무선랜단말 핸드오프지원 Diameter IAPP 서버에 대한 연구

함 영 환*, 정 병 호*, 정교일*

*한국전자통신연구원 정보보호연구본부

A Study On Diameter IAPP Server Supporting WirelessLAN Terminal Handoff

YoungHwan Ham*, ByungHo Chung*, Kyoil Chung*

*Information Security Research Division, ETRI

요 약

무선랜 환경에서 무선랜 단말이 AP(Access Point)사이를 로밍(Roaming)할 때 무선랜단말의 안전한 핸드오프를 위한 프로토콜로서 IAPP(InterAccess Point Protocol)가 있고 관련된 IEEE표준으로 802.11f가 있다. 무선랜단말의 안전한 핸드오프를 위해서는 IAPP를 통하여 기존에 접속되었던 AP에서 새로운 AP에게 무선랜단말의 인증 또는 과금관련 정보를 안전하게 전달하는 것이 필요하다. IEEE 802.11f에서는 무선랜단말의 핸드오프를 지원하는 액세스포인트를 인증하고 AP사이의 안전한 통신을 위한 정보를 제공하는 IAPP서버로 라디우스(RADIUS) 서버를 권고한다. 본 논문에서는 라디우스 서버의 한계를 극복하고 보다 확장성과 신뢰성이 뛰어난 서버를 위해 Diameter를 사용한 IAPP 서버의 구조와 동작에 대해서 설명한다.

Ⅰ. 서 론

무선랜 환경에서 무선랜 단말이 액세스포인트(Access Point)사이를 로밍할 수 있게 하는 프로토콜로서 IAPP가 있고 IAPP는 IEEE 802.11f에 정의되어 있다 [1] [2] IAPP는 AP안의 Management Entity가 AP안에서 일어나는 이벤트를 처리하기 위해 다른 AP와 통신할 때 사용되는 통신 프로토콜이다. IAPP서비스의 구성요소는 AP, 스테이션, 그리고 연결된 DS(Distribution System)이다. 또한 IAPP에서는 IP주소의 맵핑과 키의 분배를 위해서 라디우스 서버를 사용한다 [3] [4] [5]. IAPP를 위한 라디우스 서버의 사용예를 정리하면 다음과 같다.

1) AP의 인증 : AP가 IAPP-INITIATE서비스에 ESS(Extended Service Set)에 속하는지 인증(verify), IAPP-MOVE서비스시에 old AP와 new AP가 같은 ESS에 속하는지 인증

2) BSSID와 IP주소의 맵핑 : IAPP-MOVE서비스에 사용, 새로운 AP(new AP)에게 기존의 AP(old AP)의 주소를 알려줌

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-MOVE서비스시에 pair SA를 생성하여 분배함으로써 AP사이에 보안 채널(secure channel)을 생성하여 MOVE-notify 패킷의 암호화를 위해 사용

본 논문에서는 라디우스 서버대신에 보다 확장성과 신뢰성이 뛰어난 프로토콜인 Diameter 프로토콜를 이용한 IAPP서버의 구조와 동작에 대해서 제안하였다[6].

Ⅱ. Diameter IAPP서버의 구조

1. RADIUS와 Diameter 프로토콜

RADIUS프로토콜은 다이얼업PPP/IP그리고 모바일 IP접속등을 위한 AAA(authentication, authorization, accounting)을 제공하기 위한 프로토콜로써 성공적으로 쓰여왔다. 그러나 RADIUS의 근본적인 장점으로 인해 기능이 점증하는 네트워크장비들을 위한 AAA 서비스의 요구조건들을 충족하기에는 RADIUS프로토콜에는 한계가 있다. 이와같은 한계를 극복하기 위해 제안된 것이 Diameter프로토콜이다. Diameter프로토콜설계시에 제기된 RADIUS의 단점은 다음과 같다.

- Attribute크기의 제한 : attribute크기가 255개로 제한되고 전체 attribute갯수도 255개로 제한됨
- Concurrent pending메시지의 제한 : RADIUS 의 "Identifier"필드가 1 바이트이므로 동시에 pending되어 있는 메시지는 255개를 초과할 수 없다.
- Flow Control이 불가능 : RADIUS는 UDP를 사용함으로 양단간의 flow control이 불가능함
- Server Failure detection 제한 : 서버가 RADIUS요청에 응답이 없을 경우 네트워크 문제인지 서버의 문제인지 알기 어려움
- Silent Packet Discarding : RADIUS서버는 요청메시지에 에러가 있는 경우 조용히 패킷을 폐기함으로써 클라이언트에서 요청을 계속 반복할 수 있는 단점이 있다.

Diameter프로토콜에서는 위에서 언급된 문제들을 해결또는 보완하였고 그 외에도 unsolicited server message 지원, end-to-end security, vendor-specific command, IPSec과 TLS지원, 서비스사업자간의 로밍지원 등 다양한 기능을 지원할 수 있도록 설계되었다.

2. 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 대한BSSID 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[7]. 여기서 이와 같은 기능을 하는 Diameter 서버를 Diameter IAPP서버로 정의한다. Diameter IAPP서버, 무선랜단말 그리고 액세스포인트 등으로 전체적인 시스템이 구성된다. 무선랜단말(Station)은 하나의 액세스포인트(Old AP)로부터 다른 액세스포인트(New AP)로 로밍하고 있음을 볼 수 있고 이 때 무선랜단말의 핸드오프를 위해서 Old AP와 new AP간의 안전한 IAPP통신이 필요하고 이를 위한 정보들(IP주소, 키)은 IAPP서버가 라디우스와 Diameter 프로토콜을 이용하여 AP에게 제공한다

3. Diameter IAPP서버와의 연동

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.

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.

4. 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 1과 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.

아래의 그림과 같이 Base Protocol과 어플리케이션을 다른 쓰레드(Thread)로 구분하여 기본적인 프로토콜 기능(AVP전달, Peer 연결, Capability협상, 세션과 과금처리, 사용자인증정보전송 등)과 프로토콜 메시지를 Base Protocol에서 처리하고, 어플리케이션 메시지는 IAPPmain 모듈 쓰레드와 AP등록모듈쓰레드에서 처리하게 함으로써 서버의 부하를 각각의 쓰레드 분산시킬 수 있다. 또한 IAPP메시지의 경우 각 메시지들간에 독립적인 메시지이고 큐를 통해 다른 쓰레드에게 전달되고 큐는 여러 개의 쓰레드에서 접근이

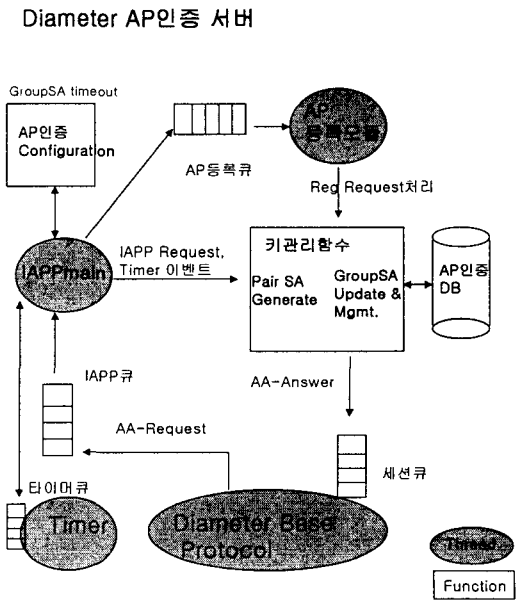

그림 1. Diameter IAPP서버의 구조

Ⅲ. Diameter IAPP서버의 동작

가능한 구조이므로, 만약에 특정 쓰레드의 부하가 커지는 경우 특정 쓰레드의 개수를 증가시킴으로써 서버 전체의 성능을 향상시킬 수 있는 구조를 채택하였으므로 안정성과 확장성이 뛰어나다.

Diameter Base Protocol모듈, Timer모듈, IAPPmain모듈, AP등록모듈과AP인증DB로 이루어진 Diameter IAPP서버에서는 클라이언트로부터 오는 AA-Request메시지를 처리하고 주기적인 GroupSA갱신을 위하여 유기적인 상호작용을 통하여 동작한다. 여기에서는 이와 같은 Diameter IAPP서버의 동작과 메시지 처리방법에 대하여 설명한다. Diameter IAPP서버는 크게 3가지의 이벤트를 처리한다. 첫번째는 GroupSA timeout 이벤트로 Configuration 파일에 설정되어서 Timer모듈에서 주기적으로 발생되는 이벤트이다. IAPPmain모듈은 시작시에 Configuration파일의 Timeout시간을 타이머큐를 통해서 타이머에 셋팅하면, 타이머는 그 시간에 맞추어 Timeout이벤트를 발생시키고 이를 응용큐를 통해서 IAPPmain모듈에 전달한다. Timeout 이벤트가 발생하면 IAPPmain모듈은 키관리함수를 호출하여 Group SA를 갱신하고 갱신된 GroupSA는 다시 AP인증DB에 저장된다.

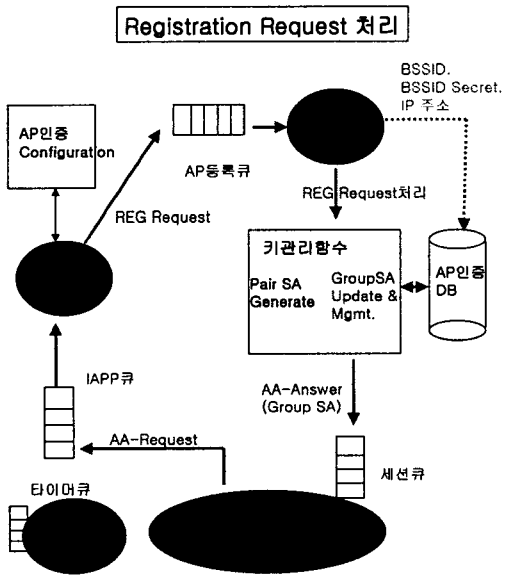

그림 2. IAPP서버의 Registration Request처리

두번째는Registration request 이벤트이다. 그림 2는 Registration request이벤트의 처리과정을 보여준다. IAPP서버에 AA-Request메시지가 도착하면 Base Protocol은 도착한 메시지를 응용큐를 통하여 IAPPmain모듈에 전달한다. IAPPmain모듈에서 AA-Request 메시지를 받으면 "Service-Type" AVP를 가지고 이것이 Registration Request인지 아닌지를 구별한다. 메시지가 Registration Request인 경우IAPPmain모듈은 메시지를 AP등록큐를 통하여 AP등록모듈에게 전달하고 AP등록모듈은 BSSID Secret, IP주소, Nas-Identifier 등의 정보를 AP인증DB에 저장한다. 그 다음에 키관리함수를 호출하여 Group SA정보(주기적으로 갱신되어 있는 GroupSA)를 AP인증DB로부터 읽어들이고 이를 포함하는 AA-Answer 메시지를 생성하여 세션큐에 넣어서 Base Protocol로 보낸다. Base Protocol은 AA-Request를 보낸 TA에게 AA-Answer메시지를 보낸다.

세번째는 IAPP request이벤트이다. 그림 3은 IAPP request이벤트의 처리과정을 보여준다. IAPP서버에 AA-Request메시지가 도착하면 Base Protocol은 도착한 메시지를 응용큐를 통하여 IAPPmain모듈에 전달한다. IAPPmain모듈에서 "Service-Type"이 IAPP Request인 AA-Request메시지를 받으면 키관리함수를 호출하여 Pair SA정보를 생성하고 Registration 이벤트시에 저장해 두었던 각각(Pair AP)의 BSSID Secret과 IP주소 정보를 읽어들인다. Pair SA정보는 IP주소정보와 함께 Old-BSSID-Security-Block과 New-BSSID- Security-Block으로 만들어진 후에 각각의 BSSID Secret에 의하여 암호화되고 AA-Answer안에 담겨서 세션큐를 통하여 Base Protocol로 보내진다. Base Protocol은 AA-Answer메시지를 AA-Request를 보낸 TA에게 보낸다.

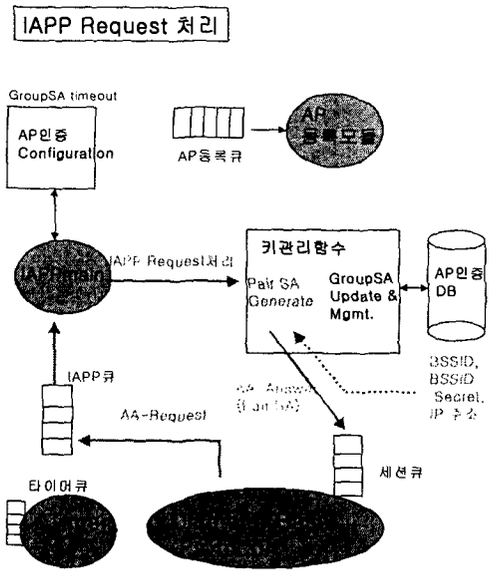

그림 3. IAPP서버의 IAPP Request처리

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 Interoperability 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", RFC3588, September, 2003.