cung cấp truy cập mạng...
- Hợp đồng chuyển vùng giữa các nhà cung cấp dịch vụ mạng: Hợp đồng này thiết lập cam kết chuyển vùng giữa các nhà cung cấp dịch vụ mạng.

Các đặc điểm khi triển khai là:

- Nhà cung cấp truy cập mạng có thể triển khai một hoặc nhiều mạng dịch vụ truy cập.
- Một nhà cung cấp dịch vụ mạng có thể sử dụng nhiều nhà cung cấp truy cập mạng.
- Một mạng dịch vụ truy cập bao gồm các BS và cổng mạng dịch vụ truy cập.
- Một cổng mạng dịch vụ truy cập cung cấp kết nối tới một hoặc nhiều mạng dịch vụ kết nối. Các mạng dịch vụ kết nối đó có thể thuộc về cùng kiểu hoặc khác kiểu nhà cung cấp dịch vụ mạng. Ví dụ nhà cung cấp dịch vụ mạng 1 có thể là một nhà cung cấp dịch vụ mạng WiMAX thuần tuý, nhà cung cấp dịch vụ mạng 2 có thể là tổng đài 3G.

Hình vẽ 2.6 minh hoạ các đặc điểm trên.

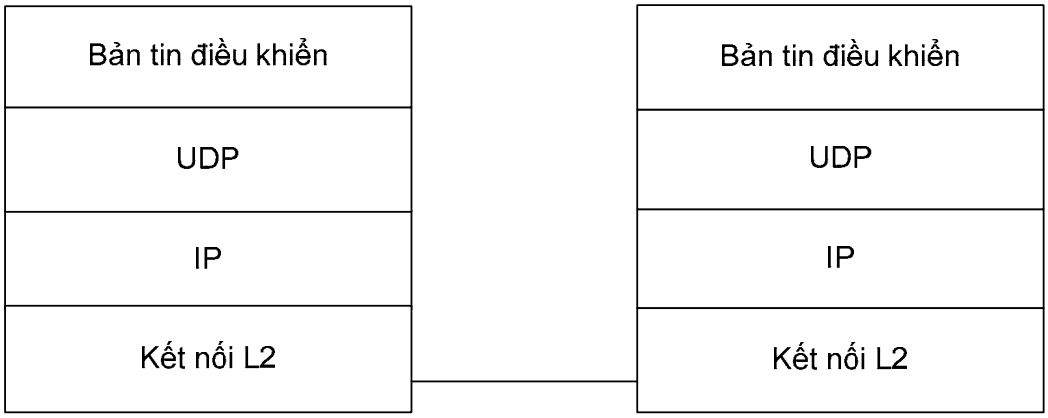


Hình 2.6 Quan hệ kết nối giữa các thành phần triển khai

2.3 Bản tin điều khiển

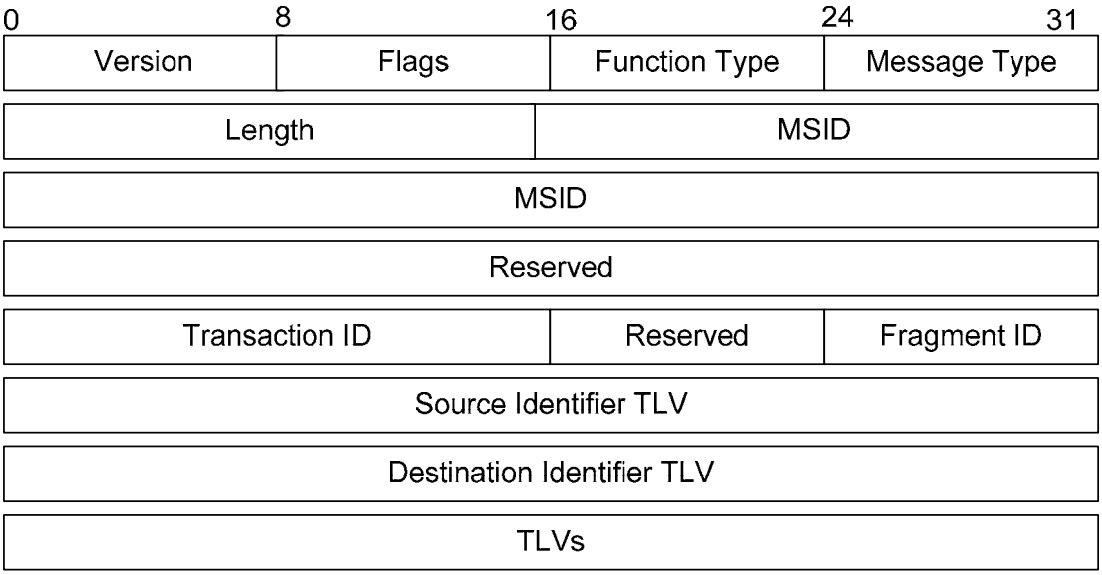
Các thực thể chức năng giao tiếp với nhau thực hiện các chức năng điều khiển. UDP/IP được sử dụng là giao thức giao vận cho việc truyền thông giữa các thực thể chức năng. Các thực thể chức năng tại mỗi điểm cuối được định danh bởi một địa chỉ IP và một giá trị cổng UDP. Các bản tin UDP/IP giữa các thực thể tại hai đầu có thể được chuyển qua đường hầm sử dụng các giao thức đóng gói nhưng việc thực hiện là trong suốt đối với các thực thể chức năng ở các điểm cuối. Khi các bản tin giữa các giữa các thực thể chức năng được chuyển qua thực thể trung gian thì bản tin vẫn là điểm tới điểm.

Ngăn xếp giao thức cho việc truyền thông các bản tin điều khiển minh hoạ trong hình 2.7. Kết nối L2/L3 biểu diễn đường truyền giữa các thực thể chức năng.



Hình 2.7 Ngăn xếp giao thức truyền thông các bản tin điều khiển

Hình 2.8 minh hoạ cấu trúc của bản tin điều khiển. Header của bản tin bắt đầu ngay sau UDP header.

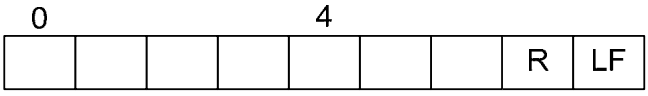


Hình 2.8 Cấu trúc bản tin điều khiển

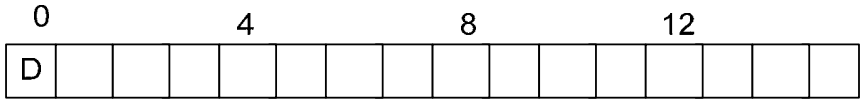
(Nguồn: [16], trang 4)

Ý nghĩa của các trường như sau:

- Version: Phiên bản giao thức có độ dài 1 byte. Phiên bản hiện tại là 1.
- Function Type: Kiểu chức năng có độ dài 1 byte. Ví dụ: chức năng chất lượng dịch vụ thì Function Type có giá trị bằng 1.
- Message Type: Kiểu bản tin có độ dài 1 byte.
- Flags: Có độ dài 1 byte. LF: Thiết lập chỉ phân đoạn cuối cùng của gói tin, R: khởi tạo lại giá trị phiên tiếp theo.



- Length: Chiều dài của bản tin (bao gồm cả header), đơn vị tính là byte. Độ dài trường là 2 byte.
- Transaction ID: Định danh của phiên, là một số 16 bít không dấu.



- MSID: Được thiết lập bằng 6 byte địa chỉ MAC của SS bản tin thuộc về. Đối với phiên không cần thông tin này, các bít được đặt giá trị bằng 0.
- Fragmentation ID: Độ dài 8 bit, bắt đầu bằng 1 và tăng cho mỗi phân đoạn. Sự phân đoạn sử dụng bởi các bản tin ứng dụng khi độ dài vượt quá 1 bản tin UDP.
- Reserved: 8 bits, chưa sử dụng
- TLVs: Mã hoá Type-Length-Value của các phần tử thông tin.
- Source Identifiers TLV và Destination Identifiers xác định các thực thể lôgíc liên quan tới việc xử lý bản tin.

Các lưu ý về sử dụng Transaction ID:

- Transaction ID phải là duy nhất đối với Source, Destination, MSID.
- Transaction ID phải bắt đầu từ 1 cho mọi truyền thông Source, Destination, MSID.
- Transaction ID phải giống nhau cho chuỗi bản tin Request/Response/Ack trong trường hợp bắt tay 3 chiều hoặc Request/Response trong trường hợp bắt tay 2 chiều. Mọi sự truyền lại thiết lập cùng Transaction ID. Đối với transaction/Request tiếp theo, Transaction ID phải tăng 1. Nếu tăng dẫn tới 0 thì phải thiết lập bằng 1. Các phân đoạn của cùng 1 bản tin có cùng Transaction ID.
- Để tránh sử dụng Transaction ID giống nhau ở hai hướng, bên gửi (Source hoặc Destination) với địa chỉ IP cao hơn sẽ thiết lập bít D của Transaction ID bằng 1, bên gửi có địa chỉ IP thấp hơn sẽ thiết lập bít D của Transaction ID bằng 0.

- Bên gửi (Source) được phép khởi tạo không giới hạn số transation đồng thời cho các SS khác nhau, giá sử rằng không quá 1 transaction cho một SS.
- Bên gửi (Source) được phép khởi tạo nhiều transaction đồng thời cho cùng một SS (với Transaction ID khác nhau). Tuy vậy, bên nhận (Destination) không được phép xử lý transaction có cùng MS ID mà mất thứ tự. Để hỗ trợ cài đặt các bên nhận khác nhau, bên gửi nên cấu hình tối đa số transaction đồng thời cho cùng một MS ID.
- Các bản tin transaction có bít R thiết lập bằng 1 sẽ khởi tạo lại mọi transaction chưa hoàn thành, bên nhận sẽ thiết lập Transaction ID tiếp theo bằng Transaction ID trong bản tin đã nhận cộng 1.

2.4 Kết chương

Trong chương này, chúng ta đã nghiên cứu về mô hình lý thuyết của kiến trúc mạng WiMAX bao gồm các thực thể chức năng và các điểm tham chiếu. Trong đó, chúng ta đi sâu nghiên cứu phân rã mô hình mạng dịch vụ truy cập và mạng dịch vụ kết nối. Trong phần các đặc điểm khi triển khai, chúng ta đã nghiên cứu quan hệ kinh tế và quan hệ kết nối giữa các thành phần triển khai. Cuối cùng, chúng ta nghiên cứu về cấu trúc bản tin điều khiển mà các thực thể chức năng giao tiếp với nhau. Trong chương tiếp theo, chúng ta sẽ đi sâu nghiên cứu về vấn đề chất lượng dịch vụ trong mạng WiMAX.

Chương 3.
VẤN ĐỀ CHẤT LƯỢNG DỊCH VỤ

3.1 Yêu cầu và đặc điểm chung

Phạm vi của phần chất lượng dịch vụ tập trung vào kết nối sóng vô tuyến của WiMAX. Để đảm bảo chất lượng dịch vụ, diễn đàn WiMAX định nghĩa một khung làm việc để đảm bảo chất lượng dịch vụ. Yêu cầu đối với khung làm việc đó là:

- Cung cấp các mức khác nhau và mức tốt nhất của chất lượng dịch vụ cho thuê bao
- Kiểm soát cho phép một yêu cầu mới dựa trên kiểm tra tài nguyên hiện có
- Quản lý băng thông
- Kiến trúc sẽ hỗ trợ các phương tiện khác nhau để thực hiện các chính sách như đã định nghĩa bởi các tổng đài cho chất lượng dịch vụ dựa trên các bản cam kết mức độ dịch vụ của họ, nó có thể đòi hỏi thực hiện chính sách cho người sử dụng và nhóm người sử dụng cũng như các yếu tố như vị trí, thời gian trong ngày,… Chính sách chất lượng dịch vụ có thể được đồng bộ giữa các tổng đài phụ thuộc vào bản cam kết mức độ dịch vụ của thuê bao.
- Kiến trúc sẽ sử dụng các cơ chế chuẩn IETF cho việc quản lý định nghĩa chính sách và thực hiện chính sách giữa các tổng đài.

Chuẩn IEEE 802.16 định nghĩa khung làm việc đảm bảo chất lượng dịch vụ cho giao diện không khí. Theo IEEE 802.16, một đăng ký được liên kết với một số luồng dịch vụ mô tả bởi các tham số chất lượng dịch vụ. Thông tin này sẽ được cung cấp trong hệ thống quản lý thuê bao (ví dụ cơ sở dữ liệu của server xác thực, uỷ quyền và kế toán) hoặc server chính sách. Theo mô hình dịch vụ tĩnh, SS không được phép thay đổi các tham số của các luồng dịch vụ cung cấp hoặc tạo các luồng dịch vụ mới động. Theo mô hình dịch vụ động,

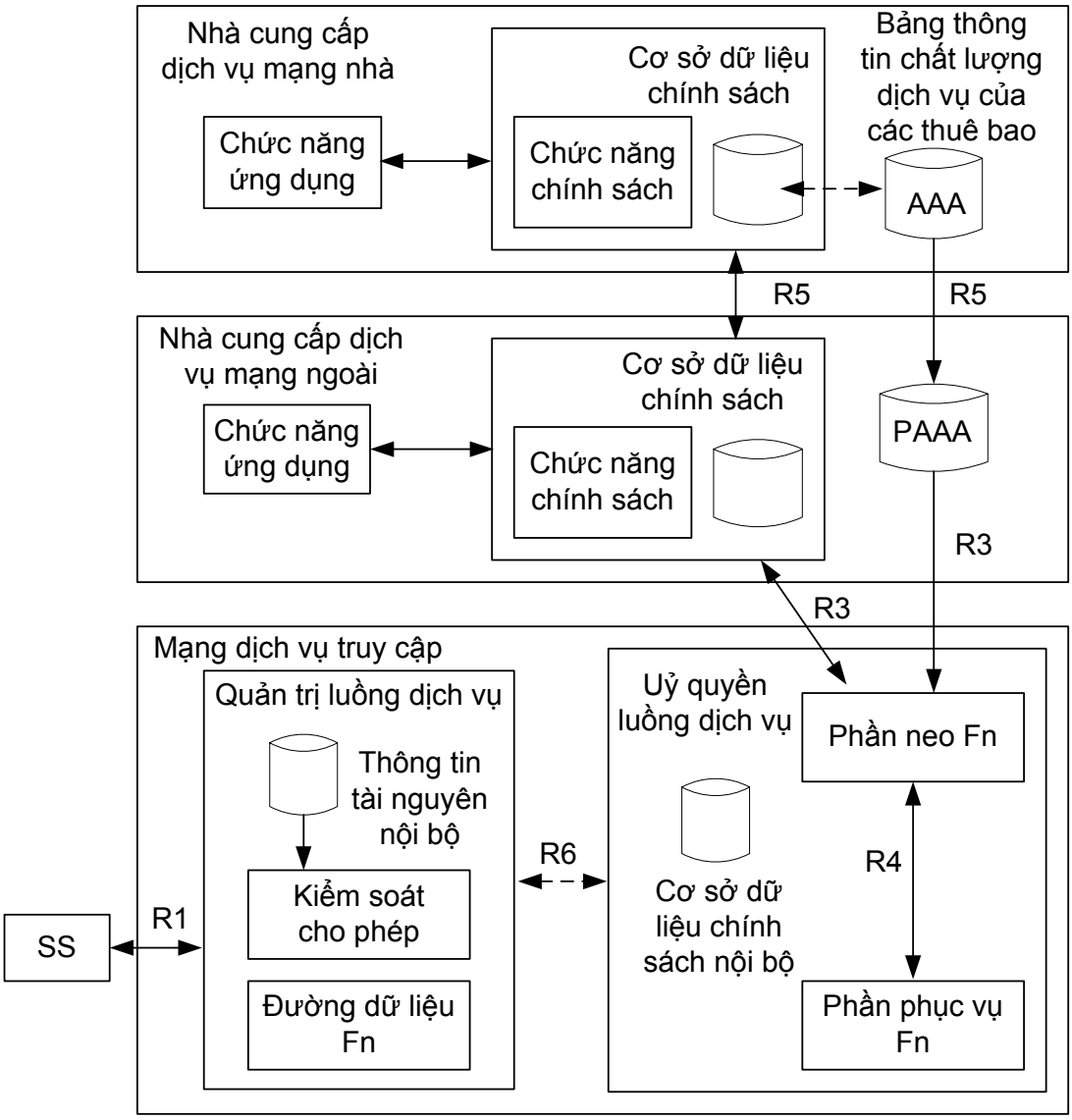
SS hoặc BS có thể tạo, thay đổi hoặc xóa các luồng dịch vụ động. Trong trường hợp này, một yêu cầu dịch vụ động được đánh giá dựa vào thông tin được cung cấp để quyết định yêu cầu có được cấp phép hay không. Chi tiết hơn chúng ta sẽ tìm hiểu trong phần 3.3.

Diễn đàn WiMAX mở rộng khung làm việc QoS trong đặc tả IEEE 802.16 cho kiến trúc tham chiếu của mạng WiMAX. Diễn đàn WiMAX không giải quyết sự cung cấp chất lượng dịch vụ trong mạng truy cập và mạng lõi. Tuy nhiên, trong phiên bản 1 diễn đàn WiMAX chưa định nghĩa tạo luồng dịch vụ động, chưa định nghĩa giao diện giữa thực thể chức năng chính sách và thực thể uỷ quyền luồng dịch vụ.

3.2 Mô hình chất lượng dịch vụ

Mô hình chất lượng dịch vụ được xây dựng dựa trên yêu cầu đảm bảo chất lượng dịch vụ, dựa trên đặc tả IEEE 802.16 và mô hình tham chiếu kiến trúc (như mô tả trong phần 2.1). Mô hình bao gồm các phần tử chức năng sau: thực thể thực hiện chức năng chính sách, thực thể quản trị luồng dịch vụ, thực thể uỷ quyền luồng dịch vụ, thực thể xác thực uỷ quyền kế toán.

Hình 3.1 minh hoạ các thực thể chức năng trong mô hình chất lượng dịch vụ. Trong hình vẽ, các mũi tên đứt nét thể hiện diễn đàn WiMAX vẫn chưa thống nhất về cách thức giao tiếp.



Hình 3.1 Mô hình đảm bảo chất lượng dịch vụ

(Nguồn: [14], trang 42)

Chức năng chính sách nhà và cơ sở dữ liệu chính sách liên kết với chức năng chính sách nhà thuộc về nhà cung cấp dịch vụ mạng nhà. Các thông tin được duy trì bao gồm các luật chính sách chung của nhà cung cấp dịch vụ mạng nhà cũng như các luật chính sách phụ thuộc vào ứng dụng. Ngoài ra, cơ sở dữ liệu của chức năng xác thực uỷ quyền và kế toán có thể cung cấp cơ sở dữ liệu của chức năng chính sách về bảng mô tả thông tin chất lượng dịch vụ

của người sử dụng và các chính sách liên quan. Tuy vậy, tương tác giữa chức năng chính sách và chức năng xác thực uỷ quyền và kế toán chưa được diễn đàn WiMAX đưa ra. Chức năng chính sách có nhiệm vụ đánh giá các yêu cầu dịch vụ dựa vào các chính sách đó. SS giao tiếp trực tiếp với chức năng ứng dụng sử dụng các giao thức điều khiển của lớp ứng dụng và chức năng ứng dụng xem xét kích hoạt luồng dịch vụ WiMAX tới chức năng chính sách (trong trường hợp chuyển vùng, chức năng ứng dụng có thể được chứa tại nhà cung cấp dịch vụ mạng nhà cũng như thông qua nhà cung cấp dịch vụ mạng ngoài nơi chức năng chính sách kích hoạt).

Thực thể quản trị luồng dịch vụ nằm trong mạng dịch vụ truy cập. Phần tử quản trị luồng dịch vụ có vai trò trong việc tạo, cho phép, kích hoạt, sửa đổi và xóa các luồng dịch vụ 802.16. Thực thể quản trị luồng dịch vụ luôn nằm tại BS. Nó bao gồm một chức năng kiểm soát cho phép, thông tin tài nguyên nội bộ liên quan và chức năng tạo đường dữ liệu. Trong đó:

- Chức năng kiểm soát cho phép sử dụng để quyết định một luồng dịch vụ mới có được chấp nhận hay không dựa vào mức độ sử dụng sóng vô tuyến và các tài nguyên nội bộ khác hiện tại.
- Chức năng tạo đường dữ liệu quản lý việc thiết lập không gian vận chuyển giữa các thực thể ví dụ như tạo đường hầm giữa hai thực thể sử dụng các giao thức tạo đường hầm như RFC 2003, RFC 2004.

Thực thể uỷ quyền luồng dịch vụ nằm trong mạng dịch vụ truy cập. Nó bao gồm phần neo và phần phục vụ. Trong đó:

- Phần neo của thực thể uỷ quyền luồng dịch vụ được gán cho mỗi SS sau khi SS đăng ký thành công. Phần neo của thực thể uỷ quyền luồng dịch vụ không thay đổi cho khoảng thời gian phiên xác thực SS.
- Một hoặc nhiều thực thể uỷ quyền luồng dịch vụ chuyển tiếp các

yêu cầu chất lượng dịch vụ và áp dụng các chính sách chất lượng dịch vụ cho một SS. Thực thể chuyển tiếp sự uỷ quyền luồng dịch vụ mà trực tiếp giao tiếp với thực thể quản trị luồng dịch vụ gọi là phần phục vụ của thực thể uỷ quyền luồng dịch vụ (khi không có sự chuyển tiếp, phần neo của thực thể uỷ quyền luồng dịch vụ cũng là phần phục vụ).

Trong trường hợp bảng thông tin chất lượng dịch vụ của người sử dụng được tải từ thực thể xác thực uỷ quyền và kế toán về thực thể uỷ quyền luồng dịch vụ tại pha vào mạng, thực thể uỷ quyền luồng dịch vụ có vai trò đánh giá yêu cầu dịch vụ dựa trên bảng thông tin chất lượng dịch vụ của người sử dụng.

Định danh của phần phục vụ nếu khác phần neo, phần neo phải biết định danh này. Tương tự, phần phục vụ phải biết định danh của phần neo. Phần neo và phần phục vụ của thực thể uỷ quyền luồng dịch vụ cũng thực hiện sự ép buộc chính sách mức mạng dịch vụ truy cập sử dụng cơ sở dữ liệu chính sách nội bộ và một chức năng chính sách nội bộ liên quan. Chức năng chính sách nội bộ cũng có thể được sử dụng để ép buộc kiểm soát cho phép dựa trên các tài nguyên khả dụng. Sự thực hiện điều này là nội bộ đối với thực thể uỷ quyền luồng dịch vụ và đặc tả không quy định.

Thực thể xác thực uỷ quyền và kế toán giữ bảng thông tin chất lượng dịch vụ của người sử dụng và các luật chính sách liên quan. Thông tin này có thể được sử dụng một trong hai cách:

- Chúng có thể được tải xuống phần uỷ quyền luồng dịch vụ tại điểm vào mạng như một phần của thủ tục xác thực và uỷ quyền.
- Chúng có thể được cung cấp trong chức năng chính sách, tùy chọn này không nằm trong phiên bản WiMAX 1.0.

Như vậy, chúng ta nhận thấy rằng:

- Nếu theo cách 1 thì thực thể uỷ quyền luồng dịch vụ đánh giá yêu

cầu dịch vụ sắp đến dựa trên bảng thông tin của người sử dụng.

- Nếu theo cách 2 thì việc đánh giá yêu cầu dịch vụ được đưa đến chức năng chính sách nhà.

3.3 Cơ chế đảm bảo chất lượng dịch vụ của IEEE 802.16

Trong các phần trên chúng ta đã nghiên cứu về cơ chế đảm bảo chất lượng dịch vụ của các lớp trên MAC. Trong phần này, chúng ta sẽ tìm hiểu cơ chế đảm bảo chất lượng dịch vụ tại mức MAC, nghĩa là cơ chế đảm bảo chất lượng dịch vụ IEEE 802.16 định nghĩa. Chuẩn IEEE 802.16 định nghĩa các phương pháp hỗ trợ dịch vụ sau:

- Phân loại luồng dịch vụ
- Quản trị luồng dịch vụ động
- Mô hình kích hoạt 2 pha

3.3.1 Phân loại luồng dịch vụ

Đặc điểm chính của việc cung cấp chất lượng dịch vụ của 802.16 khác với các chuẩn công nghệ khác (802.11 và 3G) là nó liên kết mỗi gói tin với một luồng dịch vụ. MAC của 802.16 là hướng kết nối. Mỗi kết nối có một định danh kết nối (CID) và một định danh luồng dịch vụ (SFID) của một lớp dịch vụ. Các lớp trên của MAC ánh xạ dữ liệu vào lớp dịch vụ. Các ứng dụng có thể yêu cầu các luồng dịch vụ với các tham số chất lượng dịch vụ mong muốn thông qua lớp dịch vụ. Khi ứng dụng muốn gửi gói tin, luồng dịch vụ được ánh xạ tới kết nối qua định danh kết nối. 802.16 cung cấp 4 kiểu dịch vụ lập lịch, mỗi kiểu liên kết với một lớp dịch vụ. Chúng ta sẽ tìm hiểu chi tiết về

lớp dịch vụ, luồng dịch vụ, kiểu dịch vụ lập lịch.

Lớp dịch vụ chứa tập tham số chất lượng dịch vụ. Tên của lớp dịch vụ là một chuỗi ASCII. Lớp dịch vụ sử dụng để thay vì việc định nghĩa từng tham số chất lượng dịch vụ của luồng dịch vụ, các lớp trên và các ứng dụng ngoài có thế sử dụng tên lớp dịch vụ. Luồng dịch vụ có thể định nghĩa từng tham số chất lượng dịch vụ hoặc có thể sử dụng một lớp dịch vụ đã định nghĩa tập tham số chất lượng dịch vụ hoặc sử dụng một lớp dịch vụ với một tập tham số chất lượng dịch vụ được sửa đổi.

Luồng dịch vụ là một trong những thành phần quan trọng nhất của lớp MAC. Luồng dịch vụ sử dụng như dịch vụ giao vận để chuyển các gói tin, cung cấp chất lượng dịch vụ cho các gói tin. Mỗi luồng dịch vụ có một tập các tham số chất lượng dịch vụ. Một luồng dịch vụ có thể sử dụng bởi nhiều gói tin. Luồng dịch vụ là một chiều, nó có thể sử dụng bởi BS dành cho SS hoặc SS dành cho BS. Luồng dịch vụ có 32 bít định danh, gọi là SFID.

IEEE 802.16 cung cấp 4 kiểu dịch vụ lập lịch:

- Dịch vụ cấp không phải yêu cầu (Unsolicited Grant Services - UGS): Dịch vụ này hỗ trợ tốc độ bít hằng số (CBR) như VoIP. Các ứng dụng này đòi hỏi cấp phát băng thông hằng số.
- Dịch vụ thăm dò thời gian thực (Real-Time Polling Services - rtPS): Dịch vụ này hỗ trợ cho các dịch vụ tốc độ bít thay đổi thời gian thực như MPEG video. Các ứng dụng này có các yêu cầu băng thông cụ thể cũng như độ trễ lớn nhất. Các gói tin đến chậm mà quá thời gian độ trễ lớn nhất cho phép sẽ bị bỏ qua.
- Dịch vụ thăm dò không phải thời gian thực (Non-Real-Time Polling Services - nrtPS): Dịch vụ này cho các luồng không phải thời gian thực, nó đòi hỏi tốt hơn dịch vụ Best Effort ví dụ truyền tập tin băng thông cao. Các ứng dụng này không cần thời gian thực và đòi

hỏi cấp phát băng thông tối thiểu.

- Dịch vụ cố gắng tốt nhất (Best Effort Services - BE): Dịch vụ này không cung cấp sự đảm bảo nào nhưng người sử dụng có thể sử dụng tốc độ dữ liệu tối đa. Dịch vụ này hỗ trợ các dịch vụ không phải thời gian thực như duyệt web.

3.3.2 Quản trị luồng dịch vụ động

Cơ chế này cho phép tạo mới một luồng dịch vụ, thay đổi một luồng dịch vụ, xoá một luồng dịch vụ khi cần. Nhiều luồng dịch vụ có thể được cấp cho cùng một ứng dụng vì thế các luồng dịch vụ có thể thêm nếu cần. Việc quản trị luồng dịch vụ động thực hiện thông qua các giao dịch. Sau đây, chúng ta sẽ tìm hiểu lần lượt các vấn đề về giao dịch, cơ chế thực hiện tạo, thay đổi và xoá luồng dịch vụ.

3.3.2.1 Giao dịch

Mỗi giao dịch có một định danh duy nhất. Để phân biệt giữa các giao dịch khởi tạo bởi BS và SS, SS sử dụng giá trị định danh giao dịch từ 0000 tới 7FFF, BS sử dụng giá trị định danh giao dịch từ 8000 tới FFFF.

Có tổng cộng 6 kiểu giao dịch, các giao dịch đó được khởi tạo nội bộ hoặc khởi tạo từ xa cho mỗi bản tin DSA, DSC và DSD. Bản tin DSA sử dụng để tạo mới luồng dịch vụ, bản tin DSC sử dụng để thay đổi luồng dịch vụ, bản tin DSD sử dụng để xoá luồng dịch vụ.

Một giao dịch có 3 trạng thái là pending, holding và deleting. Trong trạng thái pending, giao dịch đợi một trả lời. Trong trạng thái holding, giao dịch đã nhận một trả lời và giữ bản tin đó để có thể gửi lại trong trường hợp mất bản tin. Trong trạng thái deleting, giao dịch xoá luồng dịch vụ đang được

xử lý.

Có 2 mức xử lý thông qua 2 kiểu sơ đồ trạng thái: Sơ đồ chuyển trạng thái luồng dịch vụ động và sơ đồ chuyển trạng thái DSx (6 sơ đồ). Yêu cầu thêm, thay đổi, xoá luồng dịch vụ được chuyển tới mức sơ đồ chuyển trạng thái luồng dịch vụ động. Qua sơ đồ này, các bản tin DSx được chuyển tới sơ đồ chuyển trạng thái DSx thích hợp.

Sơ đồ chuyển trạng thái luồng dịch vụ động có thể gửi một trong các đầu vào sau tới sơ đồ chuyển trạng thái DSx, đó là SF Add, SF Change, SF Delete, SF Abort Add, SF Change-Remote, SF Delete-Local ,SF Delete-Remote, SF DSA-ACK Lost, DSA-REQ Lost, DSC-ACK Lost và DSC-REQ Lost.

Tương tự, trong trả lời tới đầu vào từ sơ đồ chuyển trạng thái luồng dịch vụ động và kết quả của quá trình xử lý đã được thực hiện trong sơ đồ chuyển trạng thái DSx. Sơ đồ chuyển trạng thái DSx gửi trở lại một trong các bản tin sau: DSA Succeed, DSA Failed, DSA ACK Lost, DSA Erred, DSA Ended, DSC Succeeded, DSC Failed, DSC ACK Lost, DSC Erred, DSC Ended, DSD Succeeded, DSD Erred, DSD Ended.

Luồng dịch vụ động có trạng thái null hoặc normal. Trong trạng thái null, không có luồng dịch vụ nào tồn tại tương ứng với SFID hoặc định danh giao dịch của bản tin giao dịch. Để chuyển luồng dịch vụ từ trạng thái null sang trạng thái normal sử dụng bản tin DSA. Luồng dịch vụ có một SFID được gán khi luồng dịch vụ tồn tại. Trong trạng thái normal, nó có thể thay đổi nhiều lần sử dụng bản tin DSC. Luồng dịch vụ quay lại trạng thái null khi bản tin DSD được sử dụng.

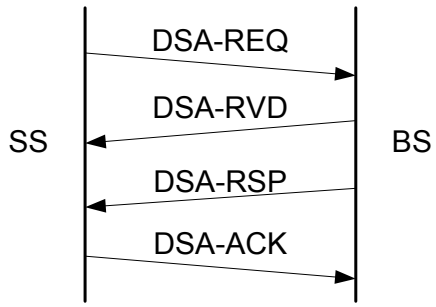
3.3.2.2 Tạo luồng dịch vụ động

Tạo luồng dịch vụ động có thể được khởi tạo bởi BS hoặc SS. Chúng gửi tập tham số chất lượng dịch vụ của luồng dịch vụ mới, một cho luồng dịch vụ

đường lên và/hoặc một cho luồng dịch vụ đường xuống trong bản tin DSA.

Quá trình tạo mới thành công luồng dịch vụ động bởi SS như sau:

- Đầu tiên, SS kiểm tra tài nguyên cho luồng dịch vụ mới là khả dụng thì gửi bản tin DSA-REQ với tập tham số chất lượng dịch vụ tới BS. SS thiết lập đồng hồ thời gian T7 và một đồng hồ thời gian T14.
- BS nhận được bản tin DSA-REQ, BS kiểm tra sự hợp lệ của bản tin và gửi DSA-RVD tới SS.
- SS nhận được bản tin DSA-RVD sẽ dừng đồng hồ T14.
- BS kiểm tra SS có được cấp phép dịch vụ không, kiểm tra tài nguyên khả dụng. Nếu mọi kiểm tra thành công thì BS tạo SFID. Đối với yêu cầu cho phép đường lên, BS ánh xạ luồng dịch vụ tới CID. Đối với yêu cầu kích hoạt đường lên thì BS cho phép nhận dữ liệu qua luồng dịch vụ mới. Sau đó, BS gửi DSA-RSP tới SS.
- SS nhận được DSA-RSP thì SS dừng đồng hồ T7. Đối với yêu cầu kích hoạt thì SS cho phép việc truyền/nhận dữ liệu qua luồng dịch vụ đường lên/đường xuống. SS gửi DSA-ACK tới BS.
- BS nhận được DSA-ACK, BS cho phép truyền dữ liệu qua các luồng dịch vụ đường xuống mới nếu nó là một yêu cầu kích hoạt.



Hình 3.2 Tạo mới luồng dịch vụ động bởi SS

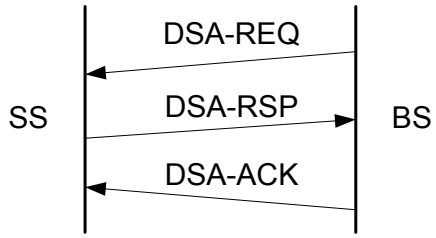
Quá trình tạo mới thành công luồng dịch vụ động bởi BS như sau:

- BS thực hiện kiểm tra SS cần luồng dịch vụ mới hay không, kiểm

tra SS có được cấp phép cho luồng dịch vụ hay không, kiểm tra tài nguyên khả dụng. Nếu mọi kiểm tra thành công thì BS tạo SFID. Đối với yêu cầu cho phép, BS ánh xạ luồng dịch vụ với CID. BS gửi DSA-REQ và thiết lập đồng hồ T7.

- SS kiểm tra nó có thể hỗ trợ dịch vụ hay không. Đối với yêu cầu kích hoạt, SS cho phép nhận dữ liệu qua luồng dịch vụ mới. SS gửi DSA-RSP tới BS.
- BS nhận được DSA-RSP, BS chấm dứt đồng hồ T17. Đối với yêu cầu kích hoạt đường xuống thì BS cho phép truyền dữ liệu qua luồng dịch vụ mới. Đối với yêu cầu kích hoạt đường lên thì BS cho phép nhận dữ liệu qua luồng dịch vụ mới. Sau đó, BS gửi DSA-ACK tới SS.
- SS nhận được DSA-ACK thì SS cho phép truyền dữ liệu qua luồng dịch vụ mới nếu nó là yêu cầu kích hoạt đường lên.

Quá trình tạo mới luồng dịch vụ động bởi BS được minh hoạ như trong hình 3.3.



Hình 3.3 Tạo mới luồng dịch vụ động bởi BS

3.3.2.3 Thay đổi luồng dịch vụ động

Quá trình thay đổi luồng dịch vụ động sử dụng bản tin DSC. Quá trình này sử dụng để:

- Thay đổi luồng dịch vụ cung cấp thành luồng dịch vụ cho phép và

luồng dịch vụ cho phép thành luồng dịch vụ kích hoạt.

- Thay đổi tập tham số chất lượng dịch vụ của luồng dịch vụ cho phép và luồng dịch vụ kích hoạt.

Các trường hợp xử lý bao gồm:

- Nếu bản tin DSC không chứa tập tham số chất lượng dịch vụ thì tập tham số chất lượng dịch vụ kích hoạt và cho phép của luồng dịch vụ thiết lập thành null và luồng dịch vụ sẽ không được cấp phép.
- Nếu bản tin DSC chỉ chứa tập tham số chất lượng dịch vụ cho phép thì tập tham số chất lượng dịch vụ cho phép của luồng dịch vụ bị sửa đổi và luồng dịch vụ sẽ không được kích hoạt.
- Nếu bản tin DSC chứa tập tham số chất lượng dịch vụ cho phép và kích hoạt, tập tham số chất lượng dịch vụ cho phép của luồng dịch vụ bị sửa đổi và nếu tập tham số chất lượng dịch vụ kích hoạt trong bản tin là tập con của tập tham số chất lượng dịch vụ cho phép của luồng dịch vụ thì tập tham số chất lượng dịch vụ kích hoạt của luồng dịch vụ bị thay thế bởi tập tham số chất lượng dịch vụ kích hoạt trong bản tin DSC.

Quá trình thay đổi thành công luồng dịch vụ bởi SS như sau:

- Nếu SS cần thay đổi luồng dịch vụ, nó gửi tập tham số chất lượng dịch vụ sửa đổi trong bản tin DSC-REQ tới BS và thiết lập đồng hồ T7 và T14.
- BS kiểm tra sự hợp lệ của bản tin và gửi DSC-RVD tới SS.
- SS chấm dứt đồng hồ T14.
- BS kiểm tra tài nguyên khả dụng và sửa đổi luồng dịch vụ. BS tăng băng thông của kênh nếu cần thiết và gửi DSC-RSP tới SS.
- SS chấm dứt đồng hồ T7 và sửa đổi luồng dịch vụ. SS thay đổi băng thông của dữ liệu tải và gửi DSC-ACK tới BS.

- BS giảm băng thông của kênh nếu cần thiết. Sơ đồ thay đổi dịch vụ thông tương tự với hình 3.2 trong đó thay DSA bởi DSC.

Quá trình thay đổi thành công luồng dịch vụ bởi BS như sau:

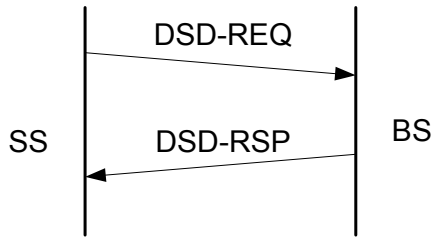
- Nếu BS muốn sửa đổi luồng dịch vụ thì đầu tiên nó kiểm tra nó có hỗ trợ thay đổi hay không. BS gửi DSC-REQ tới SS và thiết lập đồng T7.
- SS nhận DSC-REQ và kiểm tra tài nguyên khả dụng, rồi sửa đổi luồng dịch vụ. SS giảm băng thông của dữ liệu tải nếu cần thiết. SS gửi DSC-RSP tới BS.
- BS thay đổi băng thông kênh và gửi DSC-ACK tới SS.
- SS tăng băng thông của dữ liệu tải nếu cần thiết. Sơ đồ thay đổi dịch vụ động tương tự với hình 3.3, trong đó thay DSA bởi DSC.

3.3.2.4 Xoá luồng dịch vụ động

Quá xoá luồng dịch vụ sử dụng bản tin DSD. Tài nguyên dành cho luồng dịch vụ được giải phóng sau khi xoá.

Quá trình xoá thành công luồng dịch vụ động bởi SS như sau:

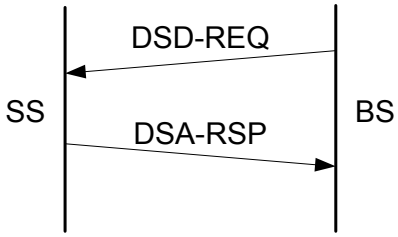
- Nếu SS không cần luồng dịch vụ thì nó xoá luồng dịch vụ đó. SS gửi DSD-REQ tới BS.
- BS kiểm tra nếu SS là chủ của luồng dịch vụ thì xoá luồng dịch vụ và gửi DSD-RSP tới SS.



Hình 3.4 Xoá luồng dịch vụ động bởi SS

Quá trình xoá thành công luồng dịch vụ động bởi BS như sau:

- Nếu BS không cần luồng dịch vụ thì nó xoá luồng dịch vụ. BS kiểm tra nếu SS liên kết với luồng dịch vụ thì BS gửi DSD-REQ tới SS.
- SS xoá luồng dịch vụ và gửi DSD-RSP tới BS.



Hình 3.5 Xoá luồng dịch vụ động bởi BS

3.3.3 Mô hình kích hoạt 2 pha

Mô hình kích hoạt 2 pha nhằm ngăn chặn sự mất mát tài nguyên. Sự kích hoạt một luồng dịch vụ được xử lý qua hai pha: Pha cấp phép và pha kích hoạt. Khi luồng dịch vụ được cấp phép thì BS và SS dành tài nguyên cho nó. Khi luồng dịch vụ được kích hoạt thì BS và SS có thể gửi nhận dữ liệu qua luồng dịch vụ đó.

Tập tham số chất lượng dịch vụ liên kết với mỗi luồng dịch vụ. Kiểu của tập tham số chất lượng dịch vụ phân biệt trạng thái của luồng dịch vụ do mô đun uỷ quyền xác định (cấp phép hoặc kích hoạt). IEEE 802.16 định nghĩa 3 kiểu tập tham số chất lượng dịch vụ:

- ProvisionedQoSParamSet: Tập các tham số chất lượng dịch vụ cung cấp bởi hệ thống quản trị mạng.
- AdmittedQoSParamSet: Tập các tham số chất lượng dịch vụ mà BS, SS dành tài nguyên cho luồng dịch vụ liên kết với tập tham số này.
- ActiveQoSParamSet: Tập tham số chất lượng dịch vụ phản ánh dịch vụ hiện tại đang được cung cấp.

Sự kích hoạt luồng dịch xử lý bởi mô đun uỷ quyền trong BS. Mô đun uỷ quyền có hai mô hình xử lý:

- Uỷ quyền tĩnh (Provisioned Authorization): Tập tham số chất lượng dịch vụ được cung cấp bởi hệ thống quản trị mạng, không thay đổi động được bởi BS và SS.
- Uỷ quyền động (Dynamic Authorization): Tập tham số chất lượng dịch vụ có thể thay đổi và được duyệt bởi mô đun uỷ quyền.

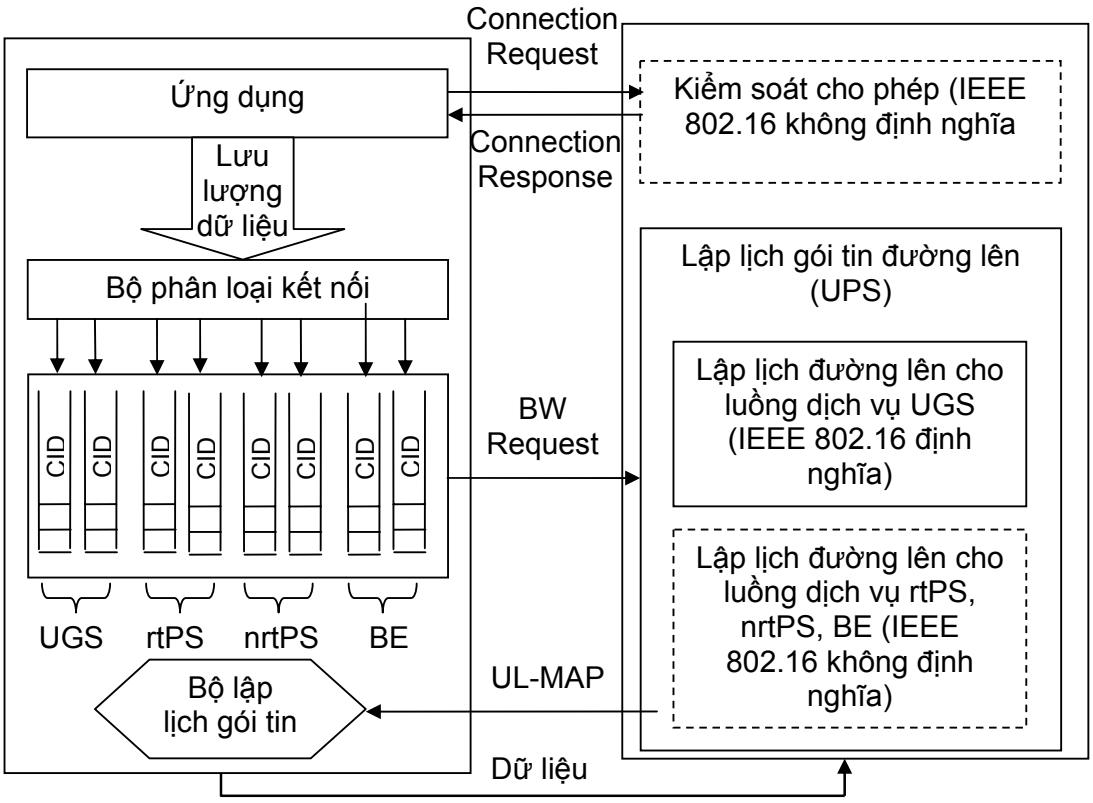
3.4 Hoàn thiện giải pháp chất lượng dịch vụ trong IEEE 802.16

Kiến trúc đảm bảo chất lượng dịch vụ của các lớp trên đang được diễn đàn WiMAX xây dựng, chưa được hoàn thiện và công bố. Vì thế, chúng ta tập trung phân tích vấn đề hỗ trợ chất lượng dịch vụ tại mức MAC do chuẩn 802.16 định nghĩa.

3.4.1 Phân tích vấn đề

IEEE 802.16 hỗ trợ nhiều dịch vụ truyền thông (dữ liệu, tiếng nói, truyền hình) với các yêu cầu chất lượng dịch vụ khác nhau. Lớp MAC định nghĩa các cơ chế báo hiệu chất lượng dịch vụ và các chức năng điều khiển việc truyền dữ liệu của BS và SS. Trên hướng xuống, việc truyền thông tương đối đơn giản vì BS là thành phần duy nhất truyền trong các khung con đường xuống. Các gói tin được truyền quảng bá tới mọi SS và SS chỉ nhận các gói tin có địa chỉ đích là nó. Vì thế chúng ta chỉ tập trung xem xét vấn đề lập lịch đường lên. Trên hướng lên, khi sử dụng ghép kênh theo thời gian, BS xác định số khe thời gian mà mỗi SS sẽ được phép truyền trong một khung con

đường lên. BS quảng bá thông tin này qua bản tin UL-MAP tại vị trí bắt đầu mỗi khung. UL-MAP chứa các phần tử thông tin. Các phần tử thông tin chứa các cơ hội truyền, nghĩa là các khe thời gian mà SS có thể truyền trong khung con đường lên. Sau khi nhận UL-MAP, mỗi SS sẽ truyền dữ liệu trong các khe thời gian đã định nghĩa trong các phần tử thông tin. Mô đun lập lịch đường lên tại BS xác định các phần tử thông tin dựa trên các BW-request mà SS gửi tới. IEEE 802.16 định nghĩa các cơ chế báo hiệu chất lượng dịch vụ nhưng nó không định nghĩa bộ lập lịch đường lên. Hình 3.6 minh hoạ kiến trúc chất lượng dịch vụ đường lên của IEEE 802.16. Trong đó, những phần vẽ nét đứt là những phần mà IEEE 802.16 không định nghĩa. Hình 3.6 cho thấy kiến trúc chất lượng dịch vụ đường lên hiện tại của IEEE 802.16.



Hình 3.6 Kiến trúc chất lượng dịch vụ đường lên của IEEE 802.16

Trong hình 3.6, chúng ta có các điểm chú ý sau:

- Lập lịch gói tin đường lên (UPS) nằm trong BS để điều khiển toàn bộ việc truyền gói tin đường lên.
- Vì giao thức MAC của IEEE 802.16 là hướng kết nối, đầu tiên ứng dụng thiết lập kết nối với BS cũng như với luồng dịch vụ liên quan (UGS, rtPS, nrtPS hoặc BE). BS sẽ gán kết nối với một định danh kết nối duy nhất (CID). Kết nối có thể biểu diễn một ứng dụng cụ thể hoặc một nhóm ứng dụng trong cùng một SS gửi dữ liệu với cùng CID. IEEE 802.16 định nghĩa báo hiệu kết nối (yêu cầu kết nối, trả lời kết nối) giữa SS và BS nhưng nó không định nghĩa quá trình kiểm soát cho phép.
- Tất cả các gói tin từ lớp ứng dụng trong SS được phân loại bởi bộ phân loại kết nối dựa trên CID và được chuyển tới hàng đợi thích hợp.
- Tại SS, bộ lập lịch sẽ triệu hồi các gói tin từ các hàng đợi và truyền chúng ra mạng trong các khe thời gian thích hợp xác định bởi UL-MAP được gửi bởi BS.
- UL-MAP được xác định bởi mô đun UPS dựa trên các bản tin BW-Request.

Tóm lại, trong kiến trúc chất lượng dịch vụ đường lên, IEEE 802.16 định nghĩa:

- Cơ chế báo hiệu cho việc trao đổi thông tin giữa BS và SS như thiết lập kết nối, BW-Request và UL-MAP.
- Lập lịch đường lên cho luồng dịch vụ UGS.

IEEE 802.16 không định nghĩa:

- Lập lịch đường lên cho luồng dịch vụ rtPS, nrtPS, BE.

- Cơ chế kiểm soát cho phép. Cơ chế kiểm soát cho phép là cần thiết để chấp nhận hay không chấp nhận việc tạo mới luồng dịch vụ hay thay đổi tham số chất lượng dịch vụ của một luồng dịch vụ ([3], trang 74-75).

Như vậy, để hoàn thiện đảm bảo chất lượng dịch vụ của IEEE 802.16 thì chúng ta phải bổ sung những phần mà IEEE 802.16 không định nghĩa cụ thể như đã nêu trên. Trong [1], các tác giả Claudio Cicconetti, Luciano Lenzini, Enzo Mingozzi và Carl Eklund đã phân tích chỉ ra thuật toán thích hợp áp dụng cho bộ lập lịch gói tin.

Sau đây là một số kết quả phân tích của các tác giả:

- Deficit Round Robin (DRR) là thuật toán lập lịch kết hợp nhiều ưu điểm, cân bằng giữa việc đảm bảo phân phối băng thông công bằng và độ phức tạp tính toán. DRR cung cấp khả năng xử lý công bằng trong trường hợp gói tin có kích thước thay đổi, thời gian xử lý một gói tin có độ phức tạp là O(1). DRR đòi hỏi một tốc độ tối thiểu dành cho mỗi luồng dịch vụ. Vì vậy, mặc dù chuẩn 802.16 không đòi hỏi, dịch vụ kiểu BE nên cung cấp tốc độ tối thiểu. Điều này có thể khai thác để tránh lưu lượng BE không được phục vụ trong trường hợp quá tải và lưu lượng BE có thể sử dụng băng thông không dành cho các dịch vụ lập lịch khác.
- DRR giả sử rằng biết kích thước của gói tin cuối mỗi hàng đợi. Vì vậy, thuật toán này không thể sử dụng bởi BS để lập lịch truyền trong hướng lên. Với hướng lên, BS chỉ có khả năng ước lượng tổng toàn bộ lượng lưu lượng chưa xử lý của mỗi kết nối mà không biết được kích thước của mỗi gói tin chưa được xử lý. Vì vậy, các tác giả chọn Weighted Round Robin (WRR) làm thuật toán lập lịch đường lên cho 802.16.

Trong giải pháp mà các tác giả trình bày, chúng ta nhận xét sau:

- Giải pháp của các tác giả chưa đề cập đến vấn đề kiểm soát cho phép.
- Các tác giả đã đề cập là mặc dù thuật toán DRR có nhiều ưu điểm nhưng không áp dụng được thuật toán DRR cho lập lịch đường lên do thuật toán DRR đòi hỏi phải biết kích thước của gói tin ở cuối của mỗi hàng đợi.

Chúng ta sẽ nghiên cứu đề xuất một cơ chế kiếm soát cho phép trong phần 3.4.2, đề xuất cách áp dụng thuật toán DRR trong việc lập lịch gói tin đường lên trong phần 3.4.3.

3.4.2 Hoàn thiện cơ chế kiểm soát cho phép

Cơ chế kiểm soát cho phép xác định một yêu cầu mới cho một kết nối có được chấp nhận hay không dựa vào băng thông rỗi còn lại. Như mô tả trong phần 3.3, có 4 kiểu luồng dịch vụ và các luồng dịch vụ có thể được tạo, thay đổi hoặc xoá sử dụng các bản tin DSA, DSC, DSD. Mỗi hành động đó có thể được khởi tạo bởi SS hoặc BS thông qua quá trình bắt tay hai hoặc ba đường.

BS cần có một mô đun kiểm soát cho phép để quyết định chất lượng dịch vụ của một kết nối có thoả mãn hay không. Nguyên tắc đó để đảm bảo chất lượng dịch vụ của các kết nối đang tồn tại và chất lượng dịch vụ của kết nối mới nếu kết nối mới được chấp nhận.

Chúng ta có thể sử dụng một nguyên tắc kiểm soát cho phép đơn giản dựa trên tốc độ lưu lượng dành riêng tối thiểu. Mô đun kiểm soát cho phép thu thập tất cả các yêu cầu DSA/DSC/DSD và cập nhật băng thông khả dụng C_a dựa trên sự thay đổi băng thông. Giả sử có I lớp dịch vụ và lớp dịch vụ thứ i có tổng số J_i kết nối, băng thông khả dụng được tính bằng:

$$C_a = C_{total} - \sum_{i=0}^{I} \sum_{j=0}^{J_i - 1} r_{\min}(i, j)$$

Trong đó, $r_{\min}(i, j)$ là tốc độ lưu lượng dành riêng tối thiểu của kết nối thứ j trong lớp luồng dịch vụ thứ i, C_{total} là toàn bộ dung lượng của liên kết không dây.

Chính sách kiểm soát cho phép là khi một luồng dịch vụ mới đến hoặc các yêu cầu của luồng dịch vụ cũ thay đổi tham số chất lượng dịch vụ của nó, quy tắc sau đây phải thoả mãn:

$$C_a \geq 0$$

Ý nghĩa của chính sách kiểm soát cho phép ở đây chúng ta sử dụng là chỉ chấp nhận yêu cầu dịch vụ khi đảm bảo được yêu cầu lưu lượng dành riêng tối thiểu cho tất cả các kết nối. Như vậy, đối với các kết nối mà $r_{\min}$ bằng 0 thì kết nối này luôn được chấp nhận bởi chính sách cho phép đã đề xuất. Nhưng chất lượng dịch vụ của những kết nối đó sẽ không được đảm bảo. Các kết nối này luôn có mức ưu tiên thấp nhất và sẽ bị ngắt bất cứ khi nào trừ khi yêu cầu chất lượng dịch vụ của tất cả các kết nối khác đã thoả mãn.

3.4.3 Hoàn thiện vấn đề lập lịch gói tin đường lên

3.4.3.1 Ý tưởng thuật toán DRR

Lập lịch gói tin được định nghĩa là chức năng xác định thứ tự phục vụ các gói tin. Kiểu phục vụ đơn giản nhất là FIFO nhưng nó không cung cấp bất kỳ sự phân biệt nào giữa các luồng dịch vụ. Nếu phục vụ theo kiểu FIFO thì nếu một luồng gửi một lượng lớn dữ liệu sẽ gây trễ cho tất cả các luồng còn lại. Một kiểu phục vụ khác là theo kiểu vòng tròn của các hàng đợi. Mỗi luồng dịch vụ được tổ chức thành một hàng đợi, các gói tin thuộc luồng dịch

vụ nào sẽ được xếp vào hàng đợi của luồng dịch vụ đó. Tuy vậy, vấn đề là sự không công bằng bởi vì có khả năng các luồng dịch vụ khác nhau có gói tin kích thước khác nhau. Khi đó, một luồng dịch vụ có thể chiếm gấp Max/Min lần băng thông của luồng dịch vụ khác, trong đó Max là kích thước lớn nhất của gói tin, Min là kích thước nhỏ nhất của gói tin.

Thuật toán DRR ([9]) giải quyết được hạn chế trên và độ phức tạp tính toán xử lý một gói tin là hằng số. Thuật toán DRR phục vụ vòng tròn các hàng đợi theo một giá trị phục vụ gán cho mỗi hàng đợi (giá trị này gọi là quantum). Sự khác nhau duy nhất so với kiểu phục vụ vòng tròn các hàng đợi truyền thống là nếu một hàng đợi không có khả năng gửi một gói tin trong vòng lặp trước bởi vì kích thước của gói tin quá lớn thì phần còn lại của quantum trước sẽ được cộng vào giá trị quantum cho vòng lặp tiếp. Vì vậy, sự thiếu hụt được theo dõi, các hàng đợi mà bị thiếu trong vòng lặp trước được bù trong vòng lặp tiếp theo.

3.4.3.2 Nội dung thuật toán DRR

Thuật toán định nghĩa $Quantum_i$ là số byte dành cho hàng đợi i mỗi vòng lặp. Một vòng lặp là một quá trình xử lý duyệt qua các hàng đợi đang chờ xử lý.

Các gói tin đến trong các luồng dịch vụ khác nhau được chứa trong các hàng đợi khác nhau. Đặt số byte gửi ra khỏi hàng đợi i trong vòng lặp thứ k là $bytes_i(k)$. Mỗi hàng đợi i được phép gửi các gói tin trong vòng lặp đầu tiên thoả mãn $bytes_i(1) <= Quantum_i$. Nếu không có gói tin trong hàng đợi i sau khi hàng đợi đã được phục vụ, biến trạng thái $DeficitCounter_i$ sẽ khởi tạo lại giá trị 0. Ngược lại, phần còn lại $(Quantum_i - bytes_i(k))$ được gán cho biến trạng thái $DeficitCounter_i$. Trong các vòng lặp sau, lượng băng thông sử dụng bởi luồng dịch vụ này là tổng của $DeficitCounter_i$ của vòng lặp trước với

$Quantum_i$.

Để tránh kiểm tra các hàng đợi rỗng, thuật toán DRR xây dựng một danh sách *ActiveList* là danh sách của các hàng đợi chứa ít nhất một gói tin. Bất kỳ khi nào một gói tin tới một hàng đợi rỗng i, i được bổ sung vào cuối của *ActiveList*. Khi nào chỉ số i nằm ở đầu danh sách *ActiveList*, thuật toán phục vụ hàng đợi i với giá trị tối đa là $Quantum_i + DeficitCounter_i$ byte. Nếu tại cuối quá trình phục vụ hàng đợi i này, hàng đợi i vẫn có gói tin để gửi, chỉ số i được di chuyển tới cuối của *ActiveList*, ngược lại $DeficitCounter_i$ được gán giá trị 0 và chỉ số i sẽ bị loại bỏ khỏi *ActiveList*.

Mô đun Enqueueing thực hiện xử lý khi một gói tin đến. Mô đun Dequeueing xử lý lập lịch cho việc gửi gói tin. Sau đây là mã giả mô tả chi tiết thuật toán.

Các biến và thao tác:

- $Queue_i$ là hàng đợi thứ i chứa các gói tin của luồng dịch vụ i.
- Các hàng đợi được đánh số từ 0 tới (n - 1), n là số hàng đợi lớn nhất tại đường ra.
- *ActiveList* là danh sách các luồng dịch vụ hoạt động.
- $Quantum_i$ là giá trị lưu lượng dành cho $Queue_i$.
- $DeficitCounter_i$ chứa số byte mà $Queue_i$ không sử dụng trong vòng lặp trước.
- *InsertActiveList* thực hiện thêm chỉ số của luồng dịch vụ vào cuối danh sách *ActiveList*.
- *RemoveActiveList* thực hiện lấy và loại bỏ chỉ số của luồng dịch vụ ở đầu danh sách *ActiveList*.
- *Enqueue()* là thao tác đưa một gói tin vào hàng đợi.
- *Dequeue()* là thao tác lấy một gói tin ra khỏi hàng đợi.

- *ExtractFlow(p)*: xác định gói tin p thuộc hàng đợi nào

Bước khởi tạo:

For (i = 0; i < n; i = i + 1)

$DeficitCounter_i$ = 0;

Mô đun Enqueueing:

```
i = ExtractFlow(p)
If <i không có trong ActiveList> then
    InsertActiveList(i);
    DeficitCounter_i = 0;
Enqueue(i,p);
```

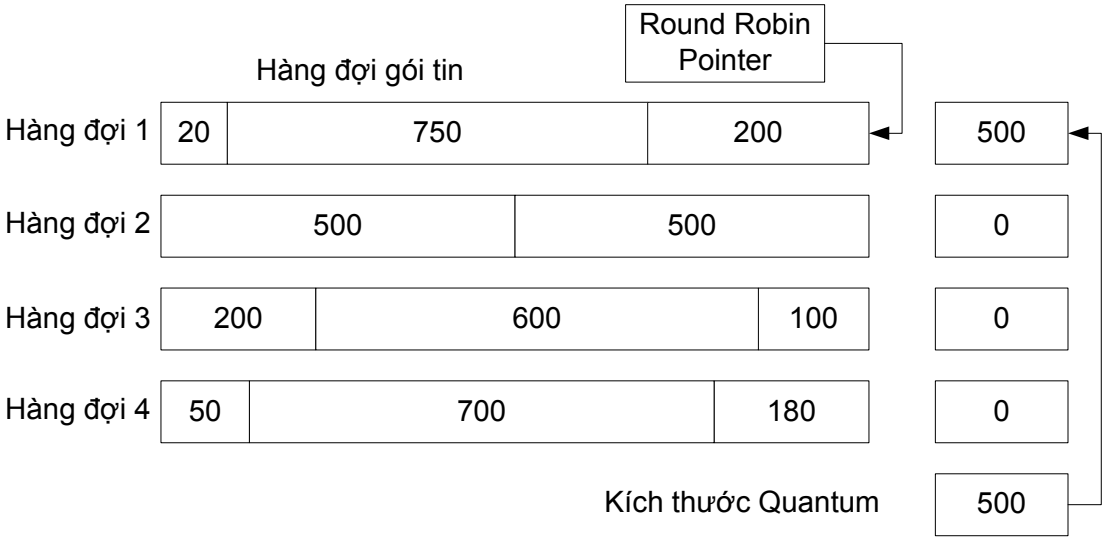
Mô đun Dequeueing:

```
While (TRUE) do
    If <ActiveList không rỗng> then
     i = RemoveActiveList()
     DeficitCounter_i = Quantum_i + DeficitCounter_i;
     While ((DeficitCounter_i > 0) and (Queue_i không rỗng)) do
          PacketSize = Size(Head(Queue_i));
          If (PacketSize <= DeficitCounter_i) then
               Send(Dequeue(Queue_i));
               DeficitCounter_i = DeficitCounter_i – PacketSize;
          Else break;
          If (Empty(Queue_i)) then
               DeficitCounter_i = 0;
          Else InsertActiveList(i);
```

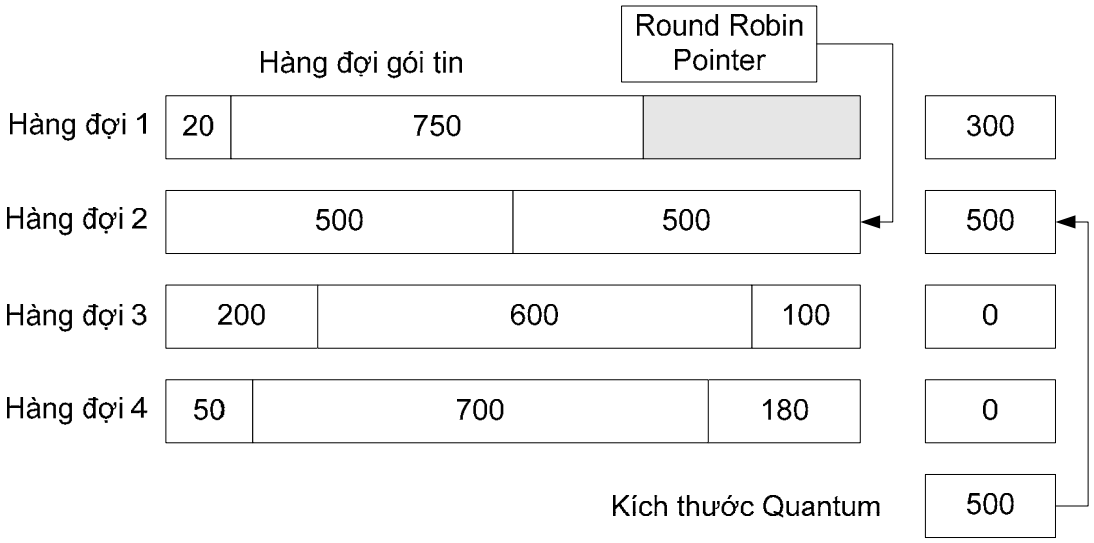
Ví dụ minh hoạ bước xử lý của thuật toán

Giả sử danh sách *ActiveList* có 4 hàng đợi. Giá trị *Quantum* bằng 500.

Bắt đầu, biến $DeficitCounter_i$ khởi tạo giá trị 0 với mọi hàng đợi i. Con trỏ Round Robin chỉ tới đỉnh của *ActiveList*. Khi hàng đợi đầu tiên được phục vụ, giá trị *Quantum* bằng 500 được gán cho biến $DeficitCounter_1$. (Hình 3.7)



Hình 3.7 Ví dụ minh hoạ thuật toán DRR (1)



Hình 3.8 Ví dụ minh hoạ thuật toán DRR (2)

Sau khi gửi một gói tin có kích thước 200, hàng đợi thứ nhất có giá trị $DeficitCounter_1 = 500 - 200 = 300$ byte. Nó không thể sử dụng trong vòng lặp hiện tại, do gói tin tiếp theo trong hàng đợi có kích thước 750 byte. Vì vậy, giá trị 300 sẽ được chuyển tới vòng lặp tiếp theo. Trong vòng lặp tiếp theo, hàng đợi này có thể gửi các gói tin kích thước nhỏ hơn hoặc bằng 800 (300 từ vòng lặp trước cộng với giá trị quantum 500). (Hình 3.8)

3.4.3.3 Áp dụng thuật toán DRR trong vấn đề lập lịch đường lên

Trong [1], các tác giả đã phân tích các ưu điểm của thuật toán DRR trong việc lập lịch gói tin IEEE 802.16. Tuy nhiên, các tác giả chỉ ra rằng không thể áp dụng thuật toán DRR cho việc lập lịch gói tin đường lên. Thuật toán DRR mô tả cho đối tượng xử lý của thuật toán là các gói tin, thuật toán cần biết kích thước của gói tin cuối mỗi hàng đợi khi xử lý. Trong khi, đối tượng xử lý của lập lịch gói tin đường lên là các BW-request chứa băng thông yêu cầu. Chúng ta không biết được kích thước của từng gói tin trong đường lên. Phương án giải quyết là chúng ta thay đổi đối tượng xử lý của thuật toán DRR là các gói tin bằng các BW-request. Khi đó, việc phân phối băng thông vẫn đảm bảo công bằng, do đó lập lịch các gói tin đường lên đảm bảo.

Các vấn đề tiếp theo chúng ta tiếp tục xác định bao gồm:

- Xác định các hàng đợi
- Cách tính giá trị quantum

Do băng thông dịch vụ UGS được dành riêng nên chúng ta không phải lập lịch cho các dịch vụ UGS. Như vậy, chúng ta có 3 hàng đợi cho các dịch vụ rtPS, nrtPS và BE. Do các dịch vụ rtPS cần đảm bảo hơn về yếu tố thời gian thực so với dịch vụ nrtPS, dịch vụ BE không có ràng buộc về đảm bảo chất lượng dịch vụ nên chúng ta sắp thứ tự ưu tiên phục vụ các hàng đợi này

như sau: rtPS > nrtPS > BE.

Danh sách *ActiveList* duy trì trong BS. DRR chỉ lập lịch các dịch vụ ứng dụng trong danh sách *ActiveList*. Nếu hàng đợi không rỗng, nó sẽ trong danh sách *ActiveList*. Ngược lại, nó sẽ bị loại bỏ khỏi danh sách *ActiveList*. Luồng dịch vụ trong danh sách *ActiveList* được xếp hàng theo độ ưu tiên cố định như trên. Trong mỗi vòng lặp, luồng dịch vụ có độ ưu tiên cao nhất sẽ luôn được phục vụ trước.

Trong thuật toán DRR, bộ lập lịch sẽ thăm mỗi hàng đợi không rỗng, xác định kích thước gói tin tại đỉnh của hàng đợi, biến *DeficitCounter* được tăng bởi một giá trị *Quantum*. Áp dụng trong bộ lập lịch đường lên, các yêu cầu băng thông sẽ được phục vụ trong hàng đợi. Bộ lập lịch thăm mỗi hàng đợi không rỗng trong danh sách hoạt động, biến *DeficitCounter* tăng bởi giá trị *Quantum* mỗi khi nó được thăm. Nếu kích thước dữ liệu yêu cầu của gói tin BW-REQ tại đỉnh của hàng đợi nhỏ hơn hoặc bằng giá trị *DeficitCounter*, biến *DeficitCounter* giảm một lượng bằng kích thước băng thông yêu cầu và gói tin được truyền tới cổng ra. Quá trình được lặp lại tới khi *DeficitCounter* nhỏ hơn hoặc bằng 0, hoặc hàng đợi rỗng. Nếu hàng đợi rỗng, giá trị *DeficitCounter* cũng được gán bằng 0. Khi điều kiện này xảy ra, bộ lập lịch chuyển tới phục vụ hàng đợi ưu tiên không rỗng tiếp theo.

Vấn đề tiếp theo là cách xác định *Quantum*. Một cách là *Quantum[i]* của lớp của luồng dịch vụ thứ i tính như sau:

$$Quantum[i] = \sum_{j=0}^{J_i} r_{\max}(i,j)$$

Trong đó, J_i là tổng số kết nối cho lớp thứ i của luồng dịch vụ. Chú ý là đối với kết nối mà $r_{\max}$ của nó không được chỉ định (ví dụ $r_{\max}$ = 0 trong bản tin DSA), $r_{\max}$ sẽ được gán bằng $r_{\min}$. Tốc độ dịch vụ của kết nối có giá trị

Quantum lớn hơn sẽ lớn hơn kết nối có giá trị Quantum nhỏ.

Các bước thuật toán DRR áp dụng trong bộ lập lịch gói tin đường lên trong IEEE 802.16 như sau:

Bước 1: Cập nhật danh sách ActiveList

Nếu một hàng đợi của kết nối là rỗng, chúng ta loại bỏ nó khỏi danh sách ActiveList. Nếu hàng đợi của kết nối thay đổi từ rỗng sang không rỗng, chúng ta thêm nó vào danh sách *ActiveList*. Các luồng dịch vụ trong danh sách ActiveList sẽ được xếp hàng theo độ ưu tiên rtPS > nrtPS > BE.

Bước 2: Cập nhật các tham số cho mỗi hàng đợi dịch vụ.

Gọi L_a là dung lượng khả dụng của một TDD frame tính theo byte, L_{total} là tổng dung lượng của một TDD frame.

Giá trị khởi tạo của L_a: $L_a = L_{total}$

Giá trị khởi tạo của *DeficitCounter[i]: DeficitCounter [i] = Quantum[i]*

Bước 3: Phục vụ các kết nối trong luồng dịch vụ với từng hàng đợi theo độ ưu tiên tới khi một trong các điều kiện sau thoả mãn:

Điều kiện (1): *DeficitCounter[i]* ≤ 0.

Điều kiện (2): Hàng đợi là rỗng.

Điều kiện (3): Không còn băng thông khả dụng, $L_a \leq 0$

Điều kiện (4): Đến thời điểm gửi bản tin UL-MAP.

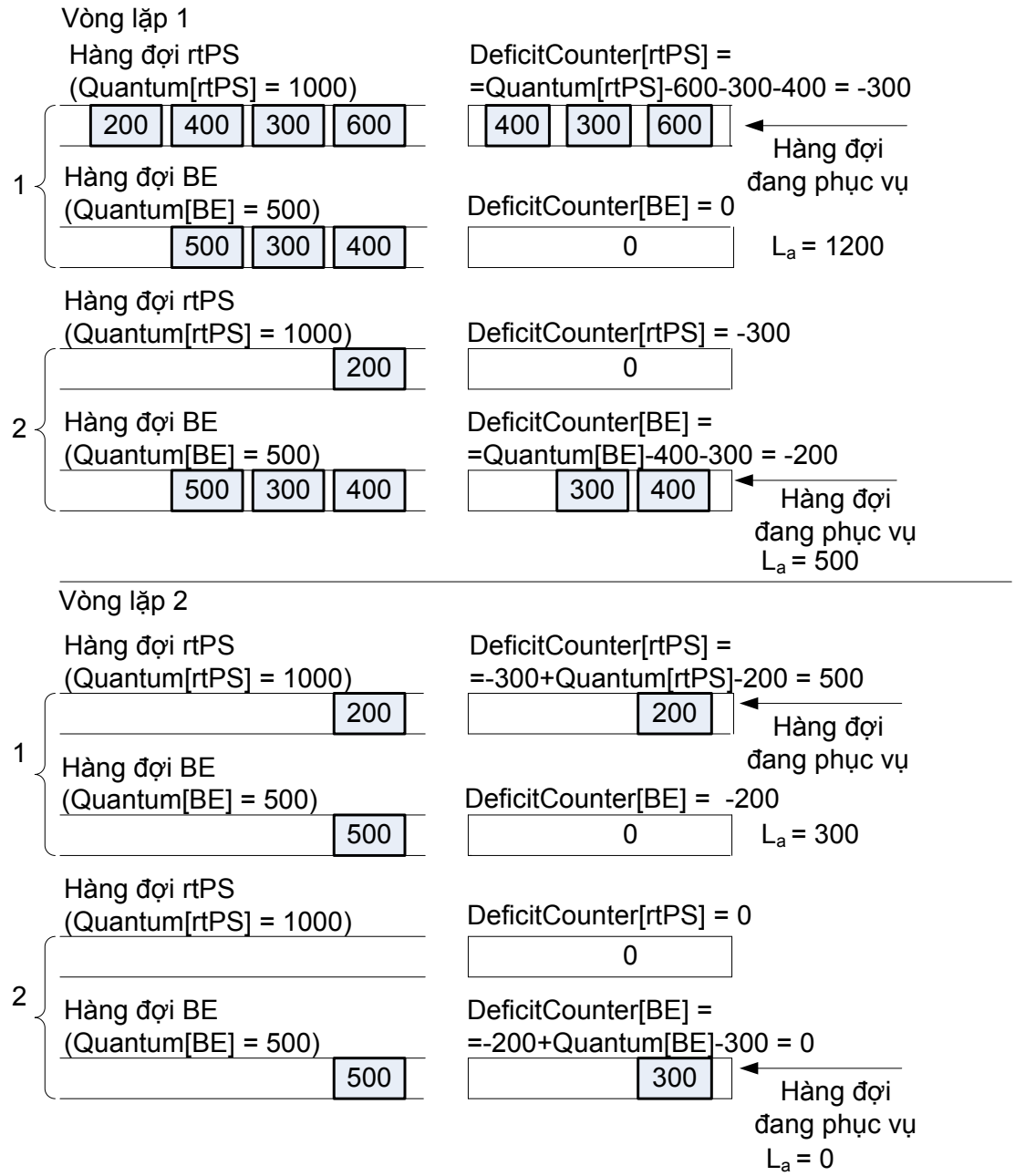
Nếu điều kiện (1) hoặc (2) thoả mãn thì chuyển sang bước 4.

Nếu điều kiện (3) hoặc (4) thỏa mãn thì chuyển sang bước 5.

Bước 4: Nếu còn hàng đợi có độ ưu tiên thấp hơn thì phục vụ các hàng đợi có độ ưu tiên thấp hơn như trong bước 3. Nếu không có hàng đợi ưu tiên thấp hơn nào, thì quay lại bước 3 và thực hiện vòng lặp lập lịch mới.

Bước 5: Gửi bản tin UL-MAP và kết thúc việc lập lịch cho TDD frame hiện tại. Quay trở lại bước 1 cho TDD frame tiếp theo.

Ví dụ: Danh sách ActiveList có hai hàng đợi của luồng dịch vụ rtPS và BE. *Quantum[rtPS]* = 1000, *Quantum[BE]* = 500, $L_{total} = 2500$



Hình 3.9 Thuật toán DRR áp dụng trong bộ lập lịch gói tin đường lên

Vòng lặp 1

Bước 1: Cập nhật danh sách ActiveList

Bước 2: Cập nhật các tham số cho các hàng đợi hoạt động

$$DeficitCounter[rtPS] = 1000$$

$$DeficitCounter[BE] = 500$$

$$L_a = 2500$$

Bước 3(1):

Vì gói tin yêu cầu băng thông BW-REQ tại đỉnh của hàng đợi rtPS nhỏ hơn giá trị của *DeficitCounter[rtPS]* = 1000, BW-REQ 600 byte được phục vụ. Giá trị *DeficitCounter[rtPS]* bị giảm đi 600, kết quả giá trị mới là 400.

Sau đó, BW-REQ 300 byte ở đỉnh hàng đợi rtPS nhỏ hơn 400 nên gói tin 300 byte được phục vụ, kết quả giá trị mới của *DeficitCounter[rtPS]* = 100.

Tiếp theo, BW-REQ 400 byte trong hàng đợi rtPS sẽ được phục vụ *DeficitCounter[rtPS]* = 100 – 400 = -300 (<0). Điều kiện (1) xảy ra, chuyển sang bước 4.

Kết thúc bước này, $L_a = 2500 - 600 - 300 - 400 = 1200$

Bước 4(1): Chúng ta kiểm tra thấy còn hàng đợi có độ ưu tiên thấp hơn là hàng đợi BE. Do đó, chuyển tới bước 3 phục vụ hàng đợi BE.

Bước 3(2):

Hàng đợi BE sẽ được phục vụ tới khi *DeficitCounter[BE]* < 0.

$$DeficitCounter[BE] = 500 - 300 - 400 = -200$$

$$L_a = 1200 - 300 - 400 = 500$$

Bước 4(2):

Vì không còn luồng dịch vụ nào khác mà vẫn còn băng thông khả dụng, nên sẽ thực hiện vòng lặp mới.

Vòng lặp 2:

Bước 3(1):

Trong vòng lặp thứ 2, luồng rtPS có độ ưu tiên cao nhất. Đầu tiên, *DeficitCounter[rtPS]* sẽ bằng tổng của *Quantum[rtPS]* và *DeficitCounter[rtPS]* trong vòng lặp trước:

$$DeficitCounter[rtPS] = 1000 + (-300) = 700$$

Sau đó, yêu cầu BW-REQ 200 byte sẽ được xử lý:

$$DeficitCounter[rtPS] = 700 - 200 = 500.$$

$$L_a = 500 - 200 = 300$$

Hàng đợi rtPS rỗng nên điều kiện (2) xảy ra, chuyển sang bước 4.

Bước 4(1): Chúng ta kiểm tra thấy còn hàng đợi có độ ưu tiên thấp hơn là hàng đợi BE. Do đó, chuyển tới bước 3 phục vụ hàng đợi BE.

Bước 3(2): Ta có $DeficitCounter[BE] = -200 + 500 = 300$

Yêu cầu BW-REQ 500 byte sẽ được xử lý, do băng thông khả dụng chỉ còn 300 nên chỉ có 300 byte được xử lý:

$$DeficitCounter[rtPS] = 300 - 300 = 0$$

$$L_a = 300 - 300 = 0$$

Điều kiện (3) thoả mãn nên chúng ta chuyển sang bước 5.

Bước 5: Việc lập lịch kết thúc cho TDD frame này.

Chú ý là trong bước 3(2) của vòng lặp 2, chỉ có 300 byte được chấp nhận trong BS cho BW-REQ 500 byte. SS thực hiện phân mảnh gói tin 500 byte. Khung con 300 byte đầu tiên sẽ được gửi đi và khung con 200 byte còn lại sẽ được truyền tiếp trong khung TDD tiếp theo.

Áp dụng thuật toán DRR trong việc lập lịch gói tin, chúng ta thấy trong mỗi vòng lập lịch, hàng đợi có độ ưu tiên cao nhất sẽ được phục vụ đầu tiên tới khi băng thông chia phần cho nó thiếu. Vì vậy, đây là lập lịch dựa vào

hàng đợi ưu tiên. Mặt khác, nếu băng thông chia phần thiếu đối với hàng đợi có độ ưu tiên cao hơn, luồng dịch vụ với hàng đợi có độ ưu tiên thấp hơn sẽ có cơ hội được phục vụ, đó là một giải pháp công bằng cho hàng đợi có độ ưu tiên thấp hơn, khác với hàng đợi có độ ưu tiên cố định.

3.5 Kết chương

Trong chương này, chúng ta đã tìm hiểu về yêu cầu và đặc điểm chung của vấn đề chất lượng dịch vụ, mô hình đảm bảo chất lượng dịch vụ do diễn đàn WiMAX đưa ra. Sau đó, chúng nghiên cứu về cơ chế đảm bảo chất lượng dịch vụ của chuẩn 802.16. Trong đó, chúng ta đã nghiên cứu về các cơ chế phân loại luồng dịch vụ, quản trị luồng dịch vụ động, mô hình kích hoạt 2 pha. Trong phần hoàn thiện giải pháp chất lượng dịch vụ của IEEE 802.16, chúng ta nghiên cứu chỉ ra các điểm mà chuẩn 802.16 bỏ trống, tập trung vào vấn đề lập lịch gói tin đường lên và đề xuất giải pháp hoàn thiện chúng. Chúng ta đã nghiên cứu đề xuất một cơ chế kiểm soát cho phép áp dụng cho vấn đề chất lượng dịch vụ của IEEE 802.16. Đối với vấn đề lập lịch gói tin đường lên, chúng ta đã nghiên cứu đề xuất giải quyết hạn chế mà các tác giả trong [1] đã chỉ ra, để áp dụng thuật toán DRR vào việc lập lịch gói tin đường lên. Trong chương tiếp theo, chúng ta sẽ đi sâu nghiên cứu về vấn đề an toàn bảo mật trong mạng WiMAX.

Chương 4.
VẤN ĐỀ AN TOÀN BẢO MẬT

4.1 Yêu cầu và đặc điểm chung

Diễn đàn WiMAX định nghĩa một khung làm việc xác thực, uỷ quyền và kế toán (Authentication, Authorization, Accounting - AAA) dựa trên đặc tả của IETF. AAA chỉ tới giao thức xác thực uỷ quyền và kế toán (Radius hoặc Diameter). Chúng ta chỉ nghiên cứu về vấn đề xác thực và uỷ quyền trong khung làm việc AAA.

Khung làm việc AAA cung cấp các dịch vụ sau cho WiMAX:

- Dịch vụ xác thực: Bao gồm xác thực SS, xác thực người dùng hoặc kết hợp cả hai.
- Dịch vụ uỷ quyền: Bao gồm sự chuyển thông tin để cấu hình phiên để truy cập, tính di động, chất lượng dịch vụ và các ứng dụng khác.
- Các dịch vụ kế toán: Bao gồm sự chuyển thông tin cho mục đích tính cước (bao gồm cả trả trước và trả sau) và thông tin sử dụng cho việc đối soát phiên bởi cả nhà cung cấp dịch vụ mạng nhà và nhà cung cấp dịch vụ mạng ngoài.

Các yêu cầu chức năng cụ thể là:

a) Khung làm việc AAA hỗ trợ chuyển vùng toàn cầu qua các mạng tổng đài WiMAX, bao gồm sự hỗ trợ cho sử dụng lại tài liệu xác thực và sử dụng nhất quán việc uỷ quyền và kế toán.

b) Khung làm việc AAA hỗ trợ chuyển vùng giữa nhà cung cấp dịch vụ mạng nhà và nhà cung cấp dịch vụ mạng ngoài.

c) Khung làm việc AAA dựa trên việc sử dụng Radius trong mạng dịch vụ truy cập và mạng dịch vụ kết nối. Khi sử dụng, một cổng phối hợp hoạt động sẽ thực hiện công việc chuyển đổi giữa các giao thức WiMAX và Radius. Chức năng phối hợp hoạt động có thể đòi

hỏi để chuyển đổi giữa một trong các giao thức đó với giao thức đặc trưng của một vùng kế thừa. Vùng kế thừa là vùng sử dụng các công nghệ khác, thường là các công nghệ ra đời trước WiMAX.

d) Khung làm việc AAA sẽ tương thích với lược đồ 3 bên AAA: SS là đối tượng yêu cầu, thực thể xác thực trong mạng dịch vụ truy cập đóng vai trò tiếp nhận yêu cầu và một AAA nền đóng vai trò là server xác thực xử lý yêu cầu.

e) Khung làm việc AAA sẽ tương thích với yêu cầu xác thực AAA (RFC 2906).

f) Khung làm việc AAA hỗ trợ cả quản lý liên kết bảo mật Mobile IPv4 và Mobile IPv6.

g) Khung làm việc AAA hỗ trợ tất cả kịch bản hoạt động từ cố định tới di động.

h) Khung làm việc AAA hỗ trợ triển khai xác thực SS, xác thực người dùng và xác thực lẫn nhau giữa SS và nhà cung cấp dịch vụ mạng dựa trên PKMv2.

i) Để đảm bảo khả năng phối hợp hoạt động, khung làm việc AAA hỗ trợ cơ chế xác thực dựa trên EAP, nó có thể bao gồm nhưng không giới hạn các cơ chế sau: mật khẩu, mô đun định danh người sử dụng (SIM), mô đun định danh người sử dụng chung (USIM), thẻ mạch tích hợp chung (UICC), mô đun định danh người sử dụng với khả năng tháo lắp (RUIM) và chứng chỉ số X.509.

j) Khung làm việc AAA cung cấp hỗ trợ thích hợp cho việc cung cấp chính sách tại mạng dịch vụ truy cập hoặc mạng dịch vụ kết nối, ví dụ mang thông tin liên quan tới chính sách từ AAA server tới mạng dịch vụ truy cập hoặc mạng dịch vụ kết nối.

k) Khung làm việc AAA sẽ hỗ trợ thay đổi động các cập nhật xác thực

theo RFC 3576.

l) Khung làm việc AAA có khả năng cung cấp mạng dịch vụ kết nối ngoài hoặc mạng dịch vụ truy cập một thẻ biểu diễn người sử dụng mà không tiết lộ định danh của người sử dụng. Thẻ này có thể được sử dụng bởi các thực thể bên ngoài mạng dịch vụ kết nối nhà để tính cước và thi hành cam kết các mức dịch vụ.

m) Để hỗ trợ một số ứng dụng như xác thực động, khung làm việc AAA có thể được đòi hỏi để duy trì trạng thái phiên. Trong trường hợp của Radius (RFC 2865) (giao thức không quản lý trạng thái) sự duy trì trạng thái của phiên do sự thực hiện cụ thể.

4.2 Mô hình an toàn bảo mật

Mô hình để triển khai khung làm việc AAA có 3 kiểu: mô hình tác tử, mô hình kéo, mô hình đẩy ([4]). Các mô hình khác nhau hai khía cạnh: cách đối tượng hỏi và server xác thực giao tiếp, cách thông tin điều khiển (ví dụ: khóa, chính sách) được cấu hình vào các SS của không gian vận chuyển. Theo các ví dụ của các ứng dụng chính được triển khai sử dụng các mô hình trên trong RFC 2095, cũng như theo diễn đàn WiMAX, mô hình kéo được sử dụng để triển khai khung làm việc AAA.

Nhà cung cấp truy cập mạng có thể triển khai một AAA proxy giữa NAS trong mạng dịch vụ truy cập và AAA trong mạng dịch vụ kết nối để cung cấp bảo mật. Trường hợp đặc biệt là khi mạng dịch vụ truy cập có nhiều NAS và mạng dịch vụ kết nối trong vùng quản trị khác. Trong trường hợp này, AAA proxy sẽ giúp dễ dàng cấu hình AAA giữa nhà cung cấp truy cập mạng và mạng dịch vụ kết nối ngoài. AAA proxy cho phép nhà cung cấp truy cập mạng kiểm soát các thuộc tính AAA nhận từ mạng dịch vụ kết nối ngoài và

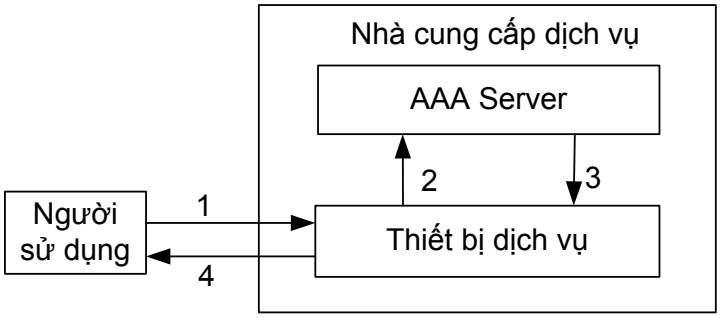
các thuộc tính AAA khác được đòi hỏi bởi NAS trong mạng dịch vụ truy cập.

Chức năng AAA trong mạng dịch vụ truy cập chứa trong một hoặc nhiều NAS. Một NAS được xem như AAA client đầu tiên ở đó các bản tin AAA khởi đầu và các thuộc tính xác thực uỷ quyền được chuyển tới. Các thuộc tính xác thực và uỷ quyền được chuyển tới các ứng dụng AAA (như thực thể xác thực, các ứng dụng di động, các ứng dụng trả trước, các ứng dụng chất lượng dịch vụ) nằm trong NAS.

Như đã trình bày, mô hình kéo là mô hình được khuyến khích sử dụng trong mạng WiMAX. Chúng ta sẽ xem xét áp dụng mô hình kéo vào trong mạng WiMAX trong hai trường hợp không chuyển vùng và có chuyển vùng.

4.2.1 Mô hình kéo không chuyển vùng

Mô hình kéo không chuyển vùng ([4], hình 4, trang 9) được mô tả như trong hình 4.1.



Hình 4.1 Khung làm việc AAA không chuyển vùng tổng quát

Hoạt động như sau:

1) Người sử dụng (SS) gửi một yêu cầu tới thiết bị dịch vụ (ví dụ như NAS).
2) Thiết bị dịch vụ chuyển yêu cầu tới AAA Server của nhà cung cấp dịch vụ.

3) AAA Server của nhà cung cấp dịch vụ đánh giá yêu cầu và trả về trả lời thích hợp tới thiết bị dịch vụ.
4) Thiết bị dịch vụ cung cấp không gian vận chuyển và thông báo người sử dụng rằng đã sẵn sàng.

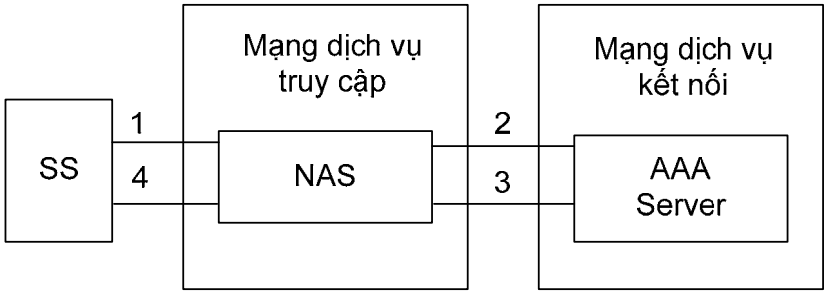
Áp dụng vào mô hình mạng WiMAX trong trường hợp không chuyển vùng, có hai trường hợp là:

- Trường hợp thứ nhất: Xây dựng mới hoặc việc xác thực uỷ quyền của nhà cung cấp dịch vụ mạng hiện tại tương thích AAA.
- Trường hợp thứ hai: Việc xác thực uỷ quyền của nhà cung cấp dịch vụ mạng hiện tại không tương thích AAA. Sự không tương thích có thể ở mức giao thức hoặc tại mức thuộc tính,...

Áp dụng vào mô hình mạng WiMAX trong trường hợp thứ nhất như sau:

- Nhà cung cấp dịch vụ được tách thành mạng dịch vụ truy cập và mạng dịch vụ kết nối.
- Thiết bị dịch vụ trong mạng dịch vụ truy cập trở thành NAS.
- Mạng dịch vụ kết nối chứa AAA server trong khi mạng dịch vụ truy cập chứa một hoặc nhiều NAS.

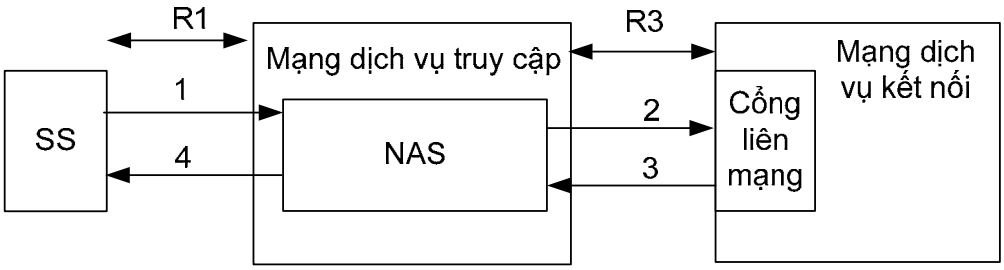
Chúng ta có kết quả là mô hình AAA cho mạng WiMAX trường hợp không chuyển vùng như hình 4.2.



Hình 4.2 Khung làm việc AAA không chuyển vùng dựng mới

Áp dụng vào mô hình mạng WiMAX trong trường hợp thứ hai: Mạng dịch vụ kết nối của nhà cung cấp dịch vụ cần chứa một cổng liên mạng để ánh

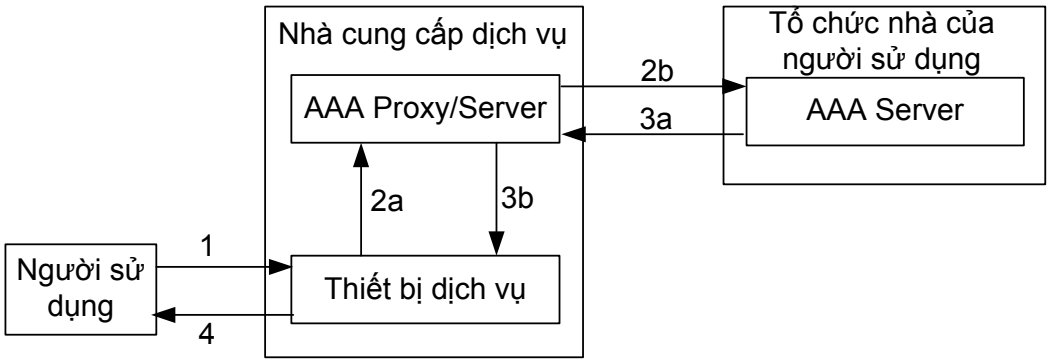
xạ giao thức và các thuộc tính AAA tới các giao thức cụ thể của nhà cung cấp dịch vụ hiện tại và ngược lại. Chúng ta có kết quả là mô hình AAA như hình 4.3.



Hình 4.3 Khung làm việc AAA không chuyển vùng khi mạng dịch vụ kết nối không tương thích AAA

4.2.2 Mô hình kéo có chuyển vùng

Mô hình kéo có chuyển vùng được minh họa như hình 4.4 ([4], hình 8, trang 12).

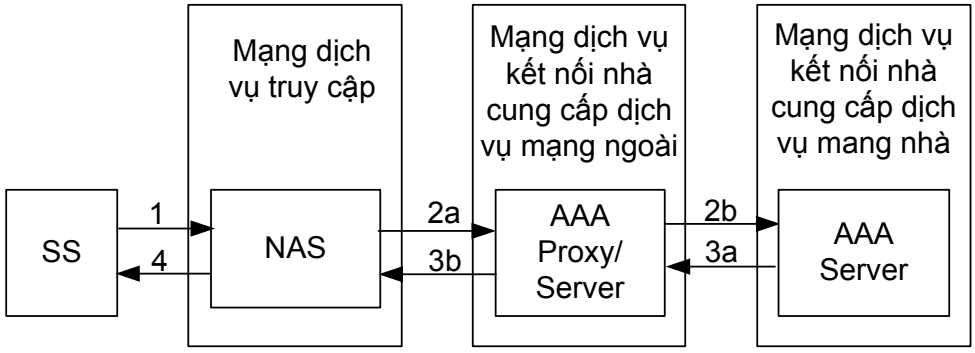


Hình 4.4 Khung làm việc AAA chuyển vùng tổng quát

Áp dụng cho mạng WiMAX, chúng ta cũng xét hai trường hợp như khi không chuyển vùng.

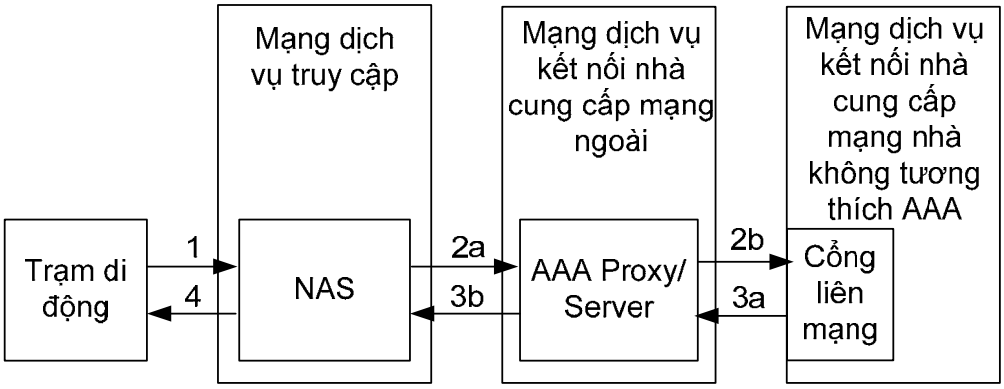
Trong trường hợp thứ nhất, chúng ta có mô hình AAA chuyển vùng của mạng WiMAX như hình 4.5. Khi triển khai chuyển vùng, tùy chọn một hoặc

nhiều các thực thể AAA proxy/server tồn tại giữa mạng dịch vụ truy cập và mạng dịch vụ kết nối nhà.



Hình 4.5 Khung làm việc AAA chuyển vùng dựng mới

Trường hợp thứ hai, việc xác thực và uỷ quyền của mạng dịch vụ kết nối của nhà cung cấp dịch vụ mạng nhà đang phục vụ không tương thích với AAA. Như trong trường hợp không chuyển vùng, nhà cung cấp dịch vụ mạng nhà đang phục vụ sẽ chứa một cổng liên mạng để ánh xạ các giao thức và các thuộc tính AAA tới các giao thức cụ thể của nhà cung cấp dịch vụ mạng hiện tại và ngược lại. Chúng ta có kết quả như hình 4.6.



Hình 4.6 Khung làm việc AAA chuyển vùng khi mạng dịch vụ kết nối không tương thích AAA

4.3 Cơ chế an toàn bảo mật của IEEE 802.16

IEEE 802.16 cung cấp các xử lý an toàn bảo mật nằm ở lớp con bảo mật. Bảo mật của 802.16 bao gồm 5 thành phần: Liên kết bảo mật, chứng nhận X.509, giao thức uỷ quyền quản lý khoá riêng, giao thức quản lý khoá riêng và mã hoá. Chúng ta sẽ lần lượt tìm hiểu chi tiết về các thành phần trên.

4.3.1 Liên kết bảo mật

Liên kết bảo mật (Security Associations - SA) duy trì trạng thái bảo mật của mỗi kết nối. IEEE 802.16 sử dụng hai SA là Data SA và Authorization SA, nhưng chỉ định nghĩa rõ ràng Data SA. ([2])

Data SA là SA bảo vệ truyền thông giữa các SS và BS. Data SA có các phần tử sau:

- 16 bit định danh SA (SAID)
- Một bộ mã để bảo vệ dữ liệu trao đổi qua kết nối. Chuẩn sử dụng DES với chế độ cipher block chaining (CBC) nhưng thiết kế cho phép mở rộng với các thuật toán khác.
- Hai khoá mã hoá lưu lượng TEK để mã hoá dữ liệu: một khoá hoạt động hiện tại và một khoá sử dụng khi khoá hiện tại hết hiệu lực.
- Hai định danh khoá 2-bit, mỗi khoá TEK có một định danh.
- Thời gian hiệu lực của TEK. Giá trị mặc định là 12 giờ, giá trị tối thiểu là 30 phút, giá trị tối đa là 7 ngày.
- Véc tơ khởi tạo 64-bit cho mỗi TEK.
- Giá trị chỉ kiểu Data SA. Primary SA được thiết lập trong quá trình khởi tạo liên kết, static SA được cấu hình tại BS và dynamic SA được xây dựng khi cần cho các kết nối giao vận tạo động.

Khi một kết nối giao vận được tạo, SS khởi tạo một Data SA. Một Data

SA có thể phục vụ cho nhiều CID. Khi SS tham gia vào mạng, tự động một SA được gán cho secondary management connection. Mọi SS có một SA chung cho kết nối giao vận đường lên và đường xuống hoặc một SA cho kết nối giao vận đường lên, một SA cho kết nối giao vận đường xuống. Như vậy, một SS có hai hoặc ba SA.

Kiểu SA thứ hai là Authorization SA không được định nghĩa rõ ràng trong chuẩn. Authorization SA được dùng chung giữa một BS và một SS. Authorization Key (AK) được BS và SS giữ bí mật. BS sử dụng Authorization SA để cấu hình Data SA trên SS. Authorization SA có các phần tử sau:

- Chứng nhận X.509 để định danh SS.
- 160-bit khoá AK.
- 4-bit để định danh AK.
- Thời gian hiệu lực của AK, từ 1 ngày đến 70 ngày, giá trị mặc định là 7 ngày.
- Một Key Encryption Key (112-bit Triple-DES key) để phân phối các TEK. KEK xây dựng như sau KEK= Truncate-128(SHA1(((AK $| 0^{44}$) $\oplus$ 53^{64})),

  Trong đó Truncate-128(·) nghĩa là loại bỏ tất cả trừ 128 bít đầu của tham số, a|b nghĩa là ghép xâu a và b, $\oplus$ nghĩa là XOR, a^n nghĩa là byte a được lặp n lần.
- Một khoá Downlink HMAC cung cấp sự xác thực dữ liệu của các bản tin phân phối khoá từ BS tới SS. Khoá này được xây dựng như sau: Downlink HMAC key = SHA1((AK $| 0^{44}$) $\oplus$ $3A^{64}$).
- Một khoá Uplink HMAC cung cấp sự xác thực dữ liệu của các bản tin phân phối khoá từ SS tới BS. Khoá HMAC đường lên được xây dựng như sau: Uplink HMAC key = SHA1((AK $| 0^{44}$) $\oplus$ $5C^{64}$).

- Một danh sách các Data SA.

Bảng 4.1 Các khoá sử dụng với SA

Khoá	**Đối tượng sinh khoá**	**Mục đích sử dụng**	**Thời gian hiệu lực**	**Thuật toán**
Authetication Key (AK)	BS	- Sinh KEK - Tính HMAC digest - Kiểm tra HMAC digest nhận được	Từ 1 đến 70 ngày	3-DES SHA1
Key Encryption Key (KEK)	BS, SS	- Mã hoá TEK để truyền (BS) - Giả mã TEK để sử dụng (SS)	Từ 1 đến 70 ngày	3-DES
Traffic Encryption Key (TEK)	BS	Mã hoá dữ liệu truyền	Từ 30 phút đến 7 ngày	DES-CBC AES-CCM

4.3.2 Chứng nhận X.509

Chứng nhận X.509 được sử dụng để định danh các thành phần truyền thông. IEEE 802.16 yêu cầu chứng nhận X.509 với các trường sau ([2], trang 301-302):

- Phiên bản của định dạng chứng nhận X.509 là v3 (giá trị 2).

- Số thứ tự của chứng nhận.
- Thuật toán chữ ký của nhà phát hành chứng chỉ: đó là mã hoá RSA và thuật toán băm SHA1.
- Nhà phát hành chứng nhận.
- Thời gian chứng nhận hiệu lực.
- Certificate subject, đó là định danh của người giữ chứng nhận, nếu là SS thì chứa địa chỉ MAC của thiết bị.
- Khoá công khai của người giữ chứng nhận.
- Thuật toán ký, thống nhất với thuật toán ký của nhà phát hành chứng chỉ.
- Chữ ký của nhà phát hành.

Chuẩn làm việc với hai kiểu chứng nhận: chứng nhận nhà sản xuất và chứng nhận SS. Nó không đưa ra chứng nhận BS. Chứng nhận nhà sản xuất sử dụng để định danh nhà sản xuất của thiết bị IEEE 802.16. Chứng nhận SS được sử dụng cho định danh một SS. BS sử dụng khoá công khai của nhà sản xuất và thông qua hạ tầng khoá công khai để kiểm tra chứng nhận SS.

4.3.3 Giao thức uỷ quyền quản lý khoá riêng

Giao thức uỷ quyền quản lý khoá riêng (Privacy Key Management Authorization protocol - PKM Authorization) là giao thức để BS cung cấp khoá uỷ quyền AK cho SS. ([6], trang 273)

Giao thức uỷ quyền bao gồm 3 bước: hai bản tin gửi từ SS tới BS và sau đó 1 bản tin gửi từ BS tới SS.

- Bước 1: SS gửi một bản tin tới BS, bản tin này chứa một chứng nhận X.509 định danh nhà sản xuất SS. BS sử dụng bản tin này để quyết định xem SS có phải là thiết bị tin cậy không.

- Bước 2: SS gửi một bản tin thứ 2 không đợi trả lời từ BS. Bản tin thứ hai chứa chứng nhận X.509 của SS, khả năng bảo mật của SS và SAID của nó. Các chứng nhận X.509 được sử dụng bởi BS để biết khoá công khai của SS. Nếu SS được uỷ quyền, khoá công khai của SS được BS sử dụng để xây dựng bản tin trả lời.
- Bước 3: Nếu BS xác định SS được uỷ quyền thì BS trả lời SS bằng bản tin thứ 3, BS khởi tạo một Authorization SA giữa BS và SS. Chỉ BS và SS biết AK, AK không bao giờ được tiết lộ cho thực thể khác.

Các bản tin như sau:

- Bản tin 1:
  SS -> BS: Cert (Manufacturer (SS))
- Bản tin 2:
  SS -> BS: Cert (SS) | Capabilities | SAID
- Bản tin 3:
  BS -> SS: RSA-Encrypt (PubKey(SS), AK) | Lifetime | SeqNo | SAIDList

Giải thích ý nghĩa các ký hiệu trong các bản tin trên mô tả trong bảng 4.2.

Bảng 4.2 Ý nghĩa các ký hiệu trong bản tin giao thức PKM Authorization

Ký hiệu	**Mô tả**
A->B:M	Thực thể A gửi cho thực thể B bản tin có giá trị M
Cert(Manufacturer(SS))	Chứng nhận X.509 định danh nhà sản xuất SS
Cert(SS)	Chứng nhận X.509 với khoá công khai của SS
Capabilities	Thuật toán mã hóa dữ liệu và uỷ quyền mà SS hỗ trợ
SAID	Liên kết an toàn giữa SS và BS (CID)
RSA-Encrypt(k,a)	Thực hiện mã hoá RSA giá trị tham số thứ hai a sử dụng khoá k
PubKey(SS)	Khoá công khai của SS, nằm trong Cert(SS)
AK	Khoá AK
Lifetime	Giá trị 32 bít không dấu chỉ ra thời gian tính bằng giây trước khi AK mất hiệu lực
SeqNo	Giá trị 4 bít định danh AK
SAIDList	Danh sách các mô tả SA, mỗi SA bao gồm một SAID, SA Type (primary, static, dynamic) và bộ mã hoá SA.

4.3.4 Giao thức quản lý khoá riêng

Giao thức quản lý khoá riêng (Privacy Key Management - PKM) là giao thức thiết lập Data SA giữa BS và SS. Điều này được thực hiện bởi hai hoặc ba bản tin gửi giữa BS và SS. ([6], trang 274)

- Bước 1: BS gửi bản tin 1 tới SS. Bước này không bắt buộc và bản

tin này được gửi chỉ khi BS muốn tạo khoá lại của Data SA hoặc muốn tạo mới SA. BS tính HMAC(1) để cho phép SS kiểm tra sự giả danh.

- Bước 2: SS gửi bản tin 2 tới BS để yêu cầu các tham số SA. SS phải sử dụng SAID từ danh sách SAID của giao thức uỷ quyền PKM hoặc từ bản tin 1 có HMAC(1) hợp lệ. SS gửi bản tin 2 cho từng Data SA. SS tính HMAC(2) để cho phép BS kiểm tra sự giả danh. BS có thể xác thực SS an toàn bởi HMAC(2) bởi vì chỉ SS có thể lấy được AK gửi trong bản tin 3 của giao thức PKM Authorization và AK không dự đoán được.
- Bước 3: Nếu BS kiểm tra thấy HMAC(2) hợp lệ và SAID thực sự là một trong các SA của SS, thì BS gửi bản tin 3. Bản tin 3 chứa OldTEK là TEK cũ sử dụng với SA đang dùng, NewTEK là TEK mới sử dụng sau khi TEK đang dùng quá hạn. Các TEK (OldTEK và NewTEK) được mã hoá sử dụng 3-DES trong chế độ ECB sử dụng khoá KEK trong Authorization SA. HMAC(3) được sử dụng để kiểm tra sự giả danh.

Các bản tin như sau:

- Bản tin 1 (không bắt buộc):
  BS -> SS: SeqNo | SAID | HMAC(1)
- Bản tin 2:
  SS -> BS: SeqNo | SAID | HMAC(2)
- Bản tin 3:
  BS -> SS: SeqNo | SAID | OldTEK | NewTEK | HMAC(3)

Giải thích ý nghĩa các ký hiệu trong các bản tin trên mô tả trong bảng 4.3.

Bảng 4.3 Ý nghĩa các ký hiệu trong bản tin giao thức PKM

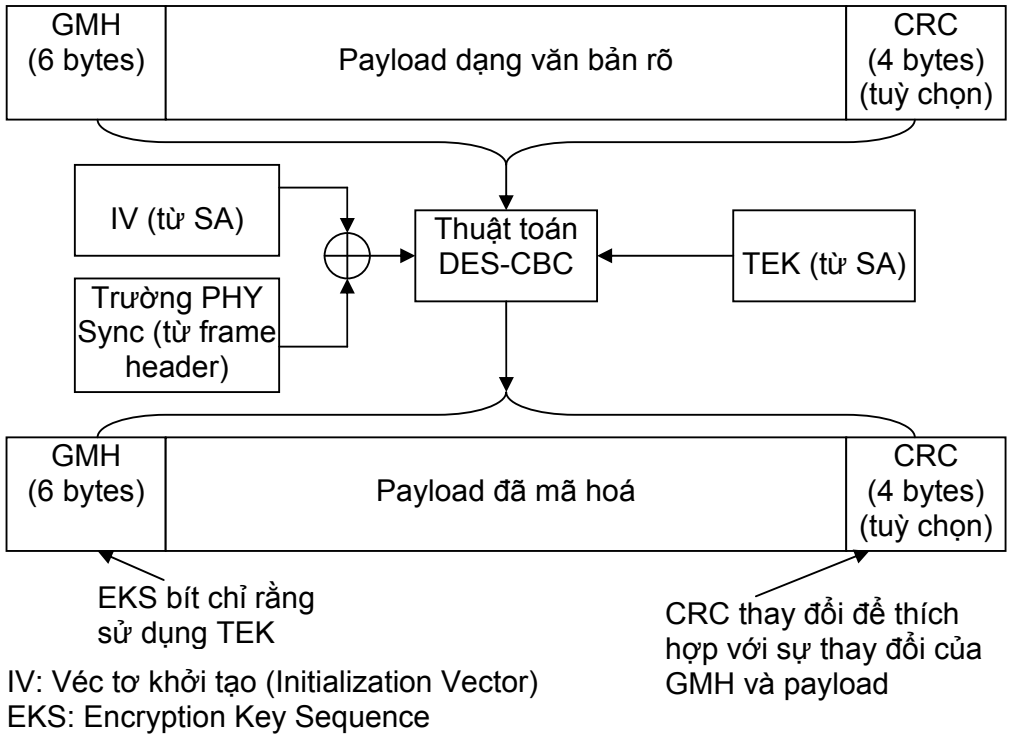
Ký hiệu	Mô tả
SeqNo	AK sử dụng cho trao đổi
SAID	Định danh của Data SA đã được tạo hoặc đã tạo lại
HMAC(1)	HMAC-SHA1 digest của SeqNo|SAID theo khoá Downlink HMAC của AK
HMAC(2)	HMAC-SHA1 digest của SeqNo|SAID theo khoá Uplink HMAC của AK
OldTEK	Véc tơ khởi tạo của TEK đã sinh trước đó, thời gian hiệu lực (theo giây), số thứ tự của Data SA chỉ định bởi SAID
NewTEK	Véc tơ khởi tạo của TEK tiếp theo, thời gian hiệu lực (theo giây), số thứ tự của Data SA chỉ định bởi SAID
HMAC(3)	HMAC-SHA1 digest của SeqNo | SAID | OldTEK | NewTEK theo khoá Downlink HMAC của AK

4.3.5 Mã hoá

Mã hoá trong lớp con bảo mật là DES-CBC, AES-CCM ([6], 295). Việc mã hoá thực hiện đối với trường payload, văn bản rõ trong MPDU nhưng không mã hoá MPDU GMH hoặc CRC (Hình 4.7). IEEE 802.16 không cung cấp sự xác thực dữ liệu. Có vấn đề không an toàn khi sử dụng mã hoá DES-CBC, vì thế chúng ta sẽ phân tích kỹ kiểu mã hoá này.

MPDU GMH có hai bít chỉ định việc sử dụng TEK. Nó không mang initialization vector chế độ CBC. Để tính toán MPDU initialization vector, mô đun mã hoá của IEEE 802.16 thực hiện XOR SA initialization vector với nội dung của trường PHY synchronization từ GMH mới nhất. Bởi vì SA

initialization vector không thay đổi và công khai cho TEK của nó và bởi vì trường PHY synchronization là lặp lại và có khả năng dự đoán, MPDU initialization vector là có khả năng dự đoán.



Hình 4.7 Quá trình mã hoá sử dụng DES-CBC trong IEEE 802.16

4.4 Phân tích vấn đề an toàn bảo mật của IEEE 802.16

Trong phần này, chúng ta tập trung xem xét vấn đề an toàn bảo mật của IEEE 802.16. Chúng ta sẽ xem xét vấn đề an toàn bảo mật theo hai khía cạnh:

- Phân tích vấn đề an toàn bảo mật của IEEE 802.16 dựa trên một số điểm yếu bảo mật đã phát hiện của IEEE 802.11.
- Phân tích xác định một số điểm yếu mới có thể của IEEE 802.16.

4.4.1 Tấn công làm mất xác thực

4.4.1.1 Đối với IEEE 802.11

Trong mạng 802.11, khi một nút mới muốn tham gia vào mạng, nó phải qua quá trình xác thực và quá trình liên kết trước khi nó được phép truy cập vào mạng. Trong quá trình xác thực và liên kết chỉ một số bản tin cho phép. Một trong các bản tin đó là bản tin cung cấp cho một nút khả năng yêu cầu làm mất xác thực từ nút khác. Khi một nút nhận bản tin bỏ xác thực, nó sẽ tự loại bỏ nó khỏi mạng và trở về trạng thái cơ sở.

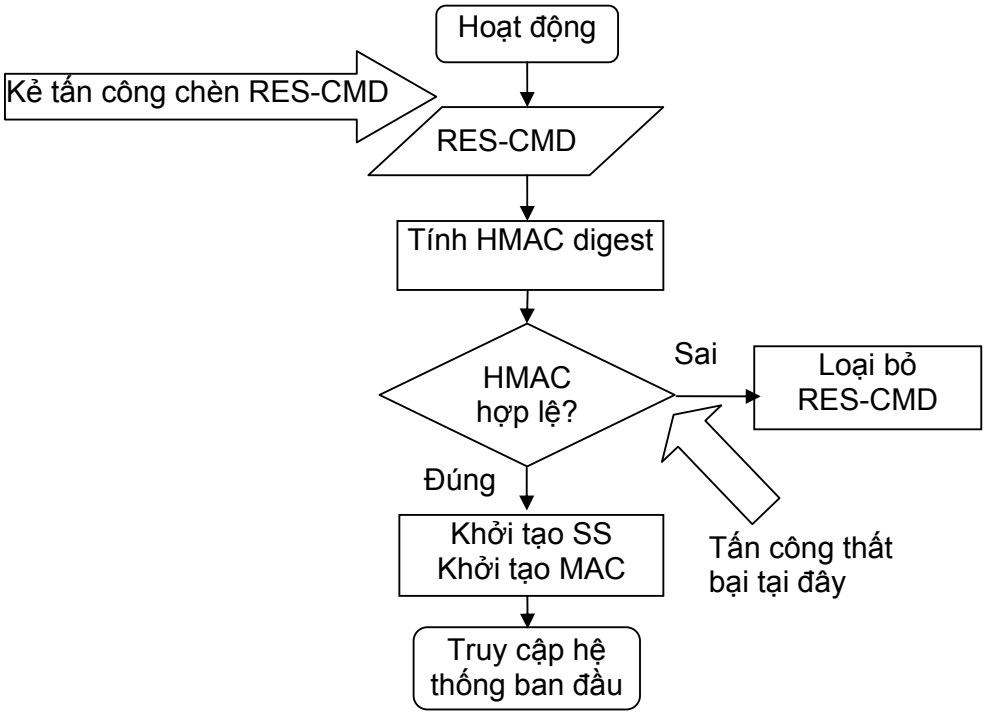
Trong tấn công bỏ xác thực, kẻ tấn công sẽ tìm địa chỉ của điểm truy cập (AP) điều khiển mạng. AP trong mạng 802.11 có vai trò tương tự BS trong 802.16. Một số AP không quảng bá sự tồn tại của nó trong mạng nhưng địa chỉ của nó có thể tìm được nếu chúng ta lắng nghe lưu lượng giữa AP và các nút khác. Khi kẻ tấn công có địa chỉ AP, người này sẽ sử dụng địa chỉ quảng bá để gửi bản tin làm mất xác thực tới tất cả các nút. Các nút nhận được bản tin này sẽ chấm dứt truyền thông với mạng. Bước tiếp theo, tất cả các nút đã bị làm mất xác thực sẽ thử kết nối lại, xác thực lại và liên kết lại tới AP. Sự truyền lặp lại các bản tin làm mất xác thực có thể làm tắc lưu lượng mạng.

Các kiểu tấn công sử dụng các bản tin khác để gây ra vấn đề tương tự thì đều được gọi là kiểu tấn công bỏ xác thực. Có 3 điểm trong bản tin làm mất xác thực khiến khả năng tấn công làm mất xác thực có thể thực hiện được là:

- Bản tin làm mất xác thực không được kiểm tra xác thực, ngoại trừ việc kiểm tra địa chỉ nguồn của bản tin.
- Không có sự mã hoá thông tin sử dụng để xây dựng bản tin, vì thế kẻ tấn công dễ dàng xác định được thông tin trong đó.
- Nút nhận bản tin làm mất xác thực giả chấp nhận nó mà không chú ý tới thời gian gửi đi.

4.4.1.2 Đối với IEEE 802.16

IEEE 802.16 có các bản tin MAC sử dụng để làm mất xác thực như trong IEEE 802.11. Đầu tiên là bản tin Reset Command (RES-CMD) được gửi bởi BS tới SS để sau đó khởi tạo lại trạng thái. Khi SS nhận bản tin RES-CMD, nó sẽ khởi tạo truy cập lại hệ thống. Tương tự, BS có thể gửi bản tin De/Re-register command tới SS để SS thay đổi trạng thái truy cập.



Hình 4.8 Tấn công làm mất xác thực sử dụng RES-CMD

Khác với 802.11, 802.16 có cơ chế bảo vệ chống lại việc lạm dụng bản tin này. IEEE 802.16 sử dụng HMAC Digest dùng SHA-1 để xác thực bản tin. HMAC làm việc như sau: Mã xác thực được tính sử dụng bản tin ban đầu và khoá mật dùng chung. Trong 802.16, 160 bít giá trị băm được thêm vào bản tin ban đầu. Khi bên nhận nhận được bản tin, bên nhận sẽ tính lại giá trị băm sử dụng bản tin đã nhận được và khoá mật dùng chung. Sau đó, bên nhận so sánh với giá trị băm đã tính với giá trị nhận được. Nếu khác nhau thì bên nhận biết bản tin đã bị thay đổi, do đó sẽ loại bỏ bản tin này. (Hình 4.8)

Việc tấn công làm mất xác thực không áp dụng được trong 802.16 vì:

- Khoá dùng chung giữa BS và SS là bí mật, sử dụng chuẩn mã hoá mạnh 3-DES 128 bít khoá hoặc RSA 1024 bít khoá.
- Thuật toán băm mạnh, kẻ tấn công không thể thử mọi khả năng của giá trị băm.
- Chuẩn 802.16 sử dụng cơ chế mô đun hoá nên trong tương lai nếu các thuật toán hiện tại không an toàn thì thuật toán khác có thể thay thế.

4.4.2 Tấn công lặp lại

4.4.2.1 Đối với IEEE 802.11

Kiểu tấn công lặp lại là kiểu tấn công mà kẻ tấn công chặn thông tin hợp lệ rồi sử dụng lại. Thông tin hợp lệ ở đây có thể là một bản tin. Kẻ tấn công không thay đổi bản tin mà chỉ gửi lại bản tin đó ở một thời điểm thích hợp.

Trong mạng 802.11, kiểu tấn công lặp lại có thể tạo ra từ chối dịch vụ. Bởi vì nút nhận bản tin hợp lệ sẽ dành thời gian để giải mã xử lý bản tin. Do 802.11 không có cơ chế để phát hiện và loại bỏ bản tin lặp lại nên có khả năng bị tấn công lặp lại.

4.4.2.2 Đối với IEEE 802.16

Trong 802.16, kẻ tấn công có thể lấy được toàn bộ bản tin (bao gồm HMAC) và lặp lại bản tin này không thay đổi gì nội dung. Trong khi HMAC đảm bảo là bản tin không thay đổi, nó không cung cấp cho chúng ta bất kỳ thông tin gì khác, chỉ người gửi và nội dung bản tin được xác thực. Nếu kẻ tấn công chặn bản tin và gửi lại, bản tin sẽ được xác thực bình thường nếu khoá mã hoá vẫn giữ nguyên.

HMAC đảm bảo bản tin không bị thay đổi, khả năng bản tin sử dụng lại dựa trên chi tiết bên trong của nó. Nếu có một thông tin tồn tại ngắn trong bản tin như nhãn thời gian hoặc số thứ tự, thì kẻ tấn công sẽ khó khăn trong việc sử dụng lại bản tin để thực hiện tấn công lặp lại. Thông tin tồn tại ngắn được sử dụng bởi bên nhận để xác định việc truyền lại và loại bỏ bản tin lặp lại.

Kẻ tấn công có thể cố gắng sử dụng RES-CMD để thực hiện tấn công lặp lại vì RES-CMD không có số thứ tự, không có nhãn thời gian. Nhưng việc tấn công lặp lại sử dụng RES-CMD đối với 802.16 vẫn không thể thực hiện thành công.

Chúng ta biết 802.16 đòi hỏi HMAC được tính sử dụng bản tin và MAC header. HMAC được truyền không thay đổi để thực hiện tấn công lặp lại và đó là vấn đề. Trong MAC header, có CID của SS, nó được khởi tạo lại khi nhận được bản tin RES-CMD. Sau khi khởi tạo lại, SS được gán CID mới được cung cấp bởi BS. Giá trị CID mới được chọn từ 65536 giá trị. Vì vậy, kẻ tấn công sẽ không thể nhận được bản tin từ cùng một SS mà có cùng CID để có thể thực hiện việc tấn công. Thậm chí nếu có được điều đó, thì SS thoả thuận một tập khoá mới để xác thực bản tin. Vì thể, kẻ tấn công không thể thực hiện tấn công lặp lại sử dụng bản tin RES-CMD. Tấn công sử dụng DREG-CMD cũng không thực hiện được với lý do tương tự.

4.4.3 Tấn công sử dụng điểm truy cập giả danh

4.4.3.1 Đối với IEEE 802.11

Tấn công sử dụng điểm truy cập giả danh (AP giả danh) là một kiểu tấn công mà kẻ tấn công đứng giữa hai nút và thao tác trên lưu lượng giữa hai nút. Kẻ tấn công có thể lấy toàn bộ thông tin qua mạng. Trong mạng có dây kiểu tấn công này khó thực hiện vì nó đòi hỏi truy cập tới phương tiện. Trong

mạng không dây, điều này thực hiện dễ dàng. Đầu tiên, kẻ tấn công thiết lập một AP. AP giả danh này được thiết lập sử dụng thông tin của AP hợp pháp. Bước tiếp theo là để nạn nhân kết nối tới AP giả danh bằng cách đợi người sử dụng kết nối tới hoặc gây từ chối dịch vụ trong AP hợp pháp để người sử dụng sẽ phải kết nối lại. Trong mạng 802.11, việc chọn AP được thực hiện dựa trên độ mạnh của tín hiệu nhận được. Điều duy nhất kẻ tấn công phải làm là đảm bảo độ mạnh tín hiệu của AP giả danh có thể bằng cách đặt gần nạn nhân hơn AP hợp pháp hoặc sử dụng ăng ten định hướng.

Sau khi nạn nhân kết nối tới AP giả danh, nạn nhân làm việc bình thường như khi kết nối tới AP hợp pháp. Sau đó, kẻ tấn công lấy các thông tin để có thể truy cập vào mạng hợp pháp.

Kiểu tấn công này tồn tại vì 802.11 không đòi hỏi xác thực hai chiều giữa AP và các nút. Các tài liệu xác thực AP thường được quảng bá qua mạng. Điều này khiến kẻ tấn công có thể nghe trộm và lấy được các thông tin. Xác thực WEP được sử dụng bởi các nút để xác thực chính chúng với AP không đủ an toàn vì kẻ tấn công có thể sử dụng bộ giải mã để lấy được mật khẩu.

4.4.3.2 Đối với IEEE 802.16

Trong giao thức PKM, có một số bản tin trao đổi giữa BS và SS để kiểm tra định danh. Như đã trình bày trong phần 4.3.3, để xác thực SS, quá trình như sau:

- SS gửi một bản tin tới BS, chứa chứng nhận X.509 định danh nhà sản xuất SS.
- SS gửi bản tin thứ hai không đợi trả lời từ BS. Bản tin thứ hai chứa chứng nhận X.509 của SS và khoá công khai, khả năng hỗ trợ an toàn bảo mật và SAID của nó. Chứng nhận X.509 được sử dụng để BS xác thực SS và khoá công khai của SS để BS xây dựng lại bản

tin trả lời.

- Nếu BS xác định SS được xác thực thì nó trả lời bản tin thứ ba, khởi tạo một SA giữa BS và SS.

Như vậy, chúng ta nhận thấy BS không được xác thực bởi SS. Đây là một điểm yếu của IEEE 802.16 có thể bị kẻ tấn công khai thác để thực hiện kiểu tấn công sử dụng điểm truy cập giả danh.

4.4.4 Tấn công RNG-RSP

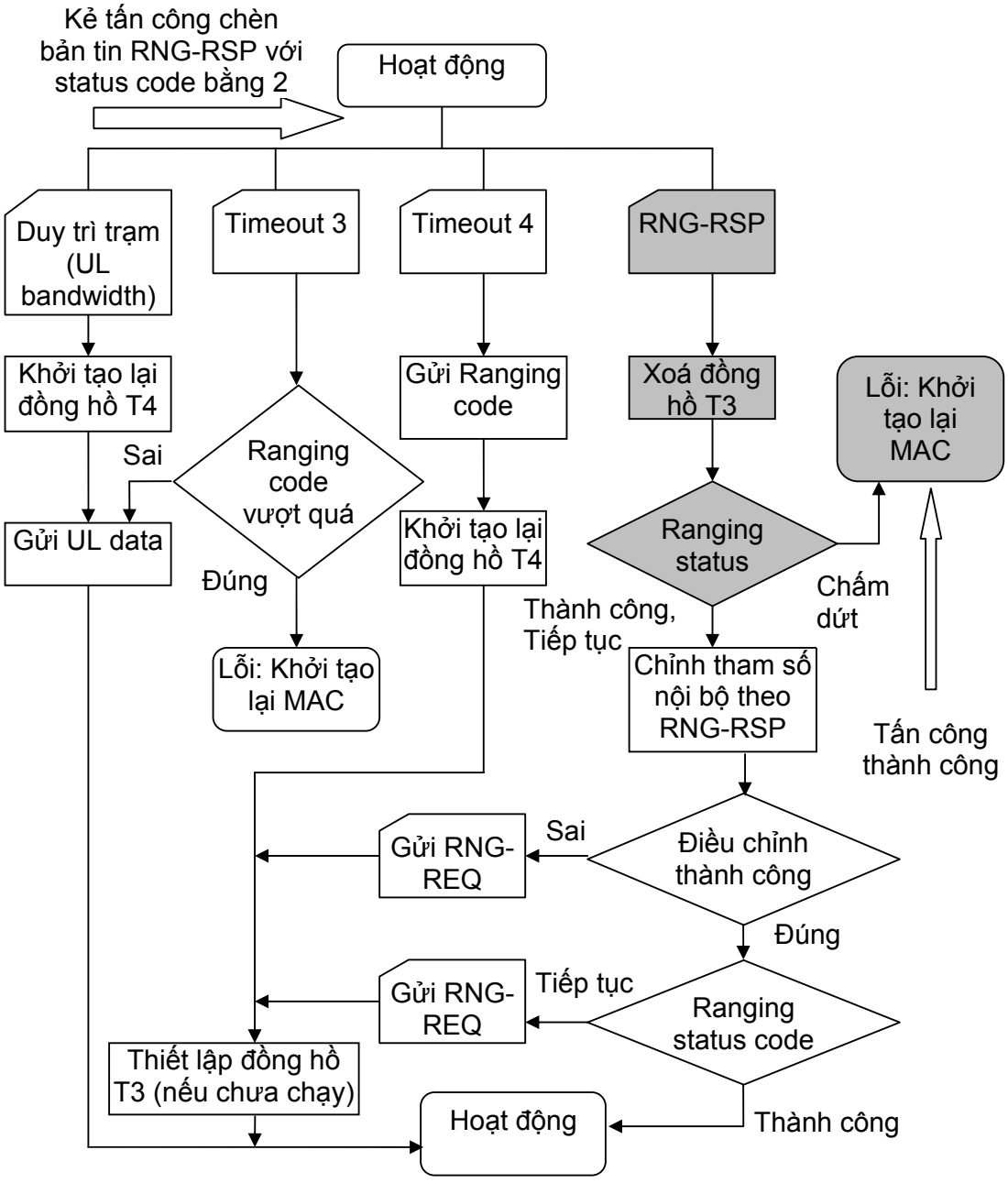
Khi SS muốn gia nhập mạng nó gửi tới BS bản tin Ranging Request (RNG-REQ). Bản tin này thông báo với BS về sự tồn tại của SS và các thông tin về tốc độ truyền, năng lượng, tần số,... BS trả lời SS bằng cách gửi bản tin Ranging Response (RNG-RSP).

Bảng 4.4 Cấu trúc của bản tin RNG-RSP

Kiểu bản tin quản lý	Uplink Channel ID (8 bít)	Nội dung bản tin
5 = RNG-RSP	Định danh của kênh đường lên trên đó BS đã nhận RNG-REQ	Các nội dung có thể mô tả trong bảng 4.5

BS có thể sử dụng RNG-RSP để nói SS thay đổi kênh đường lên và đường xuống, mức năng lượng truyền, chấm dứt việc truyền hiện tại và khởi tạo lại MAC. Lý do chính RNG-RSP có thể bị lợi dụng là bản tin này không được mã hoá và không được xác thực, không có trạng thái. Bất kỳ SS nhận RNG-RSP sẽ xử lý dựa trên thông tin của bản tin này. IEEE 802.16 chỉ yêu cầu duy nhất các trường là Timing Adjustment, Power Lever Adjustment và

Ranging Status (Bảng 4.5 mô tả chi tiết về các trường trong bản tin RNG-RSP). Một cách để lợi dụng RNG-RSP là sử dụng trường Ranging Status với giá trị 2 nghĩa là chấm dứt truyền. Hình 4.9 minh hoạ quá trình tấn công sử dụng bản tin RNG-RSP.



Hình 4.9 Quá trình tấn công RNG-RSP

Bảng 4.5 Nội dung bản tin RNG-RSP

Tên	Kiểu (1 byte)	Chiều dài (byte)	Giá trị
Timing Adjust	1	4	Giá trị thời gian điều chỉnh Tx (giá trị có dấu 32 bít).
Power Level Adjust	2	1	Giá trị năng lượng điều chỉnh (giá trị có dấu 8 bít). Chỉ ra sự thay đổi của mức năng lượng truyền để SS truyền tới BS với mức năng lượng mong muốn.
Offset Frequency Adjust	3	4	Giá trị tần số điều chỉnh (giá trị có dấu 32 bít). Chỉ ra sự thay đổi của tần số truyền để SS điều chỉnh thích hợp với tần số của BS.
Ranging Status	4	1	Chỉ ra bản tin đường lên được nhận trong giới hạn của BS hay không: 1 = tiếp tục, 2 = bỏ qua, 3 = thành công, 4 = thực hiện lại
Downlink Frequency override	5	4	Tần số trung tâm (kHz) của kênh đường xuống mới mà SS thực hiện ranging lại.
Uplink channel ID override	6	1	Định danh của kênh đường lên trong đó SS thực hiện lại ranging.
SS MAC	8	6	Địa chỉ MAC của SS

Address			
Basic CID	9	2	Basic CID được gán bởi BS khi khởi tạo truy cập
Primary Management CID	11	2	Primary Management CID được gán bởi SS khi khởi tạo truy cập
PHY Specific Value	12-16		Cung cấp hỗ trợ OFDMA và AAS

(Nguồn: [6], trang 665)

4.4.5 Tấn công Auth Invalid

Máy trạng thái uỷ quyền là một phần của PKM. Thường nó sử dụng hai bản tin quản lý MAC: PKM-REQ và PKM-RSP. SS gửi PKM-REQ tới BS và BS trả lời với PKM-RSP.

Bảng 4.6 Định dạng của bản tin PKM

Kiểu bản tin quản lý	Message Code (8 bít)	PKM Identifier (8 bít)	PKM Attribute
9 = PKM-RSP 10=PKM-REQ	Xác định kiểu của bản tin PKM	Số thứ tự của bản tin	Các thuộc tính của bản tin PKM, thay đổi phụ thuộc vào kiểu của bản tin

Trường Message Code của bản tin là trường 8 bít xác định kiểu của bản tin PKM. Nếu bản tin có mã không hợp lệ thì nó sẽ bị loại bỏ.

Bảng 4.7 Mã của bản tin PKM

Mã	Kiểu bản tin PKM
0-2	Chưa sử dụng
3	Security Association Add
4	Auth Request
5	Auth Reply
6	Auth Reject
7	Key Request
8	Key Reply
9	Key Reject
10	Auth Invalid
11	TEK Invalid
12	Authentication Info
13-255	Chưa sử dụng

PKM Identifier là một trường 8 bít như là số thứ tự. Mỗi khi PKM-REQ được gửi bởi SS, PKM Indentifier sẽ tăng. Khi BS trả lời với PKM-RSP, Indentifier của bản tin tương ứng sẽ được đưa vào. Nếu SS nhận bản tin PKM-RSP với Identifier khác với Indentifier trong bản tin yêu cầu đã gửi đi, SS sẽ bỏ qua nó.

Trường PKM Attribute thay đổi phụ thuộc vào kiểu bản tin PKM. Trường này thường chứa các thông tin như mã lỗi, thời gian tồn tại của khoá và thông báo. Ví dụ bản tin Security Association Add (mã là 3), trường PKM Attribute chứa giá trị thứ tự của khoá uỷ quyền và một chuỗi các mô tả của SA.

Trong bảng 4.7, có 4 kiểu bản tin PKM được đánh dấu: Auth Reject, Key Reject, Auth Invalid và TEK Invalid. Các bản tin này được chọn vì

chúng có tác động phủ định trong quá trình xác thực của SS. Bằng cách sử dụng chúng các bản tin này có thể thực hiện kiểu tấn công bỏ xác thực. Mặc dù, chúng nhìn có vẻ giống nhau và chúng ta thấy đều có khả năng sử dụng chúng để thực hiện kiểu tấn công bỏ xác thực. Tuy nhiên Auth Reject, Key Reject và TEK Invalid không thể sử dụng. Lý do là các bản tin này đòi hỏi HMAC digest để xác thực bản tin. Ngoài ra, Auth Reject được chấp nhận bởi SS trong trạng thái Auth Wait và khoảng thời gian trạng thái này rất ngắn. Với Key Reject, lý do thứ 2 là PKM Identifier code tương ứng với yêu cầu của SS đòi hỏi sử dụng để tính HMAC vì thế bản tin Key Reject là không thể sử dụng được để tấn công.

Bảng 4.8 Các thuộc tính của bản tin Key Reject

Thuộc tính	Nội dung
Key Sequence Number	Số thứ thự Authorization Key
SAID	Định danh của liên kết bảo mật
Error Code	Mã lỗi xác định lý do từ chối Key Request
Display String (không bắt buộc)	Chuỗi chứa lý do Key Reject
HMAC-Digest	Mã xác thực bản tin sử dụng thuật toán băm SHA

Bản tin cuối cùng là Auth Invalid. Bản tin này không xác thực HMAC digest. Nó cũng không cần được gửi tại một trạng thái nào đó của MAC, nó hầu như luôn được chấp nhận từ SS. SS trong trạng thái Auth Wait thời gian ngắn, ở trạng thái Authorized trong phần lớn thời gian hoạt động của nó. BẢn tin Auth Invalid được chấp nhận trong suốt trạng thái Authorized. Bản tin Auth Invalid không chứa số thứ tự PKM Identifier. Lý do là bản tin này không xử lý theo trạng thái. Các lý do này khiến bản tin giả danh dễ dàng được chấp nhận bởi nạn nhân.

Bảng 4.9 Các thuộc tính của bản tin Auth Invalid

Thuộc tính	Nội dung
Error Code	Mã lỗi xác định lý do Authorization không hợp lệ
Display String (không bắt buộc)	Chuỗi mô tả tình trạng lỗi

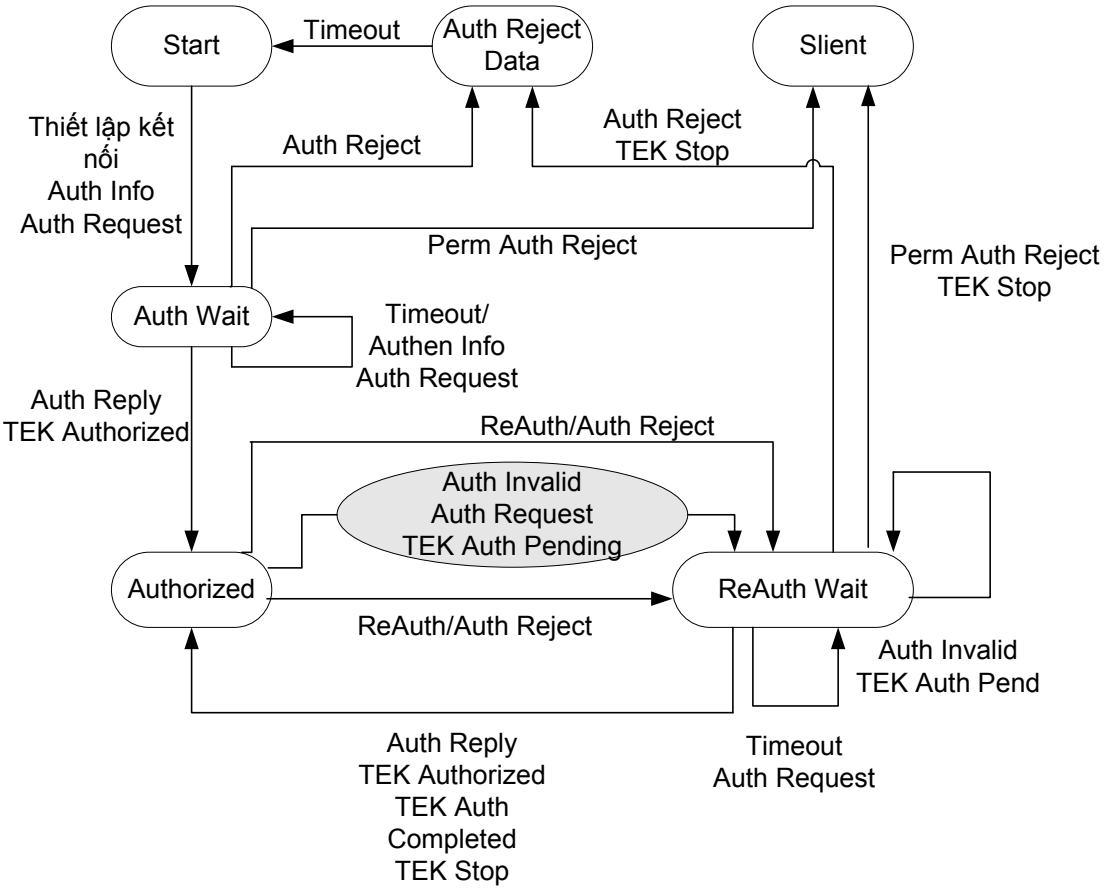
Mã lỗi được gửi từ BS khi SS HMAC không hợp lệ. Mã lỗi 0 chỉ rằng không xác định lý do gây lên lỗi xác thực có thể sử dụng trong bản tin tấn cổng.

Bảng 4.10 Các giá trị mã lỗi của bản tin Authentication

Mã lỗi	Bản tin	Mô tả
0	Tất cả	Không cung cấp thông tin
1	Auth Reject, Auth Invalid	SS không được uỷ quyền
2	Auth Reject, Key Reject	SAID không được uỷ quyền
3	Auth Invalid	Gửi không do yêu cầu
4	Auth Invalid, TEK Invalid	Thứ tự khoá không hợp lệ
5	Auth Invalid	Lỗi xác thực bản tin Key Request
6	Auth Reject	Lỗi bị xảy ra nhiều lần

Khi SS nhận bản tin Auth Invalid, SS sẽ chuyển từ trạng thái Authorized sang trạng thái ReAuth Wait và SS sẽ đợi tới khi nhận được bản tin nào đó từ BS. Nếu ReAuth Wait quá hạn trước khi nhận được bản tin từ BS, SS gửi Reauth Request để tham gia lại vào mạng. Trong khi SS ở trạng thái ReAuth, SS có thể nhận bản tin Auth Reject. Khi đó, lỗi uỷ quyền bị xảy ra nhiều lần. Khi SS nhận bản tin như thế, SS sẽ vào trạng thái silent chấm dứt mọi lưu lượng và sẵn sàng trả lời bất kỳ bản tin quản lý nào gửi bởi BS. Đây là một

cách mà kẻ tấn công có thể khả năng thao tác với máy trạng thái uỷ quyền.



Hình 4.10 Máy trạng thái uỷ quyền đánh dấu bản tin Auth Invalid

4.4.6 Đánh giá và đề xuất

Các phân tích trên chuẩn IEEE 802.16-2004 cho thấy rằng 802.16 có khả năng bảo mật tốt hơn nhiều so với 802.11, nhưng nó vẫn còn có các điểm yếu.

Để khắc phục các điểm yếu đã phân tích ở trên, chúng ta thấy cần phải:

- Xác thực lẫn nhau: Lỗ hổng nguy hiểm của 802.16 là thiếu chứng nhận của BS. Cách duy nhất để SS được bảo vệ chống lại sự giả danh là thay thế lược đồ xác thực cũ bởi lược đồ xác thực mới là

xác thực lẫn nhau.

- Bảo vệ dữ liệu: Hỗ trợ các phương pháp bảo vệ dữ liệu an toàn hơn DES-CBC. DES-CBC đòi hỏi một véc tơ khởi tạo mà véc tơ này có thể dự đoán được. Để sửa lỗi này của DES-CBC có thể véc tơ khởi tạo nên được sinh ngẫu nhiên cho mỗi frame và chèn vào trường payload. Vì thế, kẻ tấn công sẽ không thể dự đoán được véc tơ khởi tạo và giải mã dữ liệu truyền qua mạng.

Thời điểm 8/2006, khi chuẩn IEEE 802.16e-2005 công bố cho tất cả mọi người, qua nghiên cứu chúng tôi thấy rằng, hầu hết các cải tiến an toàn bảo mật đã được tích hợp vào 802.16e. Đó là PKMv2 được sử dụng thay PKM.

PKMv2 chỉ định bắt tay 3 chiều để thiết lập khoá AK giữa BS và SS. Các số ngẫu nhiên được đưa vào để đảm bảo sự trao đổi được xác thực. Sự trao đổi AK giữa BS và SS an toàn hơn. Hai phương pháp xác thực, xác thực lẫn nhau dựa vào RSA và EAP được cung cấp. Chúng sinh khoá đều dựa trên kiến trúc phân cấp khoá WiMAX. Trong xác thực lẫn nhau dựa vào RSA, chứng nhận X.509 được sử dụng cho cả BS và SS, nó giải quyết vấn đề về sự giả danh.([7], trang 331)

Chuẩn 802.16-2004 định nghĩa HMAC digest cho các bản tin quản lý. Trong PKMv2, kiểu digest này có thể thoả thuận để sử dụng HMAC hoặc CMAC ([7], trang 280). CMAC là mã xác thực bản tin dựa trên AES.

Một số kiểu mật mã an toàn hơn được đưa vào, 802.16e đưa thêm AES-CTR và AES-CBC. AES-CCM mà 802.16-2004 định nghĩa bảo vệ lưu lượng dữ liệu, bảo vệ tính toàn vẹn, riêng tư, xác thực. AES-CBC chỉ cung cấp khả năng bảo vệ tính riêng tư nhưng không cần 12 byte header mà AES-CCM sử dụng. Nó giảm lưu lượng mạng nhưng cũng giảm khả năng an toàn bảo mật. AES-CTR sử dụng để mã hoá lưu lượng MBS (Multicast Broastcast Service).

Các cải tiến của 802.16e giúp tạo các mô hình bảo mật khác nhau cho các tổ chức khác nhau, nó cung cấp sự bảo vệ các bản tin quản lý, cân bằng giữa an toàn bảo mật với lượng dữ liệu header.

4.5 Kết chương

Qua chương này, chúng ta đã nghiên cứu về các yêu cầu đặc điểm chung tìm hiểu về mô hình các thực thể chức năng đảm bảo an toàn bảo mật do diễn đàn WiMAX đưa ra. Sau đó, nghiên cứu về cơ chế đảm bảo an toàn bảo mật mà IEEE 802.16-2004 hỗ trợ. Trong đó, chúng ta đã nghiên cứu về liên kết bảo mật, chứng nhận X.509, giao thức uỷ quyền quản lý khoá riêng, giao thức quản lý khoá riêng và mã hoá của chuẩn 802.16-2004. Trong chương này, chúng ta đã tập trung nghiên cứu vấn đề an toàn bảo mật của IEEE 802.16-2004 dựa trên các kiểu tấn công đã được biết tới của IEEE 802.11 bao gồm: tấn công làm mất xác thực, tấn công lặp lại, tấn công sử dụng điểm truy cập giả danh. Chúng ta đã nghiên cứu hai kiểu tấn công dựa vào cơ chế hoạt động theo máy trạng thái của MAC là tấn công sử dụng RNG-RSP và tấn công Auth Invalid. Cuối cùng, chúng ta đã có những xem xét những cải tiến mới nhất mà IEEE 802.16e bổ sung hoàn thiện.

KẾT LUẬN

Công nghệ WiMAX là một công nghệ mạng không dây băng thông rộng mới đang được phát triển. Công nghệ này đang được nhiều nhà ứng dụng, nhà cung cấp dịch vụ, nhà nghiên cứu quan tâm và chắc chắn sẽ được triển khai cung cấp dịch vụ trong tương lai gần. Vấn đề chất lượng dịch vụ và vấn đề an toàn bảo mật là những vấn đề được quan tâm hàng đầu đối với công nghệ mạng không dây. Đứng trước vấn đề đó, chúng tôi đã thực hiện luận văn này nhằm xác định khả năng đáp ứng của công nghệ đối với vấn đề chất lượng dịch vụ và an toàn bảo mật. Sau đây là các tổng kết về những kết quả cũng như hướng phát triển của đề tài.

Những kết quả mà luận văn đã làm được:

- Tìm hiểu các vấn đề lý thuyết về mạng WiMAX như khái niệm, ứng dụng, các phiên bản WiMAX, bộ chuẩn IEEE 802.16, chứng nhận sản phẩm WiMAX, sự phát triển của công nghệ WiMAX, xu hướng phát triển của mạng không dây băng thông rộng.
- Nghiên cứu mô hình kiến trúc của mạng WiMAX, các đặc điểm khi triển khai mạng WiMAX.
- Nghiên cứu mô hình chất lượng dịch vụ của mạng WiMAX, cơ chế đảm bảo chất lượng dịch vụ của IEEE 802.16.
- Phân tích chỉ ra những điểm chưa định nghĩa trong mô hình chất lượng dịch vụ của IEEE 802.16.
- Đề xuất hoàn thiện cơ chế kiểm soát cho phép trong vấn đề chất lượng dịch vụ của IEEE 802.16.
- Nghiên cứu một giải pháp lập lịch gói tin của Claudio Cicconetti và các tác giả khác đã được trình bày trong IEEE Network. Sau đó đưa

ra các đề xuất khắc phục hạn chế đã đề cập trong giải pháp này, đề xuất phương pháp áp dụng thuật toán DRR vào việc lập lịch gói tin đường lên.

- Nghiên cứu mô hình an toàn bảo mật của mạng WiMAX, cơ chế an toàn bảo mật của IEEE 802.16.
- Phân tích chứng minh IEEE 802.16-2004 không thể bị tấn công bởi các kiểu tấn công là tấn công làm mất xác thực, tấn công lặp lại.
- Phân tích chứng minh IEEE 802.16-2004 có thể bị tấn công bởi các kiểu tấn công là tấn công sử dụng điểm truy cập giả danh, tấn công dùng bản tin RNG-RSP, tấn công dùng bản tin Auth Invalid.
- Chỉ ra các cải tiến mới nhất của chuẩn IEEE 802.16 bổ sung trong IEEE 802.16e-2005 về vấn đề bảo mật.

Một số hướng phát triển của luận văn:

- Nghiên cứu vấn đề phối hợp giữa các lớp để đảm bảo chất lượng dịch vụ theo khung làm việc chất lượng dịch vụ IntServ, DiffServ.
- Nghiên cứu đánh giá chi tiết về vấn đề an toàn bảo mật ở các mức trên MAC trong mạng WiMAX.
- Xây dựng mô đun WiMAX cho công cụ mô phỏng NS-2 để ứng dụng cho việc kiểm tra đánh giá hiệu quả các thuật toán, mô hình trên mạng WiMAX.
- Nghiên cứu vấn đề phối hợp giữa mạng WiMAX với các mạng khác.

TÀI LIỆU THAM KHẢO

[1] Claudio Cicconetti, Luciano Lenzini, Enzo Mingozzi, Carl Eklund (2006), "Quality of service support in IEEE 802.16 networks", *IEEE Network*, Vol. 20 (2), pp. 50-55.

[2] David Johnston, Jesse Watker (2004), "Overview of IEEE 802.16 Security", *IEEE Security & Privacy,* Vol. 2 (3), pp. 40-48.

[3] John Soldatos (2005), "On the Building Blocks of Quality of Service in Heterogeneous IP Networks", *IEEE Communications Surveys & Tutorials,* Vol. 7 (1), pp. 70-89.

[4] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence (2000), *RFC2904 – AAA Authorization Framework,* IETF.

[5] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence (2000), *RFC 2905 - AAA Authorization Application Examples,* IETF.

[6] LAN MAN Standards Committee of IEEE Computer Society and the IEEE Microwave Theory and Techniques Society (2004), *IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems,* IEEE STD 802.16-2004.

[7] LAN MAN Standards Committee of IEEE Computer Society and the IEEE Microwave Theory and Techniques Society (2006), *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems*

Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE STD 802.16e-2005.

[8] Michael Best, Bjorn Pehrson (2005), *Broadband provisioning for developing countries,* ITU 6th Global Symposium For Regulators.

[9] M. Shreedhar, George Varghese (1996), "Efficient Fair Queuing using Deficit Round Robin", *IEEE/ACM Transactions on Networking*, Vol. 4 (3), pp. 375-385.

[10] Senza Fili (2005), *Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks,* WIMAX Forum.

[11] WiMAX Forum (2006), *Mobile WiMAX - Part I: A Technical Overview and Performance Evaluation.*

[12] WiMAX Forum (2006), *Recommendations and Requirements for Networks based on WiMAX Forum Certified™ Products,* Release 1.0, pp. 21-25.

[13] WiMAX Forum (2006), *WiMAX End-to-End Network Systems Architecture Stage 2: Architecture Tenets, Reference Model and Reference Points, Part 1.*

[14] WiMAX Forum (2006), *WiMAX End-to-End Network Systems Architecture Stage 2: Architecture Tenets, Reference Model and Reference Points, Part 2.*

[15] WiMAX Forum (2006), *WiMAX End-to-End Network Systems Architecture Stage 2: Architecture Tenets, Reference Model and Reference Points, Part 3.*

[16] WiMAX Forum (2006), *WiMAX End-to-End Network Systems Architecture Stage 3: Detailed Protocols and Procedures.*

[17] WiMAX Forum (2006), *WiMAX Forum Mobile Certification Profile v1.0.*

[18] The IEEE 802.16 Working Group on Broadband Wireless Access Standards, www.ieee802.org/16/

[19] WiMAX Forum, www.wimaxforum.org