무선랜 기반 VoIP 서비스에서의 효율적인 이동성 지원

이윤정, 박원희, 한상범
호원대학교
skyyjlee@howon.or.kr, pwh8223@naver.com, topflite@korea.ac.kr

An Efficient Mobility Support for VoIP Service based WLAN

Yun-jeong Lee, Won-hee Park, Sang-bum Han
Dept. of Computer Science & engineering Howon University

요 약

무선랜(Wireless Local Area Network)의 보급이 증가되고 서비스 지역이 넓어지게 됨에 따라 이동성을 지원하는 VoIP 서비스의 제공에 대한 관심이 고조되고 있다. 그러나 무선랜의 표준 보안기술을 그대로 적용하는 경우 AP간의 Intra-domain handoff와 subnet 간의 Inter-domain handoff 시 사용자가 감내하기 어려운 정도의 끊김이 발생한다. 본 논문에서는 VoIP 서비스 프로토콜 중 하나인 SIP를 기반으로 하여 데이터 서비스와 VoIP서비스에서의 보안적용 방안을 달리하는 방법을 사용하여 보다 효율적으로 이동성을 지원하는 기법을 제안하였다.

1. 서 론

인터넷 서비스를 비롯한 다양한 멀티미디어 서비스의 발달과 함께 네트워킹 기술은 다양한 기술을 기반으로 매우 빠르게 성장하고 있다. 특히, 유선망 중심의 서비스가 대거 무선망으로 이동하면서 사용자 이동성을 보장하는 무선망의 특징을 활용할 수 있는 기능에 대한 욕구가 증대되었다. 또한 휴대 가능한 소형 개인용 컴퓨터의 대중화와 함께 PDA, Cellular와 WLAN을 동시에 지원하는 휴대용 전화기 등 휴대단말기의 보급이 서비스의 수요를 촉진시키고 있다. 그러나 휴대용 단말기는 CPU의 처리 능력이 낮고 저장 용량이 적으며, 전지 수명이 짧으므로 이를 해결하기 위해 Wireless I/O and Wired Computation 방식을 쓰고 있다. 무선망은 유선망에 비해 낮은 대역폭, 낮은 데이터 전송률 그리고 높은 전송 지연시간 등의 특징들을 갖고 있으므로 이를 해결하기 위한 기술들이 연구되고 있다. 이동성 측면에서, 사용 도중 발생하는 끊김이나 지연은 사용자에게 불편을 초래하며 신뢰도에도 영향을 미치므로 끊김 발생을 사전에 방지하여 이음새 없는(seamless) 이동성이 제공되어야 한다. VoIP 서비스는 유선망에서 처음 시작되었으나 무선인터넷 환경에서 킬러앱(killer Application)이 될 가능성이 높은 서비스이다. 이동전화의 경우 상대적으로 높은 통화료를 요구하므로 무선 인터넷에서의 VoIP서비스는 상당한 비교우위를 점할 수 있다. 그러나 WiBro같은 셀룰라 형상의 휴대인터넷이 아닌 무선랜 방식에서는 이동성의 지원이 가장 큰 걸림돌이다. VoIP에서 효율적으로 이동성을 지원하는 프로토콜에는 Mobile IP와 Session Initiation Protocol(SIP), H.323 등이 있다. Mobile IP는 네트워크 계층에서 이동성을 확보하는 프로토콜이며, mobile SIP는 응용 계층에서 이동성 문제를 해결하는 프로토콜이다. 본 논문에서는 이동성을 지원하는 프로토콜 중에서 SIP를 기반으로 하는 VoIP 시스템 위주로 논의하였다.

이동성은 방문한 subnet에 자신의 관련 정보를 등록(registration)하여 네트워크에게 자신의 위치를 알림으로써 보장 받을 수 있다. 핸드오프 이후에 등록을 하는 SIP Registration은 intra-domain상에서 AP에 대한 재 인증절차로 인한 지연이 발생하여 통화 중 끊김(disruption)을 유발시킨다. 즉 VoIP 서비스가 실행될 때 가장 큰 문제는 cellular 시스템에서와 같은 원활한 로밍이 WLAN에서는 지원되지 않는다는 점이다.

이에 따라 본 논문에서는 WLAN에서 VoIP 서비스를 제공 할 때 AP간의 이동 시 재 인증으로 인한 핸드오프

지연 문제를 해결하고 subnet 간의 핸드오프도 곧 원활하게 지원될 수 있도록 새로운 이동성 지원 기법을 제안하였다. 제안한 방법은 휴대단말기에서 인터넷 등 데이터 위주의 통신을 하는 경우와 음성통신을 하는 경우 모두 동일한 정도의 보안체계를 사용할 필요가 없다는 점에서 착안되었다. 음성통신과 데이터 통신에 각각의 서로 다른 보안체계를 적용함으로 사용자는 끊김이 적거나 없는 음성통신을 사용할 수 있으며 망과 휴대단말기의 부담을 줄이는데 기여한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 VoIP에 대한 관련연구와 각 프로토콜의 기술비교 및 관련환경을 살펴보았으며 제 3장에서 새로운 이동성 지원기법을 제안하였다. 제 4장에서 결론과 향후 연구과제를 언급하였다.

2. 관련연구

2.1 이동성 지원 프로토콜

VoIP 기술은 인터넷 텔레포니(Internet Telephony)와 인터넷을 통한 텔레포니(Telephony over the Internet)라는 2가지 의미상의 차이로 나누어진다[1]. 현재 유관단체의 표준화 작업을 통해 출현한 H.323, SIP, BICC, MEGACO, MGCP, SIGTRAN 등과 같은 다양한 VoIP 프로토콜이 존재한다. 이들을 크게 호 제어 프로토콜과 미디어 제어 프로토콜, SS7 인터네트워킹 프로토콜로 나누어볼 수 있다. 구체적으로 호 제어 계열에는 H.323과 SIP, BICC가 해당되며, 미디어 제어 프로토콜은 MGCP와 MEGACO,나머지는 후자에 속한다.

무선망에서 이동성을 지원하는 프로토콜로 대표적인 것은 H.323과 Mobile IP, SIP 세가지를 들 수 있다. 그 중 가장 오래된 H.323 프로토콜 스택은 1996년 ITU-T 5G16에서 표준화되었으며, 음성 및 영상데이터를 QoS가 보장되지 않는 패킷 교환방식의 네트워크인 LAN을 통해서 전송하는 기술이다. H.323은 기능에 따라 여러 개의 프로토콜로 구성되며 그 구성요소는 Terminal, Gateway, Gatekeeper및 MCU(Multipoint Control Unit)이며, 이중 Gatekeeper와 MCU는 선택항목이다. Mobile IP는 네트워크 계층에서 이동성을 해결하는 것으로 로밍과 macro-mobility 관리를 위해 사용되며, 또한 micro-mobility 지원을 위해 Regional Registration과 Cellular IP와 같은 방법도 제안되었다.

SIP와 H.323은 응용 계층에서 이동성을 해결하는 프로토콜로써, 통신 기반의 H.323은 복잡성으로 인해 구현하는데 많은 어려움이 있는 반면 SIP는 무선 멀티미디어 서비스 환경에 적합한 응용계층의 프로토콜로써 그 사용도가 더 커지고 있다. 이동성지원 측면에서 VoIP의 H.323과 SIP 기술을 이용하여 이동 통신망과의 연동을 시도한 연구[2,3]가 있었지만 모두 만족할만한 결과를 얻지 못했다. 특히 H.323은 기술의 복잡성과 방대한 호 설정 과정 등의 취약점으로 인해 빠르고 확장이 용이한 이동성지원을 얻기 어렵다. 반면 SIP는 개인 프로토콜 스펙을 가지며 redirect모드를 사용하여 보다 효과적인 이동호스트의 동작의 지원이 가능하다.

2.2 SIP

SIP는 멀티미디어 통신을 위한 Signaling Protocol로써, 오디오, 비디오, 화이트보드 등과 같은 멀티미디어 회의, 인터넷 텔레포니 등에 적용할 수 있다. SIP은 크게 user agent와 SIP server로 구성되며 user agent는 도착하는 SIP 메시지에 대응되는 listening 기능과 사용자의 동작 또는 도착한 메시지에 대응되는 SIP 메시지를 전송하는 두 가지 기본기능을 가지며 SIP server는 proxy server와 redirect server로 서로 다른 모드로 동작한다. 또한 Cilient-Server 방식의 프로토콜로써 호 시도자가 상대편을 세션에 참석시키기 위하여 호출하는 형태로 전개되는 프로토콜이다. 또한 멀티미디어 서비스 통신을 위하여 세션에 표현되어야 할 세션 정보들은 SDP(Session Description Protocol)를 이용하여 기술하며 미디어 전송을 위하여 RTP를 사용한다. SIP는 단순하고 빠른 호 설정 방식으로 인해 기존에 사용되었던 ITU-T H.323 표준에 비해 가장 일반적으로 사용되는 VoIP표준 프로토콜로 자리매김하고 있다. SIP 보안 절차는 크게 두 가지로 나눌 수 있다. 첫째, SIP 호 설정에 대한 보안과 둘째, 실시간 미디어에 대한 보안이다.

SIP 호 설정에 사용될 수 있는 보안 방식은 다음과 같다. SIP 메시지 구조는 HTTP (HyperText Transport Protocol) 모델을 기반으로 이루어지고 있으므로 HTTP에서 사용할 수 있는 모든 보안 방식을 적용할 수 있다. 또한, SIP 메시지 내에서 MIME(Multi-purpose Internet Mail Extension)을 전송함으로 PGP(Pretty Good Privacy)또는 S/MIME(Secure/MIME)[4] 과 같은 e-메일 보안 방식을 적용할 수 있다. TLS를 사용하여 안전한 전송 계층 터널을 생성하여 URI(Uniform Resource Identifiers)를 보내거나 IPSec(IP Security)을 사용하여 IP 통신에 대한 범용적인 보안 방식을 적용할 수 있다.

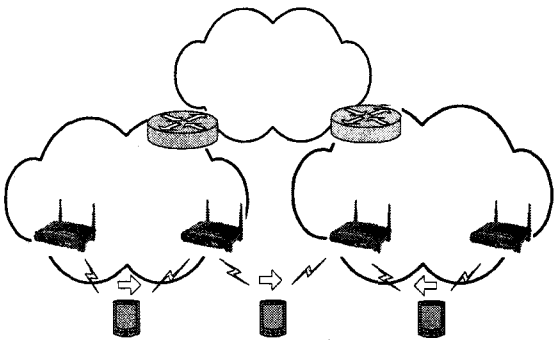
그러나 SIP 버전2에서는 HTTP 기본 인증과 PGP를 사용하지 않을 것을 권고하고 있다. 또한, 전송 계층과 네트워크 계층에서 각각 보안 기능을 제공하는 TLS와 IP-Sec은 SIP 호 설정 후 사용되는 RTP를 전송하기에 적합하지 않음으로 적용하기가 힘들다. RTP(Real-time Transport Protocol)는 실시간 오디오/비디오 전송을 위해 UDP(User Datagram Protocol)기반으로 이루어지므로 TCP(Transmission Control Protocol)기반의 TLS를 적용하기 힘들며, IPSec은 RTP를 전송을 위한 오버헤드가 30~50%에 달하므로 RTP 보안에 효율적이지 않다. 그러므로 최근에는 애플리케이션 계층에서 RTP를 보호하기 위해서 SRTP(Secure RTP)[5] 표준이 제정되었다.

SIP 보안 방식은 초기에는 주로 네트워크 측면에서 연구되어왔다. 그러나 네트워크 측면에서 보안을 적용하기 위한 IP-Sec과 TLS의 단점으로 인하여

최근에는 애플리케이션 측면에서 보안을 적용하기 위한 연구가 진행 중이다. SIP 호 설정 보안 프로토콜로 S/MIME이 주로 연구가 되고 있으며, 실시간 미디어 전송을 위한 RTP 보안 프로토콜로는 SRTP를 적용하려는 연구가 진행 중이다.[6]

2.3 SIP의 이동성 지원

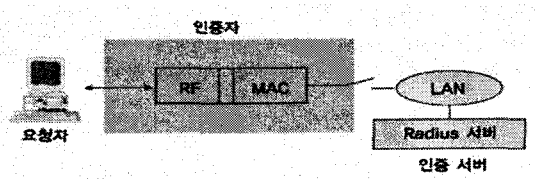
이동성은 무선통신망에게 특정 휴대단말기 및 그것과 관련된 사용자의 존재와 위치를 알려주는 방법인 등록을 통하여 보장 받을 수 있다. 이동성은 로밍(roaming), macro-mobility, 그리고 micro-mobility 등의 유형으로 구분할 수 있다. 로밍은 인터넷 연결이 안된 사용자를 위한 것으로 단말기가 인터넷 접속을 시도할 때의 경우이다. Macro-mobility와 micro-mobility는 인터넷 접속을 유지하면서 핸드오프와 같이 접속점을 변경할 때로써 macro-mobility는 특정 도메인에서 다른 도메인으로(inter-domain) 이동할 경우로써 사용자에게 끊김 없는 서비스를 제공해야만 한다. Micro-mobility는 같은 도메인(intra-domain) 내 에서의 사용자의 이동을 말한다. [그림 1]에 WLAN환경에서 두 가지 이동성의 개념을 표현하였다.



[그림 1] micro-mobility와 macro-mobility

2.4 WLAN의 보안기술

WLAN이 보급되면서 가장 큰 이슈로 등장한 것은 보안이다. 유선 네트워크에서는 보안에 대한 이슈는 건물 내부로 한정되고 도청을 위해서는 유선 케이블을 태핑(tapping)해야 하는 과정이 필요했지만, 무선에서는 건물 밖으로 전파되는 신호를 쉽게 가로챌 수 있기 때문이다. IEEE 802.11 초기 과정에서는 WEP(Wired Equivalent Privacy) 알고리즘 기반의 보안 대책이 WLAN의 표준으로 채택 되였으나 이의 취약점이 공개되면서[3,4] IEEE 802.11 워킹 그룹에서는 2001년 5월부터 IEEE 802.11 워킹그룹 산하에 TGi(Task Group i)를 결성하여 무선랜 MAC 계층 보안 기능 향상을 위한 표준화를 진행하기 시작하였다. IEEE 802.11 TGi의 표준화 목표는 하나의 액세스 포인트(AP)가 관할하는 기본 서비스 셋(BSS, Basic Service Set) 안에서 액세스 포인트와 무선 단말(MS, Mobile Station) 사이에 인증과 키 교환 및 무선구간 데이터 보호를 통해 튼튼한 보안망(RSN, Robust Security Network)을 구축하여 무선랜 사용자를 보호한다는 것이다. IEEE 802.11i 표준은 무선랜 사용자 보호를 위해서 사용자 인증 방식, 키 교환 방식 및 향상된 무선구간 암호 알고리즘을 정의하고 있으며, IEEE 802.1X 인증, 4-Way handshake 키 교환 및 CCMP(Counter mode with CBC-MAC Protocol) 암호 알고리즘을 필수 구현 기능으로 정의하였다. IEEE 802.11i 표준에서는 사용자 인증과 키 교환의 큰 틀로써 IEEE 802.1X를 사용한다고 규정하고 있으며, 나아가 구체적인 키 교환 방식인 4-Way handshake 방식, 교환된 키의 계층적 사용구조 (key hierarchy), 그리고 새로운 무선 구간 암호 알고리즘 (cipher suites)의 정의를 포함하고 있다. [그림 2]는 IEEE 802.1X의 인증 개념을 보여준다.



[그림 2] 802.1X의 인증체계

3. VoIP를 위한 이동성 지원 기법

WLAN 표준인 IEEE 802.1x에서는 실시간 음성 통신을 사용하고자 할 때는 보안에 필요한 다단계 절차로 인해 핸드오프에 지연이 발생한다. 또한, 물리계층과 데이터링크 계층만을 지원하는 WLAN 장비 특성에 따라 네트워크 계층에서 핸드오프를 제공하지 못하는 문제가 있다. 그러므로 WLAN 상에서 음성통신을 사용하기 위해서는 AP간을 이동할 때의 핸드오프 문제와 subnet 간을 이동할 때의 핸드오프 문제를 고려하여야 한다. 본 장에서 이러한 문제를 해결하기 위해 음성통신을 사용할 때 이동성을 지원하기 위한 핸드오프 기능을 제공하면서 보안 기능을 동시에 제공하기 위한 기법을 제안한다.

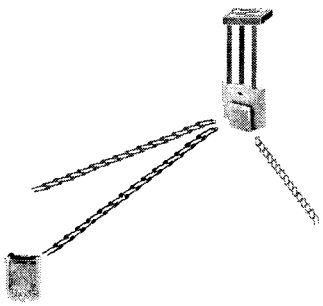
3.1 AP 간 핸드오프

현재 WLAN 표준 중에서 가장 일반적으로 사용되는 기술은 IEEE 802.11g 또는 IEEE 802.11a 이며, 이러한 표준방식으로 무선랜을 구축할 때 802.1X와 802.11i는 보안을 위해 일반적으로 적용되는 기술이다. 802.1X 인증 방식에 있어 사용자가 기존에 접속되었던 AP에서 새로운 AP로 접속을 할 때는 재인증이 요구되며, 802.1X 재인증에 필요한 다단계 절차는 AP 간 핸드오프 시 음성과 같은 실시간 데이터에 대해 전송 지연 문제를 발생시킨다. 재인증 절차에 의한 전송 지연은 결국 실시간 데이터에 대한 패킷 손실로 인해 음성의 찌그러짐 현상이나 음성 통화가 단절되는 현상이 발생한다. 그러므로 기존에 문자나 이미지 등 전송 시간에

상대적으로 덜 민감한 데이터를 위주로 다루었던 WLAN의 인증 및 보안 절차를 실시간 데이터 전송이 필요한 VoWLAN 서비스에 그대로 적용할 때는 서비스 품질에 문제가 발생한다.

이러한 문제를 해결하기 위해서 AP의 데이터링크 계층에서 음성통신과 데이터통신에 대한 트래픽을 분리하고 각각의 트래픽에 대해 보안 정책을 별도로 설정하는 방법을 적용할 수 있다. WLAN에 접속하여 음성통신을 사용할 때는 AP간 핸드오프에 대한 전송 지연 문제를 해결하기 위해 802.1X 인증 방식 대신 무선단말의 MAC 주소를 이용한 인증을 실행하고 음성통신에 대한 사용자 인증 및 암호화는 SIP프락시 서버의 애플리케이션 계층에서 S/MIME, SRTP 등을 적용하여 시스템을 구현한다. 즉, 음성통신에 대해서는 L2 (Layer 2)데이터링크 계층에서는 음성통신에 대한 로밍을 위해 최소의 인증 기능만을 지원하고 애플리케이션 계층인 L7에서 추가적인 보안 기능을 제공하도록 한다.

한편, 전송 시간에 대해 상대적으로 덜 민감한 데이터 통신에 대해서는 WLAN 구축 시 802.1X 인증 방식과 802.11i보안을 적용하여 AP에서 데이터 전송에 대한 강력한 보안기능을 제공하도록 한다. [그림 3]은 AP에 적용한 다중 VLAN의 개념을 보여준다.



[그림 3] AP에 적용한 다중 VLAN의 예

이와 같이 L2에서 VoIP서비스와 데이터서비스를 분리하고 각 서비스에 대해 별도의 보안 정책을 지원할 수 있도록 하기 위해서는 WLAN AP에 다중 VLAN[7] 및 다중 SSID(Service set Identifier) 기능이 구현되어야 한다. 또한 AP에서 각 VLAN 별로 별도의 보안 정책을 설정할 수 있는 기능이 구현되어야 하는데 실제 다중 SSID와 다중의 VLAN이 구현되는 AP가 개발되어 상용화 되어있다.

WLAN의 데이터링크 계층에서 음성통신과 데이터 통신의 트래픽을 분리하기 위해 AP에 음성통신을 위한 VLAN과 데이터통신을 위한 VLAN을 별도로 생성하고 각 VLAN에 서로 다른 IP 인터페이스를 지정하도록 한다. 또한 사용자가 음성통신 또는 데이터통신 서비스를 이용하기 위해 WLAN에 접속할 때는 각 서비스를 위해 별도로 할당된 VLAN을 구별하여 접속할 수 있도록 음성 VLAN과 데이터 VLAN에 서로 다른 SSID를 설정하도록 한다. 이와 같은 환경에서 사용자는 데이터통신을 사용하고자 할 때는 무선단말에서 무선랜 접속 프로그램을 실행시켜 데이터 VLAN에 부여한 SSID로 AP에 접속하면 802.1X 인증을 요청하고 사용자 인증이 성공하면 사용자의 무선단말과 AP에 암호화 키가 설정되어 이후 실행되는 모든 데이터통신에 대해 암호화 통신을 진행 할 수 있다. 사용자가 음성 통신을 사용하고자 할 때는 무선랜 접속 프로그램에서 음성 VLAN에 부여된 SSID로 접속하면 인증서버에 이미 등록된 무선단말에 설치된 NIC의 MAC 주소에 의해 사용자가 의식하지 못한 채 MAC 인증이 실행되고 무선랜 접속이 완료되면 사용자는 무선단말에서 VoIP 클라이언트를 실행시켜 VoIP 서비스를 이용할 수 있게 된다. VoIP 클라이언트가 SIP 프락시서버(proxy server)에 접속하면 S/MIME를 통해 안전한 call setup이 이루어지며, call setup이 완료된 이후에는 SRTP를 이용하여 송신자와 수신자 간에 이루어지는 음성통신에 대한 암호화가 이루어지게 된다.

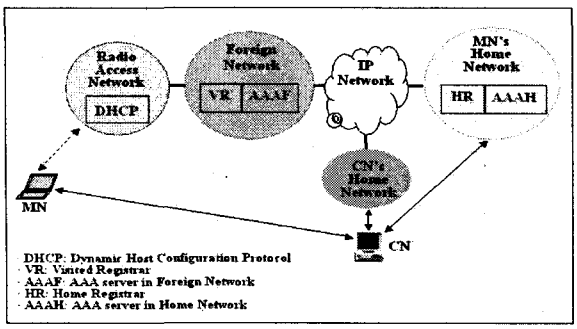
3.2 subnet 간 핸드오프

사용자가 서로 다른 subnet 간을 이동할 때는 inter-domain 핸드오프이므로 무선단말이 이전 subnet에서 할당 받았던 IP 주소는 더 이상 유용하지 않다. 그러므로 subnet 간을 이동할 때는 새롭게 접속되는 AP에 대한 재인증뿐만 아니라 새로운 subnet에 접속할 수 있도록 지원할 수 있는 방법이 필요하다. 그러나 AP는 데이터링크 계층에서 MAC 주소에 의해 트래픽 경로를 제어하는 브리지(bridge)장비로써 네트워크 계층의 IP를 처리할 수 있는 기능이 없다. 따라서 WLAN을 접속하여 subnet 간을 이동할 때는 네트워크 계층에서 핸드오프를 지원하기 위한 추가적인 방법이 필요하다. 네트워크 계층인 L3에서 로밍을 지원하기 위해 일반적으로 연구되는 것은 Mobile IP를 이용하는 방법과 SIP를 이용하는 방법이 있다.

Mobile IP를 이용한 방법에서는 무선단말이 홈에이전트(home agent)에 접속한 이후 외부 에이전트(foreign Agent)로 이동하는 경우 홈 에이전트와 외부 에이전트 간에 IP 터널링이 구성되고 이동한 무선단말에 전송되는 모든 패킷은 홈 에이전트가 프락시 역할을 하여 터널을 통해 외부 에이전트로 전송한다. 이와 같은 방법으로 외부 에이전트로 이동한 무선단말이 전송하는 모든 패킷은 외부 에이전트가 프락시 역할을 하여 홈 에이전트로 전송하는 방식을 적용하는 것이다.

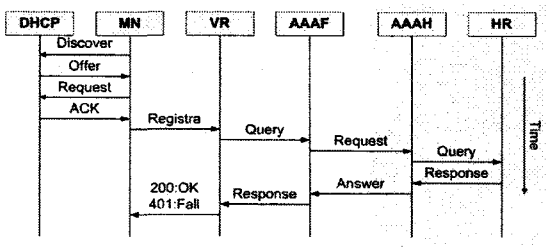
[그림 4]는 SIP의 일반적인 구조를 설명한 것이다. 여기서 MN(Mobile Node)은 무선단말을 의미한다. SIP에서는 사용자의 이동성을 지원하기 위해 DHCP(Dynamic Host Configuration Protocol) 와 AAA(Authentication, Authorization, Accounting) 등을 조합한 구조를 사용하고 있다. MN은 무선망(RAN: Radio Access Network)을 통해 방문 네트워크(Foreign Network)와 연결되어 있으며, 이들 간에 DHCP 서버가 사용되고 있다. 방문 네트워크와 홈 네트워크(Home

Network), 상대 노드(CN: Correspondent Node)의 홈 네트워크들이 IP망(Internet Protocol Network)을 통해 서로 연결되어 있다. Registrar는 방문 네트워크에 VR(Visited Registrar), 홈 네트워크에 HR(Home Registrar)이 각각 존재하며 여기에는 SIP 프락시서버(Proxy server), 위치 서버(Location Server), 사용자 에이전트 서버(User Agent Server) 등이 결합되어 있다. 또한 AAA 서버는 방문 네트워크에 AAAF, 홈 네트워크에는 AAAH가 각각 위치해 있다.



[그림 4] SIP의 일반적인 구조

[그림 5]는 일반적인 SIP Registration의 시그널링 흐름을 설명한 것이다. 먼저 MN와 DHCP 서버간에 새로운 IP 주소를 할당 받기 위해 다음과 같은 메시지 교환이 이루어진다. 먼저 MN가 DHCP 서버에게 *DHCP_DISCOVER* 메시지를 브로드케스트하면, 해당 서버들은 *DHCP_OFFER* 메시지를 통해 MN에게 새로운 주소를 요구한다. 그러면 MN는 선택된 서버에게 *DHCP_REQUEST* 메시지를 보내고, DHCP 서버는 MN에게 *DHCP_ACK*로 답한다. 새로운 IP 주소를 할당 받은 후, MN는 방문 네트워크의 레지스트라(VR)에 SIP 등록을 하기 위해 자신의 홈 네트워크의 레지스트라(HR)에 SIP *Request* 및 *Answer* 메시지를 주고 받게 된다. MN는 CN에게 *Invite* 메시지를 보내어 초대하게 된다. 그림 2와 그림 3에서 알 수 있듯이 SIP Registration에서는 interdomain 간에 핸드오프가 발생한다.



[그림 5] SIP의 일반적인 구조

이렇게 SIP를 적용하여 subnet 간의 inter-domain 핸드오프를 수행하는 경우 AAAF와 AAAH의 인증에 지연시간이 발생하나 AAAF와 AAAH는 대역폭이 상대적으로 넓은 유선망 이므로 비교적 지연시간이 적다. 또한 이 경우에도 많은 지연은 AP의 인증에서 발생하므로 전술한 AP의 VLAN을 활용한 별도의 보안정책을 적용함으로 전체 지연시간은 사용자가 감내할 수 있을 만큼 줄게 된다.

4. 결론 및 향후 연구과제

현재 IEEE 802.11 표준 단체에서는 WLAN 기반에서 음성과 같은 실시간 데이터를 전송하기 위한 표준을 제정 중이다. 802.11r에서는 AP 간의 이동 시 빠른 핸드오프를 위한 표준 작업과 802.11e에서는 QoS (Quality of Service)를 지원하기 위한 표준화가 진행되고 있다. 또한, IETF에서는 네트워크 계층에서 핸드오프를 지원하기 위해 Mobile IP 표준을 제정하였지만, 아직도 핸드오프 시의 전송 지연을 해결하기 위해 많은 연구가 진행 중이다. 본 논문에서는 WLAN 상에서 핸드오프 및 보안 문제를 해결하기 위해 음성 VLAN과 데이터 VLAN을 분리하는 방법과 subnet 간 핸드오프를 위해 mobile SIP를 적용하는 방법을 제시하였다. 본 논문에서 제시한 VLAN을 이용한 보안 및 핸드오프 기능을 제공하기 위한 방법은 음성통신과 데이터통신에 대해 별도의 subnet 대역을 구분함으로써 자원의 낭비를 초래할 수 있다. 특히 CPU능력이 작은 무선단말에는 이중의 클라이언트 프로그램이 필요하다는 단점이 있으나 WLAN에서 강력한 보안과 빠른 핸드오프를 동시에 제공할 수 있다. 향후 제안한 시스템의 실제 구현과 정확한 성능분석을 위한 연구가 필요하다.

참 고 문 헌

[1] 김영한, 고석갑, " VoIP기술 표준화 동향," 한국통신학회지 Vol.18, no.3, 2001, pp. 326-339

[2] M. Moh, G. Berquin and Y. Chen, " Mobile IP Telephony: Mobility Support of SIP," IEEE, 1999, pp. 554-559.

[3] W. Liao, J. Liu, " VoIP Mobility in IP/Cellular Network internetworking," IEEE Comm. Mag., Apr. 2000, pp. 70-75.

[4] Ramsdell B., " S/MIME Version 3 Message Specification," IETF RFC 2633, 1999.

[5] Baugher M., et al., " The Secure Real-time Transport Protocol (SRTP)," IETF RFC 3711, March 2004.

[6] Andreas Steffen, et al., " SIP Security," DFN-Arbeitstagung ber Kommunikationsnetze, pp. 397-412, 2004.

[7] IEEE Std 802.1Q," Virtual bridged local area networks," May 2003.