802.11f 로밍을 지원하는 Diameter IAPP 서버의 설계

함 영 환*, 정 병 호**

요 약

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 이와 같은 무선랜 환경에서 무선랜 단말이 AP(Access Point)사이를 로밍(Roaming)할 수 있게 하는 프로토콜로서 IAPP(InterAccess Point Protocol)가 있고 관련된 IEEE표준으로 802.11f가 있다. 이와 같은 802.11f를 지원하는 액세스포인트를 위해서는 IAPP서버의 역할을 수행하는 라디우스(RADIUS) 서버가 필요하다. 여기에서는 라디우스 대신 보다 확장성과 신뢰성이 뛰어난 프로토콜인 Diameter를 사용한 IAPP서버의 설계와 기존 시스템과의 연동방안에 대해서 제안하였다.

Ⅰ. 서 론

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 이와 같은 무선랜 환경에서 무선랜 단말이 액세스포인트(Access Point)사이를 로밍할 수 있게 하는 프로토로서 IAPP가 있고 IAPP는 IEEE 802.11f에 정의 있다[1] [2].

IAPP는 AP안의 Management Entity가 AP안에 어나는 이벤트를 처리하기 위해 다른 AP와 통신할 때 사용되는 통신 프로토콜이다. IAPP서비스의 구성요소는 AP, 스테이션, 그리고 연결된 DS(Distribu System)이다. 또한 IAPP에서는 IP주소의 맵핑과의 분배를 위해서 라디우스 서버를 사용한다[3] [4] [5]. IAPP를 위한 라디우스 서버의 사용예를 정리하면 다음과 같다.

1) AP의 인증 : AP가 IAPP-INITIATE서비스에 ESS에 속하는지 verify, IAPP-MOVE서비스시에 old AP와 new AP가 같은 ESS에 속하는지 verify

2) BSSID와 IP주소의 맵핑 : IAPP-MOVE서비스에 사용

3) 키분배

* Group SA(Security Association) 의 분배 : IAPP-INITIATE서비스에 AP에 전송하여 ADD-Notify패킷의 multicast시에 패킷 암호화를 위해 사용

* AP-to-AP pair SA의 분배 : IAPP-MOVE 서비스시에 pair SA를 생성하여 분배함으로써 AP사이에 보안 채널(secure channel)을 생성하여 MOVE-notify 패킷의 암호화를 위해 사용

* 한국전자통신연구원 정보보호연구본부 함영환(yhham@etri.re.kr)
** 한국전자통신연구원 정보보호연구본부 정병호(cbh@etri.re.kr)

본 논문에서는 라디우스 서버대신에 보다 확장성과 신뢰성이 뛰어난 프로토콜인 Diameter 프로토콜를 이용한 IAPP서버를 설계와 기존 시스템과의 연동방안에 대해서 제안하였다 [6].

II. Diameter IAPP서버의 구조

1. 시스템의 구성 요소

무선랜환경에서 ESS(Extended Service Set)은 BSS(Basic Service Set)의 집합이고, 무선랜 단말은 ESS안의 하나의 BSS에서 다른 BSS로 투명한 서비스를 받을 수 있도록 해야한다. ESS안의 액세스포인트는 같은 SSID(Service Set Identifier)를 사용하므로써 하나의 ESS를 구분한다. IAPP는 같은 ESS안에서 액세스포인트 사이에 무선랜 단말 정보의 안전한 핸드오프(handoff)를 제공하기 위하여 정의되었다. IAPP는 ESS안의 액세스포인트를 등록하기 위해서 라디우스를 사용할 수 있다. 여기에서는 Diameter 서버를 사용하는 것을 가정한다. ESS을 지원하는 IAPP의 기능은 세가지 수준으로 정의될 수 있다 .

1) 중앙적인 관리나 보안이 없는 기능지원

2) BSSID와 IP의 동적인 맵핑 기능 지원

3) IAPP메시지의 암호화와 인증(authentication)을 지원하는 기능 지원

위에 첫 번째 수준의 기능은 각각의 액세스 포인트 안에 ESS안의 모든 액세스 포인트에 대한 BSSID to IP 맵핑을 설정함으로써 지원할 수 있다. 이와 같은 메커니즘은 작은 규모의 ESS에서는 가능하지만 보다 큰 규모의 ESS에서는 불가능하다. 대부분의 서비스 제공자들은 적어도 두 번째나 세 번째 수준의 IAPP기능 지원이 필요하고 이것은 중앙 집중적인 Diameter 서버가 필요하다. 여기서 이와 같은 기능을 하는 Diameter 서버를 Diameter IAPP서버로 정의한다. Diameter IAPP서버, 무선랜단말 그리고 액세스포인트를 포함하는 전체적인 시스템의 구성은 아래의 그림 1과 같다. 그림에서 무선랜단말(Station)은 하나의 액세스포인트(Old AP1)로부터 다른 액세스포인트(New AP2)로 로밍하고 있음을 볼 수 있다.

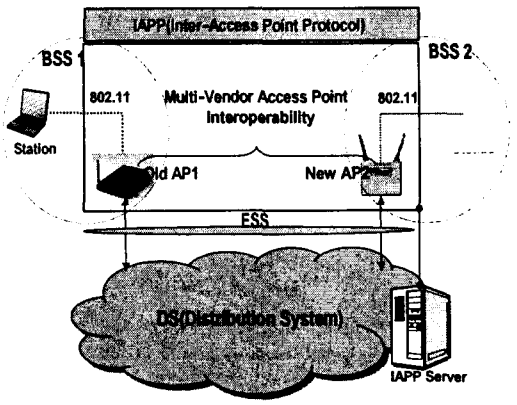

그림 1. 시스템의 구성요소

2. Diameter IAPP서버와의 연동

Diameter 서버를 IAPP서버로 이용하기 위해서는 액세스포인트에 Diameter 클라이언트를 포함하던지 아니면 중간에 Radius-to-Diameter TA(Translation Agent)를 두어야 한다. 여기에서는 기존의 액세스포인트를 위해 개발된 라디우스 클라이언트 모듈을 사용하고 기존 시스템과의 원활한 통합을 위해 중간에 TA를 두는 구조를 제안한다. 제안된 시스템의 구조는 다음과 같다.

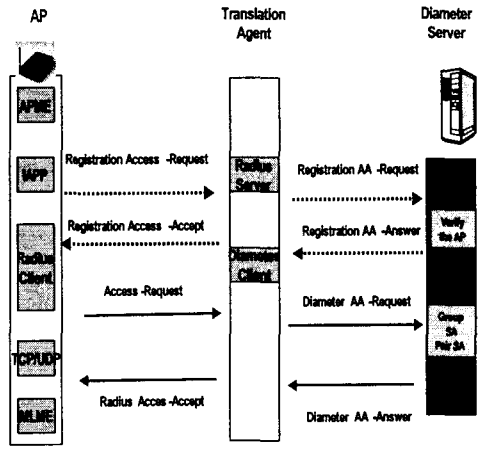

그림 2. Diameter IAPP서버와의 연동

위와 같은 라디우스 클라이언트- TA- Diameter 서버의 구조에서는 기본적으로 라디우스 프로토콜에서 Diameter 프로토콜로의 프로토콜 변환이 필요하다. 또한 TA는 라디우스 서버의 역할과 Diameter 클라이언트의 역할을 수행해야 한다. 라디우스 서버의 역할을 수행하기 위해서 TA에는 각각의 액세스 포인트(라디우스 클라이언트)를 위한 Shared Secret정보가 설정되어 있어야 한다. IAPP 서비스를 위해 라디우스에서는 access-request와 access-accept(access-reject) 메시지를 사용하는데 이에 부합하는 Diameter 어플리케이션으로 NASREQ어플리케이션을 이용했다. Diameter NASREQ어플리케이션은 라디우스에서 많은 개념을 도입했기 때문에 기본적인 메시지 구성이 비슷하고 라디우스의 attribute들은 대부분 NASREQ의 AVP에 매칭된다 [7].

표 1. 라디우스와 Diameter NASREQ 맵핑 테이블

RADIUS attribute	**Diameter NASREQ AVP**
User-Name	User-Name
User-Password	User-Password
NAS-IP-Address	NAS-IP-Address
Framed-IP-Address	Framed-IP-Address
Called-Station-ID	Called-Station-ID
Service-Type	Service-Type
NAS-Identifier	NAS-Identifier
NAS-Port-Type	NAS-Port-Type
Vendor Specific Attribute	Vendor AVP
Message-Authenticator	없음

라디우스의 registration access-request메시지는 Diameter의 AA-Request메시지로 TA에서 변환되고 User-Name(BSSID)과 User-Password(BSSID Secret)등과 같은 attribute도 Diameter 의 해당 AVP로 변환되어 Diameter IAPP서버로 전달된다. Diameter AA-Answer 메시지와 메시지안의 Vendor AVP(Group SA정보)도 반대의 과정을 거쳐 라디우스의 access-accept메시지로 변환되어 액세스포인트 안의 라디우스 클라이언트에게 전달된다. 라디우스의 access-request메시지는 Diameter IAPP서버에게 액세스 포인트사이의 보안채널 형성을 위한 Pair SA 정보를 요청하고 서버에서는 Vendor AVP에 각각의 SA정보를 registration시에 등록된 각각의 BSSID Secret로 암호화해서 New-BSSID-Security-Block과 Old- BSSID-Security-Block으로 만든 후 전달한다. 전달된 Security Block중 New-BSSID-Security-Block은 현재의 액세스포인트에서 복호화되어 저장되고, Old-BSSID-Security-Block은 IAPP보안 채널을 필요로 하는 이전의 액세스포인트에게 IAPP를 이용하여 전달된다.

2. Diameter IAPP 서버의 구조

로밍 무선랜 단말은 새로운 액세스 포인트에게 reassociation request보낼 때 이전의 액세스 포인트의 BSSID를 넣어서 보낸다. 이와 관련하여IAPP서버에는 각각의 BSSID에 관련된 아래와 같은 정보들을 유지해야 한다.

1) BSSID

2) BSSID Secret (160 bit 이상)

3) IP 주소 또는 도메인 이름

4) IAPP 통신을 보호하기 위한 Cipher suites(AP에서 지원)

위와 같은 정보들을 유지하고 AA-Request 메시지의 처리, AA-Answer 메시지의 생성, SA정보의 생성, Diameter Base 프로토콜 지원 등을 수행하기 위한 Diameter IAPP서버의 구조는 그림 3 과 같다.서버는 크게 Diameter Base Protocol 모듈, IAPPmain, SA관리모듈, AP인증 DB로 분류된다. Diameter Base Protocol 모듈은 Diameter Base Protocol에 정의된 프로토콜 동작을 수행하여 Diameter IAPP서버에서 필요로 하는 서비스를 제공한다. IAPPmain 모듈에서는

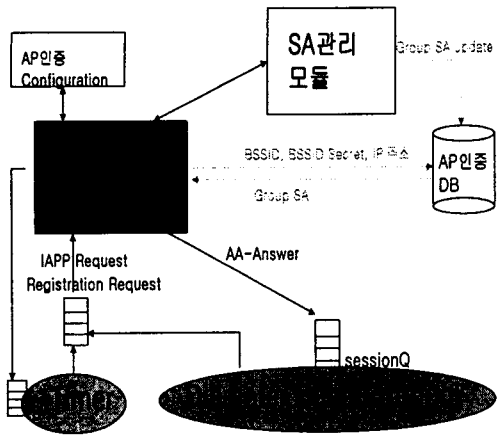

그림 3. Diameter IAPP서버의 구조

Base Protocol모듈에서 넘어오는 AA-Request메시지를 받아서 이것이 Registration request이면 SA관리모듈에 Group SA를 요청하고 일반 request이면 SA관리모듈에 Pair SA정보를 요청한다. 또한 생성된 SA정보를 포함하는AA-Answer 메시지를 만들어 보낸다. SA관리모듈에서는 요청된 Group SA정보의 생성 및 갱신, 그리고 Pair SA정보의 생성 등의 역할을 수행한다. AP인증 DB에는 BSSID별로 BSSID Secret, IP주소, Transform ID, Authentication ID등이 저장되고, SSID별로 Group SA정보가 저장된다. 이 밖에 Group SA의 update timeout시간을 지정하는 AP인증Configuration 모듈과 지정된 시간마다 timer event를 발생시키는 timer모듈이 있다.

III. Diameter IAPP서버의 동작

Diameter IAPP서버는 크게 3가지의 이벤트를 처리한다. 첫번째는 GroupSA timeout 이벤트로 Configuration 파일에 설정되어서 주기적으로 발생되는 이벤트이다. Timeout 이벤트가 발생하면 IAPPmain모듈은 SA관리모듈을 호출하여 Group SA를 갱신한다. 두번째는 Registration request 이벤트이다. IAPPmain모듈에서 AA-Request 메시지를 받으면 "Service-Type" AVP를 가지고 이것이 Registration Request인지 아닌지를 구별한다. Registration 이벤트가 발생하면 IAPPmain모듈은 메시지안의 BSSID Secret, IP주소, Nas-Identifier 등의 정보를 저장한다. 그 다음에 SA관리모듈을 호출하여 Group SA정보를 넘겨받은 후에 AA-Answer 메시지안에 넣어서 보낸다. 세번째는 IAPP request 이벤트이다. IAPPmain모듈에서 "Service-Type"이 IAPP Request인 AA-Request메시지를 받으면 역시 SA관리모듈을 호출하여 Pair SA정보를 넘겨받은 후에 Registration 이벤트시에 저장해 두었던 각각의 BSSID Secret을 읽어들인다. Pair SA정보는 Old-BSSID-Security-Block과 New-BSSID-Security-Block으로 만들어진 후에 각각의 BSSID Secret에 의하여 암호화되고 AA-Answer안에 담겨서 보내진다.

IV. 결론

무선랜 환경에서 무선랜 단말이 AP(Access Point) 사이를 로밍(Roaming)할 수 있게 하는 프로토콜로서 IAPP(InterAccess Point Protocol)이 있고 관련된 IEEE표준으로 802.11f가 있다. 이와 같은 802.11f를 지원하는 액세스포인트를 위해서는 IAPP서버의 역할을 수행하는 라디우스(RADIUS) 서버가 필요하다. 여기에서는 라디우스 대신 보다 진보된 프로토콜인 Diameter 를 사용한 IAPP서버를 제안하였다. 제안된 Diameter IAPP서버와 기존의 액세스포인트를 위해 개발된 라디우스 클라이언트 모듈과의 통합을 위해 중간에 TA를 두는 구조를 제안했다. TA는 라디우스 클라이언트 Diameter IAPP서버와의 연동을 위해 라디우스 서버의 역할과 Diameter 클라이언트의 역할을 동시에 수행함으로써 프로토콜을 변환해준다. Diameter IAPP서버는 NASREQ 어플리케이션을 이용함으로써 새로운 프로토콜을 정의하는 부담을 피할 수 있다. 제안된 Diameter IAPP서버를 통하여 보다 성능과 확장성이 뛰어나고 무선랜 서비스 사업자간의 연동이 원활한 IAPP 지원 시스템을 구축할 수 있다.

참 고 문 헌

[1] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", June 2001.

[2] IEEE 802.11F, "Recommended Practice for Multi-Vendor Access Point Interoper

ability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation", January 2003.

[3] W.Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[4] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP) ", RFC2284, March 1998.

[5] C.Rigney, "Remote Authentication Dial In User Service(RADIUS)" RFC 2865, June 2000.

[6] Pat R. Calhoun, Glen Zorn, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-11.txt, February, 2003.

[7] Pat R. Calhoun, John Loughney, "Diameter Base Protocol", draft-ietf-aaa-diameter-13, October, 2002.