무선랜 단말의 안전한 핸드오프를 위한 Diameter IAPP서버의 설계

정회원 함 영 환*, 정 병 호**, 정 교 일***, 서 창 호****

The Design of IAPP Server for Secure Handoff of wireless LAN Terminal

Young-Hwan Ham*, Byung-Ho Chung**, Kyo-Il Chung***, Chang-Ho Seo**** *Regular Members*

요 약

최근에 초고속 무선인터넷 서비스로 각광받고 있는 무선랜 환경에서 무선랜 단말이 액세스포인트사이를 로밍할 때 무선랜단말의 안전한 핸드오프를 위한 프로토콜로서 IAPP가 있고 관련된 IEEE표준으로 802.11f가 있다. 무선랜단말의 안전한 핸드오프를 위해서는 IAPP를 통하여 기존에 접속되었던 액세스포인트에서 새로운 액세스포인트에게 무선랜단말의 인증 또는 과금관련정보를 안전하게 전달하는 것이 필요하다. IEEE 802.11f에서는 무선랜단말의 핸드오프를 지원하는 액세스포인트를 인증하고 액세스포인트사이의 안전한 통신을 위한 정보를 제공하는 IAPP 서버로 라디우스 서버를 권고한다. 본 논문에서는 라디우스 서버의 한계를 극복하고 보다 확장성과 신뢰성이 뛰어난 서버를 위해 Diameter를 사용한 IAPP서버를 설계하고 서버의 동작과 기존 시스템과의 연동방안에 대해서 설명한다.

Key Words : IAPP, Secure Handoff, Access Point, Diameter

ABSTRACT

As the need for stable and high speed wireless Internet service grows, the wireless LAN service provider hurries to preempt wireless LAN service market. IAPP(InterAccess Point protocol) is defined to be able to provide a secure handoff mechanism of wireless LAN terminal information between AP(Access Point)s, and the related IEEE standard is IEEE 802.11f. For the secure handoff of wireless LAN terminal, it is necessary to transfer terminal's authentication & accounting information securely from old AP to new AP. IEEE 802.11f recommends RADIUS server as IAPP server which authenticates AP and provides information for secure channel between APs. This paper proposes IAPP server using Diameter protocol to overcome the limit of RADIUS server, and describes about the interaction between server components and integration method with the current IAPP client system.

* ETRI 정보보호연구본부(yhham@etri.re.kr), ** ETRI 정보보호연구본부(cbh@etri.re.kr), ***ETRI 정보보호연구본부(kyoil@etri.re.kr), ****공주대학교 응용수학과(chseo@kongju.ac.kr)

논문번호 : 030409-0917, 접수일자 : 2003년 9월 18일

Ⅰ. 서 론

공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 무선랜 기술은 현재 급속도로 진화중인 초고속 무선인터넷, 차세대 유무선통합망, 스마트홈, 유비쿼터스망을 위한 필수적인 무선 액세스 기술로 인식되고 있다.

1999년에 제정된 무선랜은 WEP(Wired Equivalent Privacy)을 이용하여 유선랜 수준의 보안 서비스 제공을 목표로 하였으나 최근 보안상의 취약점이 드러나면서 IEEE 802.11i TG(Technical Group)을 중심으로 사용자가 액세스포인트(Access Point)를 핸드오프하는 환경에서도 견고한 실시간 보안 서비스를 제공할 수 있도록 표준 규격을 개발하고 있다. 무선랜 접속 구간에서의 보안 문제는 첫째, 비인가자의 접속차단 둘째, 무선 구간에서 불법도청, 암호화, 데이터 위변조 방지를 위한 프라이버시 강화로 분류된다. IEEE802.1x기반의 접속제어 기능은 인증된 사용자에게만 접속을 허용하는 중요한 수단을 제공하였지만, 무선 구간에서 사용자의 프라이버시 강화에 필요한 키 분배 기능은 고려하지 않았다. 이는 사용자가 인증 과정에서 동의한 키를 이용한 보안서비스를 제공받지 못함을 의미한다[1]. 따라서 이러한 문제 해결을 위하여 결성된 IEEE 802.1aa TG에서는 802.1x의 인증, 접속제어, 키 관리 기능 중에서 접속제어와 80211i키관리 기능 간의 인터페이스를 명확히 정의하고, 사용자 인증과 키 분배가 성공적으로 종료된 경우에 한하여 접속을 허용하도록 함으로써 비인가자의 접속 차단과 프라이버시 강화를 위한 키 관리 기능을 결합하는 방향으로 규격을 수정하고 있다[2]. IEEE 802.11i TG는 2002년 3월 무선랜의 프라이버시 강화를 위한 방안으로 RSN(Robust Security Network)보안 구조를 채택하여 협상을 통한 세션관리, 계층적 키관리를 통한 4단계 키교환, 새로운 프라이버시 메커니즘, 선인증(Pre-authentication) 메커니즘, 그리고 IBSS(Independent Basic Service Set) 보안 규격을 제정하고 있다[3]. 현재 무선랜에서의 핸드오프 보안을 지원하는 선인증 문제와 Ad-Hoc보안을 지원하는 IBSS보안 문제를 제외한 나머지 규격은 완성 단계에 도달한 것으로 보인다. 802.11i TG는 단기적인 프라이버시 메커니즘으로 TKIP(Temporary Key Integrity Protocol)을 그리고 중장기적인 메커니즘으로 CCMP (Counter-mode/CBC-MAC Protocol)를 제안하고 있다. CCMP는 고속으로 견고한 무선 프라이버시를 제공하는 장점이 있지만 모뎀 칩셋이 바뀌어야 하므로 하드웨어적인 호환성의 문제가 있는 반면, TKIP은 기존의 하드웨어에 소프트웨어적인 업그레이드를 통하여 보안기능을 강화할 수 있는 장점이 있다.

위와 같은 접속보안 강화방안과 함께 무선랜환경에서의 이동보안을 강화하기 위한 방안으로 802.11f TG에서는 무선랜 단말이 액세스포인트사이를 로밍할 때 무선랜단말에 관련한 정보를 새로운 액세스포인트에게 전달해 주기 위한 프로토콜로서 IAPP(Inter-Access Point Protocol)를 제정하고 있다[4].

IAPP는 AP안에 있는 관리객체(Management Entity)가 AP안에서 일어나는 이벤트를 처리하기 위해 다른 AP와 통신할 때 사용되는 통신 프로토콜이다. IAPP서비스의 구성요소는 AP, 스테이션(무선랜단말), 그리고 연결된 DS(Distribution System)이다. 또한 IAPP에서는 IP주소의 맵핑과 키의 분배를 위해서 라디우스 서버를 사용한다[5][6][7]. 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-MOVE 서비스시에 pair SA를 생성하여 분배함으로써 AP사이에 보안 채널(secure channel)을 생성하여 MOVE-notify 패킷의 암호화를 위해 사용.

IAPP를 위한 라디우스 서버의 동작을 살펴보면 아래의 그림 1과 같다. 처음에 IAPP를 위해 AP는 IAPP서버에 유효한 멤버로 등록되어야 한다(IAPP-INITIATE서비스). AP는 먼저 라디우스 서버에게 Registration Access-Request패킷을 전송한다. 이 패킷에는 BSSID(Basic Serivice Set Identifier : AP의 MAC주소)와 BSSID secret(최소 160bit의 비밀값)를 포함한다. 라디우스 서버가 이 패킷을 수신하면 서버는 AP가 등록되어 있는지 검증한 후에 패킷안의

BSSID Secret과 IP주소를 저장하고 Group SA를 포함하는 Registration Access-Accept패킷으로 응답한다.

두번째로 AP사이에서 무선랜단말의 로밍이 일어났을 때 (IAPP-MOVE서비스) 즉 단말이 old AP로부터 new AP로 로밍한다고 할 때 new AP는 old AP를 인증하고 둘 사이의 보안채널을 위한 Pair SA를 요청하기 위해 라디우스 서버에 Access-Request 패킷을 보낸다. 라디우스 서버는 new AP와 old AP를 인증하고 요청한 Pair SA를 생성(old AP의 IP주소도 포함)하여 AP등록(IAPP-INITIATE서비스)시에 저장되었던 BSSID secret정보를 이용하여 Pair SA(New-BSSID-Security-Block, Old-BSSID-Security-Block에 각각 포함됨) 암호화한 후 Access-Accept패킷에 넣어 보낸다. Pair SA를 수신한 new AP는 old AP에게 Old-BSSID- Security- Block을 보냄으로써 두개의 AP는 보안채널을 위한 키를 공유하게 된다[8].

본 논문에서는 IEEE 802.11f에 권고되어 있는 라디우스 서버대신에 보다 확장성과 신뢰성이 뛰어난 프로토콜인 Diameter 프로토콜를 이용한 IAPP서버의 설계와 기존 시스템과의 연동방안에 대해서 제안하였다[9][10].

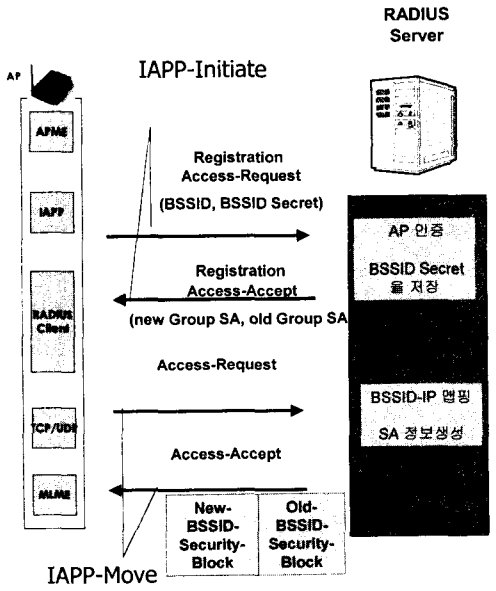


그림 1. IAPP를 위한 라디우스 서버의 동작

II. Diameter IAPP서버의 구조

1. 라디우스와 Diameter 프로토콜 비교

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

- Attribute크기의 제한 : attribute크기가 255개로 제한되고 전체 attribute갯수도 255개로 제한됨
- Concurrent pending메시지의 제한 : 라디우스의 "Identifier"필드가 1 바이트이므로 동시에 pending되어 있는 메시지는 255개를 초과할 수 없다.
- Flow Control이 불가능 : 라디우스는 UDP를 사용함으로 양단간의 flow control이 불가능함
- Server Failure detection 제한 : 서버가 라디우스 요청메시지에 응답이 없을 경우 네트워크 문제인지 서버의 문제인지 알기 어려움
- Silent Packet Discarding : 라디우스서버는 요청메시지에 에러가 있는 경우 조용히 패킷을 폐기함으로써 클라이언트에서 요청을 계속 반복할 수 있는 단점이 있다.
- 불충분한 서버 Fail-Over : 대부분의 액세스포인트에서는 여러개의 라디우스서버를 지정할 수 있으나 정상적인 서버를 찾기 위한 메커니즘이 없다.
- Replay attck : 라디우스 프로토콜은 재전송을 방지하기 위한 방법을 제공하지 않으므로 DoS (Denial of Service)공격에 취약하다
- Hop-by-hop 보안 : 라디우스 프로토콜은 액세스포인트와 AAA서버사이의 보안만을 제공하고 중간에 proxy server가 추가되는 경우의 end-to-end보안은 제공하지 않는다.
- Vendor-specific 명령을 지원하지 않음 : 라디우스는 vendor-specific attribute는 지원하나 vendor-specific 명령을 지원하지 않는다.
- 의무적인 Shared Secret 사용 : 라디우스 프로토

콜은 하위계층에서 IPSec과 같은 보안기능을 제공하더라고 반드시 Shared Secret을 사용하여 동작하도록 되어있다.

Diameter프로토콜에서는 위에서 언급된 문제들을 해결 또는 보완하기 위해서 설계되었다. Diameter는 신뢰성있는 전송계층을 위해 TCP또는 SCTP (Stream Control Trans- mission Protocol)을 사용한다. Diameter에서는 특정 도메인에 대해 최소 2개 이상의 연결을 기본적으로 설정하고 상태머신을 통해 연결상태를 감시하다가 실패가 발생할 경우 보조 연결을 통해 기본 연결로 전송된 메시지들을 재전송한다. 또한 전송계층의 보안을 위해서 IPSec 또는 TLS를 이용한다.

응용서비스 측면에서는 AVP의 코드크기를 32비트로 정의해서 기존의 라디우스의 한계를 극복했다. 라디우스에서는 뚜렷한 정의가 없던 에이전트의 명확한 정의를 통해 망 구성의 효율성을 높일 수 있고 서비스사업자간의 로밍을 지원하고 다양한 네트워크에서의 인증 및 과금을 하나의 Diameter서버로 해결할 수 있다. 그 외에도 서로 지원가능한 서비스를 협상할 수 있는 capability negotiation, 프로토콜 에러, 어플리케이션에러와 같이 다양하게 분류된 에러를 처리할 수 있는 error handling, DNS를 이용한 동적인 peer discovery의 지원, Peer-to-peer 모델의 서버방식에 의한 server-initiated 메시지 지원 등 더욱 다양하고 효과적인 서비스를 제공해 줄 수 있다. 이와같은 Diameter 프로토콜을 이용한 IAPP서버를 설계함으로써 확장성과 신뢰성이 뛰어난 서버시스템을 구축할 수 있다.

2. 시스템의 구성요소

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 사용함으로써 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(authen- tication)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 2와 같다. 그림에서 무선랜단말(Station)은 하나의 액세스포인트(Old AP1)로부터 다른 액세스포인트(New AP2)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.

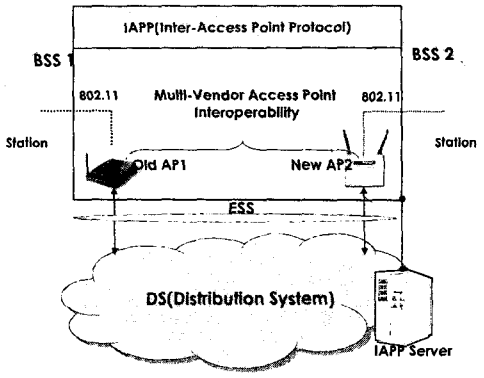


그림 2. 시스템의 구성요소

3. Diameter IAPP서버와의 연동

Diameter 서버를 IAPP서버로 이용하기 위해서는 액세스포인트에 Diameter 클라이언트

를 포함하던지 아니면 라디우스 클라이언트를 사용하면서 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 그림 3과 같다.

아래의 그림 3과 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 Diameter어플리케이션으로 NASREQ어플리케이션을 이용했다. Diameter NASREQ어플리케이션은 라디우스에서 많은 개념을 도입했기 때문에 기본적인 메시지 구성이 비슷하고 라디우스의 attribute들은 대부분 NASREQ의 AVP에 매칭된다[11].

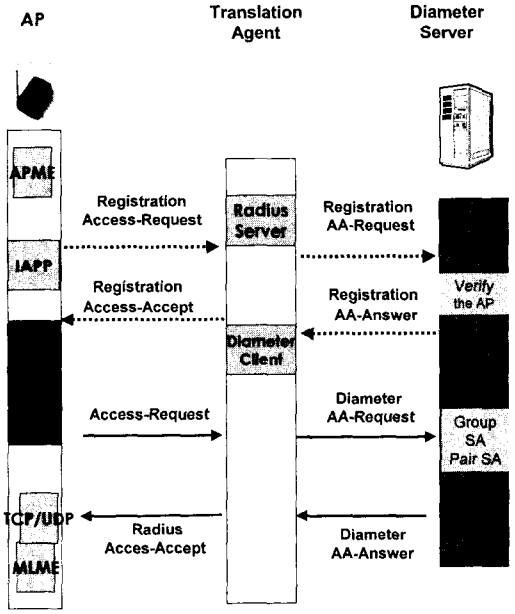


그림 3. Diameter IAPP서버와의 연동

표 1. 라디우스와 Diameter NASREQ 맵핑 테이블

라디우스 attribute	Diameter NASREQ AVP	실제값
User-Name	User-Name	BSSID
User-Password	User-Password	BSSID Secret
NAS-IP-Address	NAS-IP-Address	AP의 IP주소
Framed-IP-Addr	Framed-IP-Addr	Old AP의 IP주소
Called-Sta-ID	Called-Sta-ID	Old BSSID
Service-Type	Service-Type	메시지 구별
Nas-Identifier	Nas-Identifier	AP의 NAS-ID
NAS-Port-Type	NAS-Port-Type	IAPP에 할당된 값
Vendor Specific attribute	Vendor Specific attribute	키관련 정보
Message Authenticator	없음	메시지 인증값

라디우스의 registration access-request메시지는 Diameter의 AA-Request메시지로 TA에서 변환되고 User-Name(BSSID)과 User-Password(BSSID Secret)등과 같은 attribute는 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 SA정보를 요청하고 서버에서는 Vendor AVP에 Pair SA정보를 registration시에 등록된 각각의 BSSID Secret로 암호화해서 New-BSSID-Security-Block과 Old-BSSID-Security-Block 으로 만든 후 전달한다. 전달된 Security Block중 New-BSSID-Security-Block은 현재의 액세스포인트(new AP)에서 복호화되어 저장되고, Old-BSSID-Security-Block은 IAPP보안 채널을 필요로 하는 이전의 액세스포인트(old AP)에게 IAPP를 이용하여 전달된다.

4. Diameter IAPP메시지의 구성

Diameter IAPP메시지는 Diameter 헤더와 필요한 AVP로 구성되어지고, 필요한 AVP는 표1에서와 같이 라디우스와 Diameter NASREQ맵핑 테이블에서 보여지듯이 라디우스 attribute로부터 만들어지는 Diameter AVP가 있고 Diameter 프로토콜을 수행

하기 위해서 필수적인 AVP가 있다. Diameter 프로토콜 수행을 위한 필수 AVP는 AA-Request의 경우 TA에서 생성하여야 하고, AA-Answer의 경우 IAPP서버에서 생성되어야 한다. Diameter IAPP메시지는 크게 AA- Request메시지와 AA-Answer메시지가 있고 각각에 대해서 필요한 AVP를 정리하면 아래의 표2, 표3과 같다.

표 2. Diameter AA-Request AVP

AVP 종류	AVP이름
AVP from 라디우스 attrbiute	User-Name User-Password NAS-IP-Address Framed-IP-Address Called-Station-ID NAS-Port-Type NAS-Identifier Service-Type Vendor-AVP
필수 AVP(TA생성)	Origin-Host Origin-Realm Destination-Realm Auth-Request-Type Auth-Session-State Proxy-Info

표 3. Diameter AA-Answer AVP

AVP종류	AVP이름
AVP from 라디우스 attribute	User-Name User-Password NAS-IP-Address NAS-Identifier Service-Type Session-Timeout Vendor AVP
필수 AVP(IAPP서버생성)	Session-Id Auth-Application-Id Origin-Host Origin-Realm Auth-Request-Type Auth-Session-State Proxy-Info

필수 AVP의 의미는 다음과 같다.

- Session-Id : 특정한 Diameter 세션을 식별하기 위한 Identifier AVP
- Auth-Application-Id : 지정된 어플리케이션 ID(NASREQ : 1)가 들어가며 어플리케이션 인증을 지원하는지를 알리는 AVP
- Origin-Host : Diameter 메시지를 보낸 호스트를 식별하는 AVP
- Origin-Realm : Diameter 메시지를 보낸 도메인을 식별하는 AVP
- Destination-Realm : Diameter 메시지가 라우팅되는 목적지 식별 AVP
- Auth-Request-Type : Authentication(인증)인지 Authorization(권한부여)인지 식별 AVP
- Auth-Session-State : 특정 세션을 위해 상태가 유지(maintained)되는지의 여부 식별 AVP
- Proxy-Info : TA를 식별하는 AVP로 라디우스 Identifier, 라디우스 패킷의 source IP 와 port등도 저장될 수 있음.

5. Diameter IAPP 서버의 구조

로밍 무선랜 단말은 새로운 액세스포인트(new AP)에게 reassociation request보낼 때 이전의 액세스포인트(old AP)의 BSSID를 넣어서 보낸다. 이와 관련하여 IAPP서버에는 각각의 BSSID에 관련된 아래와 같은 정보들을 유지해야 한다.

1) BSSID
: AP를 식별하는 MAC 주소
2) BSSID Secret
: 160 bit 이상의 AP비밀값으로 Pair SA암호화에 사용
3) IP 주소 또는 도메인 이름
: AP의 주소
4) IAPP 통신을 보호하기 위한 Cipher suites(AP에서 지원하는 암호,인증방식)

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 4와 같다.서버는 크게 Diameter Base Protocol 모듈, IAPPmain모듈, AP등록모듈, AP인증 DB로 분류된다. Diameter Base Protocol 모듈은 Diameter Base Protocol에 정의된 프로토콜 동작을 수행하여 Diameter IAPP서버에서 필

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

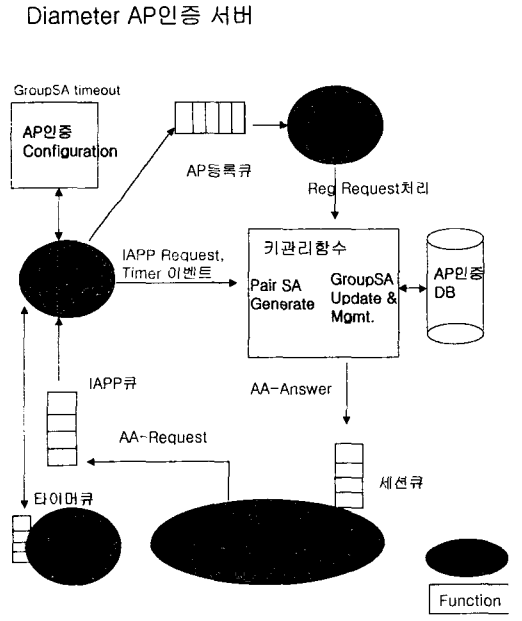


그림 4. Diameter IAPP서버의 구조

Base Protocol모듈에서 넘어오는 AA-Request메시지는 IAPP큐를 통해서 IAPPmain모듈에서 받아서 이것이 Registration request이면 AP등록큐를 통해서 AP등록모듈에 Group SA를 요청하고 일반 Request이면 IAPPmain모듈에서 직접 처리한다. IAPPmain모듈이나 AP등록모듈에서는 각각 생성된 SA정보를 포함하는AA-Answer 메시지를 만들어 보낸다. IAPPmain모듈이나 AP등록모듈은 요청된 Group SA정보의 생성 및 갱신, 그리고 Pair SA정보의 생성 등의 역할을 수행하기 위해서 키관리함수(PairSA Generate, GroupSA Update & Mgmt)를 호출한다. AP인증DB에는 BSSID별로 BSSID Secret, IP주소, Transform ID(암호화방식 식별ID), Authentication ID(메시지해쉬인증방식 식별ID)등이 저장되고, SSID별로 Group SA정보가 저장된다. AP인증 DB는 빠른 저장과 검색이 가능하여 서버의 성능을 향상시킬 수 있도록 메모리데이터베이스(Memory DB)를 사용하였다. 이 밖에 Group SA의 update timeout시간을 지정하는 AP인증 Configuration 모듈과 지정된 시간마다 timer event를 발생시키는 timer모듈이 있다.

모듈간 인터페이스를 위하여 큐는 매우 중요한 역할을 한다. 큐는 기본적으로 크기가 고정된 배열 형태로 구성되고 큐안에 메시지와 이벤트를 동시에 포함할 수 있는 자료구조를 가진다. 큐에 대한 오퍼레이션은 큐입력(input_q()) 함수와 큐출력(del_queue())함수를 통하여만 접근이 가능하고 함수내부는 mutex lock을 사용하여 큐에 대한 임계영역을 보호한다. 그림 5는 큐의 자료구조에 대한 그림이다.

•이벤트 및 메시지 큐(NASREQ Queue) 의 자료구조

```
enum {
    ...
    DIAMETER_IAPP_REQEUST,    // AA-Request 또는 AA-Answer
    DIAMETER_IAPP_ANSWER,     // AA-Request 또는 AA-Answer
    DIAMETER_IAPP_TIMEOUT,    // GroupSA Timeout
    ...
} eventType;

typedef struct _QUEUE_DATA{
    eventType etype;              // 위에서 정의된 Event 종류
    void * msg;                   // 실제 메시지 포인터
    void * etc;                   // 세션 ID 등을 넘겨줄 경우
} queueData;

typedef struct _EVENT_Q {
        int front;
        int rear;
        queueData data[MAX_Q];
} EVENT_Q;

EVENT_Q NASREQ_Queue;
```

•이벤트 및 메시지 큐(NASREQ Queue) 입출력함수 Prototype

```
queueReturnCode input_q(EVENT_Q * queue, queueData data, ...);
queueReturnCode del_queue(EVENT_Q * queue, queueData *data);
```

그림 5. 큐의 자료구조 및 Prototype

Ⅲ. Diameter IAPP서버의 동작

Diameter Base Protocol모듈, Timer모듈, IAPPmain모듈, AP등록모듈과 AP인증DB로 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.

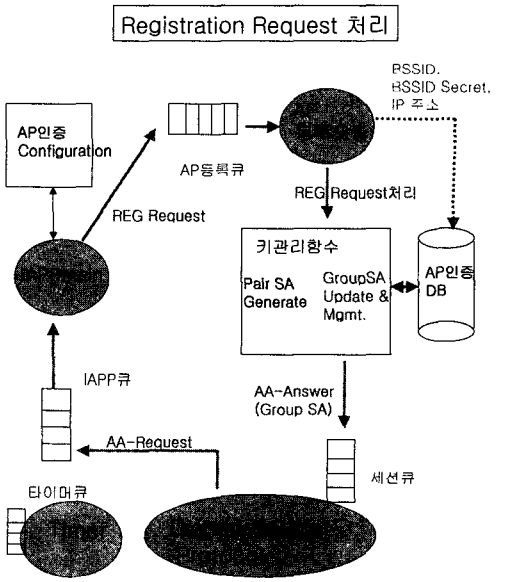


그림 6. IAPP서버의 Registration Request처리

두번째는 Registration request 이벤트이다. 그림 6은 Registration request이벤트의 처리과정을 보여준다. IAPP서버에 AA-Request메시지가 도착하면 Base Protocol은 도착한 메시지를 응용큐를 통하여 IAPPmain 모듈에 전달한다. IAPPmain모듈에서 AA-Request 메시지를 받으면 "Service-Type" AVP를 가지고 이것이 Registration Request인지 아닌지를 구별한다. 메시지가 Registration Request인 경우 IAPPmain모듈은 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 7은 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 Regis- tration 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.

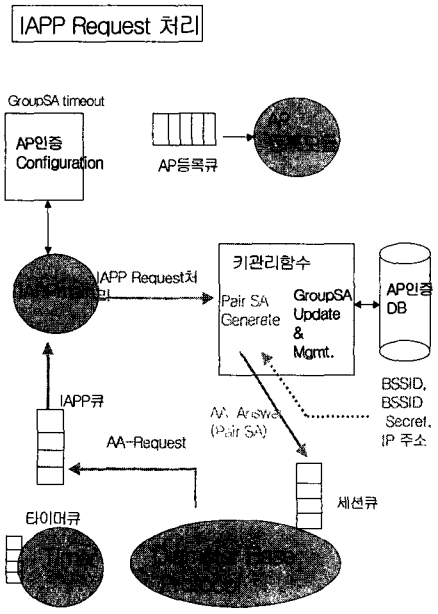


그림 7. IAPP서버의 IAPP Request처리

Ⅳ. 결 론

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 IAPP 서버의 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 클라이언트와 Diameter IAPP 서버와의 연동을 위해 라디우스 서버의 역할과 Diameter 클라이언트의 역할을 동시에 수행하며 프로토콜을 변환해줌으로써 기존 시스템과도 용이하게 통합구축될 수 있도록 한다. 제안된 IAPP서버 시스템의 구조는 각각의 모듈을 쓰레드로 하고 쓰레드 간의 인터페이스를 위하여 큐를 두는 구조이므로 쓰레드의 개수를 증가시킴으로써 서버 전체의 성능을 향상시킬 수 있는 구조를 채택하였으므로 서버의 부하를 분산시킬 수 있고 안정성과 확장성이 뛰어나다

Diameter IAPP서버는 NASREQ 어플리케이션을 이용함으로써 새로운 프로토콜을 정의하는 부담을 피할 수 있고 기존의 다른 Diameter 어플리케이션인 무선랜단말을 위한 사용자인증서버어플리케이션 및 과금서버 어플리케이션과도 비교적 쉽게 통합될 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 802.1aa/D5, "Draft Standard for Local and Metropolitan Area Networks - Port Based Network Access Control - Amendment 1, February 2003.

[3] IEEE 802.11i/D7, "Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11 Medium Access Control (MAC) - Security Enhancements" , October 2003.

[4] IEEE 802.11F/D5, "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.

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

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

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

[8] 박미애, 김용희, 이옥연, "AP사이의 상호 운영에 관한 연구", 한국정보보호학회하계학술대회, pp.235-240, 2003.

[9] 이진우, 김관연, 박세현, "공중 무선랜의 이동환경을 위한 Diameter 기반 선불 과금모델 연구", 한국정보보호학회하계학술대회, pp.241-244, 2003.

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

[11] Pat R. Calhoun, John Loughney, "Diameter Base Protocol", RFC3588, September, 2003.

함 영 환(Young-Hwan Ham) 정회원

1994년 2월 : 성균관대학교 컴퓨터공학과 졸업
1996년 2월 : 성균관대학교 컴퓨터공학과 석사
1995년 12월 ~ 1999년 10월 한국전자통신연구원 슈퍼컴퓨터 센터 연구원
2000년 6월 ~ 2001년 10월 : (주) 이니텍 연구원
2001년 12월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 연구원

<주관심분야>네트웍 보안 프로토콜, 무선인터넷 보안

정 병 호(Byung-Ho Chung) 정회원

1988년 2월 : 전남대학교 전산통계학과졸업
2000년 2월 : 충남대학교 컴퓨터 과학과 석사
2000년 3월 ~ 현재: 충남대학교 컴퓨터 과학과 박사수료
1998년 2월 ~ 2000년 6월 : 국방과학연구소 선임연구원
2000년 6월 ~ 현재 : 한국전자통신연구원 무선인터넷보안연구팀 팀장

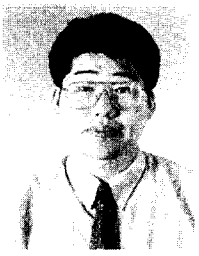
<주관심분야> 무선/이동 QoS, MONET Security, 네트워 보안 프로토콜

정 교 일(Kyo-Il Chung) 정회원

1981년 2월 한양대학교 전자공학과 (공학사)
1983년 8월 한양대학교 산업대학원 전자계산학과 (공학석사)
1997년 8월 한양대학교 대학원 전자공학과 (공학박사)
1980년 12월 - 1981년 11월 엠시스템즈 사원
1981년 12월 - 1982년 2월 한국전기통신연구소 위촉연구원
1982년 3월 - 현재 한국전자통신연구원 정보보호기반연구부장/책임연구원

<주관심분야> IC Card, Security, Biometrics, 국가기반보호, 신호처리

서 창 호(Chang-Ho Seo) 정회원



1986년 ~ 1990년 고려대학교 수학과 졸업(학사)
1990년 ~ 1992년 고려대학교 일반대학원 수학과 (이학석사)
1992년 ~ 1996년 고려대학교 일반대학원 수학과 (이학박사)
1996년~1997년 국방과학연구소 선임연구원
1997년~2000년 한국전자통신연구원 선임연구원, 팀장
2000년~현재 공주대학교 응용수학과(정보보호)조교수

<주관심분야>암호 알고리즘, PKI, 이동통신 보안등