情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

VoWLAN 보안 및 로밍 설계

김 미 연*, 김 계 진*, 이 동 훈**

요 약

네트워크 컨버전스 및 사용자 이동성의 중시로 무선랜 기반에서 음성 서비스를 이용하고자 하는 VoWLAN 서비스에 대한 관심이 고조되고 있다. 그러나 무선랜 보안 표준기술을 그대로 적용하고자 할 때는 AP 간을 이동할 때와 서브넷 간을 이동할 때 로밍에 대한 문제가 발생한다. 이에 본 논문에서는 VoWLAN 서비스를 구현할 때 로밍과 보안 기능을 동시에 제공하기 위한 설계방법을 제안한다.

Ⅰ. 서 론

VoIP (Voice over Internet Protocol)는 오늘날 가장 빠르게 성장하는 인터넷 서비스 중의 하나이다. 또한, 이동성과 광대역 네트워크 서비스를 제공하는 무선랜 (Wireless Local Area Network: WLAN)도 그 요구가 점차 증대하고 있어 추후 최단 가입자 구간 (last mile) 인터넷 서비스로써 자리매김 할 것으로 예상되고 있다. 이러한 두 가지 기술의 융합으로 VoWLAN (Voice over WLAN)은 가장 중요한 인터넷 서비스로 부각될 것이 예상된다.[1]

그러나 WLAN이 보급되면서 가장 큰 이슈로 등장했던 보안 표준 기술을 VoWLAN 서비스에 그대로 적용하려고 할 때는 이동성 측면에서 두 가지 문제점이 발생한다. 첫째, 사용자가 AP (Access Point)와 AP 간을 이동할 때 발생되는 새롭게 접속되는 AP에 대한 재인증 절차로 인한 로밍 지연 문제와 둘째, 사용자가 서브넷 간을 이동할 때 발생되는 네트워크 계층에서의 로밍이 WLAN에서는 지원되지 않는다는 점이다.

이에 따라 본 논문에서는 VoWLAN 서비스를 제공할 때 재인증으로 인한 로밍 지연 문제를 해결하고 서브넷 간 이동 시 로밍이 지원될 수 있도록 VoWLAN 시스템의 설계 방법을 제안한다. 본 논문의 제 2장에서는 이제까지 연구되어 왔던 WLAN 보안 기술 및 VoIP 보안 기술을 분석한다. 제 3장에서는 VoWLAN 시스템을 구축하고자 할 때 음성통신과 데이터통신에 대한 보안을 유지하면서 AP간을 이동할 때의 로밍 문제와 서브넷 간을 이동할 때의 로밍 문제를 해결하기 위한 시스템 설계 방법을 기술한다. 마지막으로 제 4장에서 결론을 맺는다.

Ⅱ. 관련 연구

VoWLAN 서비스는 네트워크 측면에서 WLAN을 기반으로 하여 애플리케이션 측면에서 음성통신을 이용하기 위한 서비스이다. 그러나 음성통신을 위한 WLAN 시스템을 별도로 구축하기 보다는 데이터통신과 음성통신을 동일한 WLAN 상에서 이용하기 위해 설계되어야 한다. 현재 WLAN 표준 단체에서는 WLAN 기반으로 음성을 전송하기 위해 표준 제정을 진행하고 있지만 이제까지의 대부분의 연구는 무선 데이터통신 중심의 WLAN 기술과 유선 음성통신 중심의 VoIP 기술이 독립적으로 연구되어왔다.

본 장에서는 VoWLAN 시스템 설계에서 로밍과 보안을 지원하기 위한 기술을 제안하기에 앞서 WLAN 분야와 VoIP 분야에서 기존에 연구되어 왔던 보안 기술에 대해 먼저 분석한다.

2.1 WLAN 보안

WLAN 표준으로 가장 널리 보급된 IEEE 802.11[2] 표준에서 초기에 제정하였던 공유키 인증 방식과 WEP (Wired Equivalent Privacy) 암호화 방식의 취약

* KT 컨버전스본부 (miyeon@kt.co.kr, kyejin@kt.co.kr)
** 고려대학교 정보보호대학원 (donghlee@korea.ac.kr)

성이 증명되면서 802.11 표준 단체에서는 802.11i[3] 라고 하는 새로운 보안 표준을 제정하였다.[4] 802.11i는 기존의 공유키 인증 방식을 개선하기 위해 802.1X[5] 인증 표준을 적용하고 무결성과 기밀성을 개선하기 위해 새로운 암호화 알고리즘을 적용하였다.

2.1.1 802.1X 표준

802.11 표준에서는 두 가지 형태의 인증 방식을 정의하고 있다. 첫째, 오픈시스템 (open system) 방식은 인증 알고리즘이 존재하지 않는 방식을 의미한다. 둘째, 공유키 인증 방식은 AP에 고정된 WEP 키를 미리 분배하고 무선단말이 AP에 접속을 요청할 때 이 키를 이용하여 인증을 요청하는 방식이다. 그러나 공유키 인증 방식은 AP에 미리 분배된 고정된 키가 노출될 우려가 있고 설치된 AP마다 고정된 키를 관리해야하는 문제점이 발생하였다. 그래서 이러한 인증 방식을 개선하기 위해 802.1X 인증 방식을 도입하였다. 802.1X 인증 시스템은 인증요청자 (supplicant), 인증자 (authenticator) 및 인증서버 (Authentication Server: AS)로 구성된다. 인증요청자는 WLAN NIC (Network Interface Card)이 장착된 무선단말을 의미하며 인증자는 WLAN AP를 의미한다. AS는 일반적으로 RADIUS (Remote Authentication Dial-In User Service) 서버를 사용한다. AS에서는 인증을 위해 사용자 또는 단말 정보를 관리하고 무선단말이 AP를 통해 AS에 요청한 인증이 성공하면 AS와 무선단말 간에 동일한 암호화 키가 자동으로 생성된다. AS는 세션마다 재생성된 암호화 키를 AP에게 전달하고 이후에 진행되는 모든 데이터통신은 무선단말과 AP사이에서 암호화되어 전송한다. 이와 같은 과정을 통해 802.1X는 기존의 공유키 인증 방식의 문제점을 해결한다.

802.1X는 MD5 (Message Digest 5), TLS (Transport Layer Security), TTLS (Tunneled TLS), PEAP (Protected Extensible Authentication Protocol) 등 다양한 인증 방식을 지원하기 위해 EAP와 결합하여 사용된다. 이 중 MD5는 암호화를 위한 키 생성을 지원하지 않고, TLS는 공개키 인증서에 대한 PKI (Public Key Infrastructure) 구축의 복잡성으로 인해 EAP-TTLS[6]와 PEAP이 가장 많이 사용된다.

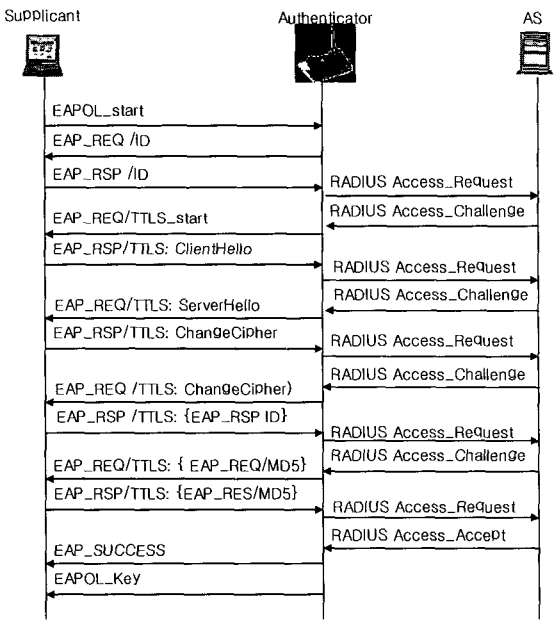
그림 1은 EAP-TTLS 프로토콜을 사용하여 인증이 성공했을 때의 메시지 흐름을 보여 준다.

EAP-TTLS는 두 단계로 구성된다. 1단계는 TLS 핸드쉐이크 (handshake) 단계로 단말이 서버를 인증하는 과정을 포함하며, 2단계는 TLS 터널 단계로 단말과 서버사이에 생성된 터널을 통해 사용자 인증 및 키 분배 과정이 이루어진다. 사용자 인증을 위한 프로토콜은 EAP를 재사용하거나 PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) 등이 사용될 수 있다. 그림 1에서는 사용자 인증 프로토콜로 EAP-MD5가 사용된 예를 보여준다. 인증자는 실제로 인증요청자 및 AS에 의해 생성된 EAP 정보를 전달하는 역할을 수행하며 인증과정에 필요한 EAP-REQ (EAP-Request) 정보 및 EAP-RSP (EAP-Response) 정보는 AS 및 인증요청자에 의해 생성된다.

802.1X 인증 과정은 무선단말이 최초에 AP에 접속한 이후에 실행될 뿐만 아니라 사용자가 이전에 접속했던 AP에서 새로운 AP로 이동하여 접속하는 경우에도 실행된다. 그림 1에서 보는 바와 같이 802.1X 인증과정은 인증요청자, 인증자 및 AS 간에 다단계 정보 전달 절차를 필요로 한다. 그러므로 사용자가 음성통신과 같이 실시간 데이터를 전송해야 하는 경우에는 이동하는 과정에서 로밍 지연이 발생되는 문제가 발생한다.

2.1.2 802.11i 표준

802.11 표준에서 정의한 WEP 암호화 방식은 다



(그림 1) EAP-TTLS를 이용한 인증 성공 과정

음과 같은 취약성을 가진다.[7] 첫째, 키 관리가 정의되지 않아 고정된 키를 사용하여 암호화를 해야 한다. 둘째, 암호화 키 스트림 (key stream)을 생성하기 위한 IV (Initialization Vector)는 24비트의 짧은 길이를 가짐으로 인해 공격자에게 키 스트림 또는 WEP 키가 노출될 확률이 높아진다. 셋째, 무결성 검사를 위한 ICV (Integrity Check Value) 알고리즘의 선형함수 (linear function) 특성으로 인해 공격자에 의해 메시지가 수정되고, 수정된 메시지에 대해 ICV를 재생성할 수 있도록 한다. 이와 같은 WEP 보안의 취약성으로 인해 IEEE 802.11i에서는 사용자 인증 방식, 키 교환 방식 및 무선구간에서 향상된 암호화 알고리즘을 정의하여 WLAN 보안 기능을 향상시켰다.

802.11i 표준에서는 사용자 인증 방식으로 802.1X 인증 방식과 사전 공유키 (Pre-Shared Key: PSK) 인증 방식을 정의한다. 첫 번째, 802.1X 인증은 필수 항목으로 무선구간에 필요한 마스터키 (Pairwise Master Key: PMK)를 매 세션마다 생성하여 전달할 수 있으며 두 번째, PSK 인증은 별도의 인증서버가 필요 없이 무선단말과 AP가 미리 고정된 키를 공유하고 공유키에 의사난수 함수 (Pseudo-Random Function: PRF)를 적용하여 마스터키를 유도하는 방식이다.

802.11i에서는 무선 구간 데이터를 보호하기 위한 방법으로는 TKIP (Temporal Key Integrity)과 CCMP (Counter mode with Cipher block chaining-Message authentication code Protocol)를 정의한다. TKIP은 WEP을 확장하는 방법으로 WEP과 같이 RC4 (Revest's Cipher algorithm)에 기반한다. 그러나 TKIP에서는 IV를 48비트로 확장하였으며, 키 재사용을 막기 위해 802.1X에 의해 TK (Temporal Key)를 생성하고 TK와 무선단말의 MAC (Media Access Control) 주소 및 16 비트의 IV를 결합하여 암호화 키를 생성한다. 또한, 순차번호 (sequence number)를 적용하여 재사용 공격을 방지함은 물론 해쉬함수를 사용하여 MIC (Message Integrity Code)를 생성하여 공격자가 무결성 검사 값을 재생성하지 못하도록 함으로써 기존의 WEP 보안 방식의 취약성을 해결하였다. CCMP는 보안 강도를 높이기 위해 RC4 대신 CCM 모드의 AES (Advanced Encryption Standard)를 암호화 알고리즘으로 사용하는 방식이다. TKIP이 WEP에 대한 단기적인 대안 방법으로 기존의 802.11 AP의 펌웨어를 업그레이드를 하여 구현할 수 있는 방식인 반면 CCMP는 WEP에 대한 장기적인 대안 방법으로 기존의 802.11 AP의 칩셋 (chip set)을 교체하여 구현할 수 있다.

802.11i 표준은 이동성을 위한 기초적인 기능으로 선인증과 PMK 관련 정보에 대한 캐시 (cache) 기능을 제공한다. 선인증은 무선단말이 현재 접속된 AP 뿐만 아니라 인접해있는 AP에도 인증을 요청해서 미리 다수의 AP로부터 인증을 받아놓은 기능이다. 선인증의 결과로 무선단말은 인접한 AP에 대한 PMK 역시 미리 저장한다. 이러한 기능을 통해 향후 로밍을 위한 사전 작업을 준비하지만 실시간 로밍을 요구하는 VoIP 등의 응용에서는 보완이 필요할 것으로 보인다.[8]

2.2 VoIP 보안

SIP (Session Initiation Protocol)는 단순하고 빠른 호 설정 방식으로 인해 기존에 사용되었던 ITU-T H.323 표준에 비해 가장 일반적으로 사용되는 VoIP 표준 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)[9]와 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 버전 2에서는 HTTP 기본 인증과 PGP를 사용하지 않을 것을 권고하고 있다. 또한, 전송 계층과 네트워크 계층에서 각각 보안 기능을 제공하는 TLS와 IPSec은 SIP 호 설정 후 사용되는 RTP를 전송하기에 적합하지 않음으로 적용하기가 힘들다. RTP (Realtime 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) [10] 표준이 제정되었다.

SIP 보안 방식은 초기에는 주로 네트워크 측면에서 연구되어왔다. 그러나 네트워크 측면에서 보안을 적용하기 위한 IPSec과 TLS의 단점으로 인하여 최근에는 애플리케이션 측면에서 보안을 적용하기 위한 연구가 진행 중이다. SIP 호 설정 보안 프로토콜로는 S/MIME이 주로 연구가 되고 있으며, 실시간 미디어 전송을 위한 RTP 보안 프로토콜로는 SRTP를 적용하려는 연구가 진행 중이다.[11]

Ⅲ. VoWLAN 보안 및 로밍 설계

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 있었기 때문이다. 이에 WLAN 표준 단체인 802.11에서는 802.11i라는 보안 표준을 제정했지만, VoIP와 같은 실시간 음성 통신을 사용하고자 할 때는 보안에 필요한 다단계 절차로 인해 로밍이 지연되는 새로운 문제가 발생되었다. 또한, 물리계층과 데이터링크 계층만을 지원하는 WLAN 장비 특성에 따라 네트워크 계층에서 로밍 기능을 제공하지 못하는 문제가 있다. 그러므로 WLAN 상에서 음성통신을 사용하기 위해서는 AP 간을 이동할 때의 로밍 문제와 서브넷 간을 이동할 때의 로밍 문제를 고려하면서 VoWLAN에 대한 보안 설계가 필요하다.

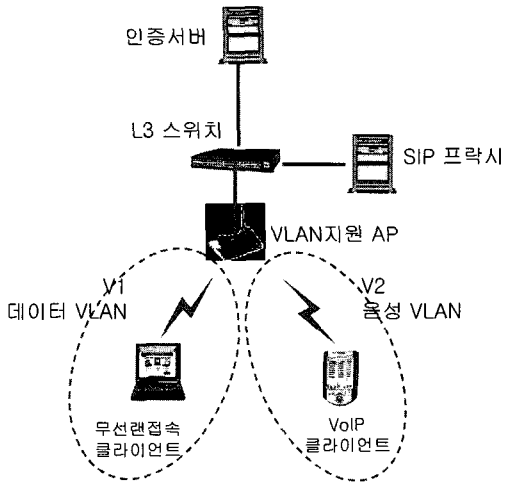
본 장에서 이러한 문제를 해결하기 위해 VoWLAN 서비스에서 음성통신을 사용할 때 이동성을 지원하기 위한 로밍 기능을 제공하면서 보안 기능을 동시에 제공하기 위한 VoWLAN 설계 방법에 대해 제안한다.

3.1 AP 간 음성 로밍을 고려한 보안 설계

현재 WLAN 표준 중에서 가장 일반적으로 사용되는 기술은 IEEE 802.11g 또는 IEEE 802.11a 이며, 이러한 표준 방식으로 무선랜을 구축할 때 802.1X와 802.11i는 보안을 위해 일반적으로 적용되는 기술이다. 그러나 보안을 강화하기 위한 이러한 표준은 WLAN을 기반으로 한 VoIP 서비스에 적용할 때는 로밍에 대한 지연문제를 발생시킨다. 802.1X 인증 방식에 있어 사용자가 기존에 접속되었던 AP에서 새로운 AP로 접속을 할 때는 재인증이 요구되며, 802.1X 재인증에 필요한 다단계 절차는 AP 간 로밍 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 로밍에 대한 전송 지연 문제를 해결하기 위해 802.1X 인증 방식 대신 무선 단말의 MAC 주소를 이용한 인증을 실행하고 음성통신에 대한 사용자 인증 및 암호화는 SIP 프락시 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 하도록 한다. 한편, 전송 시간에 대해 상대적으로 덜 민감한 데이터통신에 대해서는 WLAN 구축 시 802.1X 인증 방식과 802.11i 보안을 적용하여 AP에서 데이터 전송에 대한 강력한 보안기능을 제공하도록 한다.

이와 같이 L2에서 음성통신과 데이터통신의 트래픽을 분리하고 각 트래픽에 대해 별도의 보안 정책을 지원할 수 있도록 하기 위해서는 WLAN AP에 다중 VLAN[12] 및 다중 SSID (Service Set IDentifier) 기능이 구현되어야 한다. 또한, AP에서 각 VLAN 별로 별도의 보안 정책을 설정할 수 있는 기능이 구현되어야 한다. 그리고 VoWLAN 서비스 시스템을 구축할 때 다중 VLAN 및 다중 SSID 기능을 지원하는 AP를 이용하여 인프라스트럭처 모드(infrastructure mode)로 WLAN을 구축한다. WLAN의 데이터링크 계층에서 음성통신과 데이터통신의 트래픽을 분리하기 위해 AP에 음성통신을 위한 VLAN과 데이터통신을 위한 VLAN을 별도로 생성하고 각 VLAN에 서로 다른 IP 인터페이스를 지정하도록 한



〔그림 2〕 AP에서 음성 VLAN과 데이터 VLAN 분리 구축

다. 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.

그림 2는 AP에서 음성통신과 데이터통신에 대해 별도의 VLAN을 구현한 시스템 구성도이다.

이와 같은 환경에서 사용자는 데이터통신을 사용하고자 할 때는 무선단말에서 무선랜 접속 프로그램을 실행시켜 데이터 VLAN에 부여한 SSID로 AP에 접속하면 802.1X 인증을 통해 사용자 ID와 패스워드를 입력하여 사용자 인증을 요청하고 사용자 인증이 성공하면 사용자의 무선단말과 AP에 암호화 키가 설정되어, 이후 실행되는 모든 데이터통신에 대해 암호화 통신을 진행할 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 프락시 서버 (proxy server)에 접속하면 S/MIME를 통해 안전한 호 설정이 이루어지며, 호 설정이 완료된 이후에는 SRTP를 이용하여 송신자와 수신자 간에 이루어지는 음성통신에 대한 암호화가 이루어지게 된다.

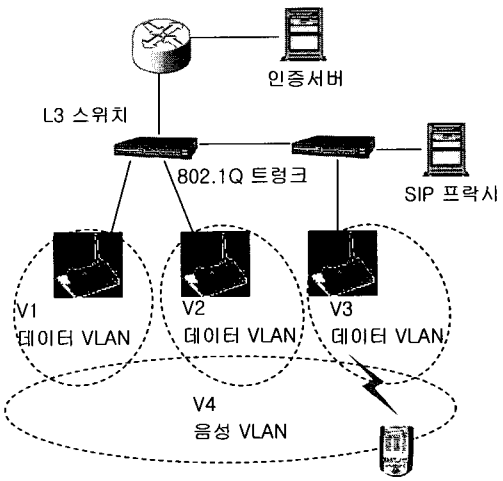
음성 VLAN이 데이터 VLAN에 비해 보안이 낮은 레벨로 설정되었기 때문에 L3 스위치에서 음성 VLAN의 패킷이 데이터 VLAN으로 라우팅(routing) 되지 않도록 제어해야 한다. 또한, SIP 프락시 서버를 음성 VLAN 대역에 설치하여 사용자가 음성 VLAN에 접속하였을 때 SIP 프락시 서버에 접속할 수 있도록 설치한다.

3.2 서브넷 간 음성로밍을 고려한 보안 설계

사용자가 서로 다른 서브넷 간을 이동할 때는 무선단말이 이전 서브넷에서 사용했던 IP 주소는 새로운 서브넷으로 이동했을 때는 더 이상 유용하지 않다. 그러므로 서브넷 간을 이동할 때는 새롭게 접속되는 AP에 대한 재인증뿐만 아니라 새로운 서브넷에 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. 그러므로 WLAN을 접속하여 서브넷 간을 이동할 때는 네트워크 계층에서 로밍을 지원하기 위한 추가적인 방법이 필요하다.

네트워크 계층인 L3에서 로밍을 지원하기 위해 일반적으로 연구되는 것은 Mobile IP를 이용하는 방법이다.[13] Mobile IP를 이용한 방법에서는 무선단말이 홈 에이전트 (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 (proxy) 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. 그러나 Mobile IP에서 홈 에이전트와 외부 에이전트 간에 패킷을 재전송하는 과정에서 발생하는 전송 지연 문제는 현재 연구가 이루어지고 있으나 아직 실용화 단계에 이르지 못하였다. 또한 L3 로밍을 위해 Mobile IP를 적용할 때는 Mobile IP를 위한 별도의 클라이언트가 필요하지만, 소형 Wi-Fi 단말이나 PDA (Personal Digital Assistant)와 같이 소량의 CPU 능력을 가진 단말에 추가적인 클라이언트를 탑재하는 것은 무선단말에서 처리속도를 지연시켜 실시간 음성 전송에 적용하기에는 부적합하다.

본 장에서는 서브넷 간의 L3 로밍을 위한 방법으로써 VLAN을 이용하여 브로드캐스팅 (broadcasting) 영역을 확장하는 방법을 제안한다. VLAN을 이용하여 서브넷 간 로밍을 지원하는 방법은 음성 VLAN으



(그림 3) 802.1Q 태킹을 이용한 음성 VLAN 영역 확장

로부터 전송되는 패킷이 서브넷 간 이동시에도 해당 서브넷으로 패킷이 전송될 수 있도록 802.1Q VLAN 태깅을 이용하여 음성 VLAN의 브로드캐스팅 영역을 전체 서브넷 영역으로 확장하는 방법이다.

그림 3은 음성 VLAN에 접속하는 경우 서브넷 간 이동시에도 로밍이 지원되도록 시스템을 구성한 예이다. 데이터 VLAN은 각 서브넷 영역으로 브로드캐스팅 영역이 한정되지만 음성 VLAN은 VLAN 태깅을 이용하여 서로 다른 서브넷 간에도 브로드캐스팅이 가능하도록 설정한다. 이와 같이 VLAN을 이용한 서브넷 간 로밍 방법은 다수의 인원이 음성통신을 사용하는 경우 브로드캐스팅에 따른 트래픽 부하로 성능이 저하될 수 있는 단점이 있지만 현재 실용화할 수 있는 기술로써 적용 가능하다.

Ⅳ. 결 론

현재 IEEE 802.11 표준 단체에서는 WLAN 기반에서 음성과 같은 실시간 데이터를 전송하기 위한 표준을 제정 중이다. 802.11r에서는 AP 간에 이동시 빠른 로밍 (fast roaming)을 위한 표준 작업과 802.11e에서는 QoS (Quality of Service)를 지원하기 위한 표준화가 진행되고 있다. 또한, IETF에서는 네트워크 계층에서 로밍을 지원하기 위해 Mobile IP 표준을 제정하였지만, 아직도 로밍 시 전송 지연을 해결하기 위해 많은 연구가 진행 중이다. VoWLAN은 이동성에 대한 요구와 VoIP 서비스에 대한 급성장으로 많은 관심을 집중하고 있지만, 음성 품질 및 로밍을 위한 기술은 아직 실용화 단계에 이르지 못하였다.

본 논문에서는 VoWLAN 상에서 로밍 및 보안 문제를 해결하기 위해 음성 VLAN과 데이터 VLAN을 분리하는 방법과 서브넷 간 로밍을 위해 802.1Q VLAN 태깅을 이용하는 방법을 제시하였다. 본 논문에서 제시한 VLAN을 이용한 보안 및 로밍 기능을 제공하기 위한 방법은 음성통신과 데이터통신에 대해 별도의 서브넷 대역을 구분함으로써 사용자에게 불편함을 제공할 수 있다. 그러나 WLAN에서 강력한 보안과 빠른 로밍을 동시에 제공하기 위한 표준의 제정 및 IP 망에서 Mobile IP 기술이 상용화 단계에 이르기까지는 보안과 편리성에 대한 손익상쇄 (trade-off)를 두면서 VoWLAN 시스템을 구현하기 위한 정책이 필요하다.

향후에는 현재 진행되는 802.11r, 802.11e 및 Mobile IP 등에 대한 연구로 VoWLAN 서비스 기술을 향상시킬 수 있는 방법을 연구할 계획이다.

참 고 문 헌

[1] Wei Wang, SoungChang Liew, and Victor O. K. Li, "Solution to Performance Problems in VoIP Over 802.11 Wireless LAN," *IEEE Transactions on* Vehicular technology, vol.54, no.1, pp. 366-384, Jan. 2005.

[2] ANSI/IEEE Std 802.11-1999, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Jun 2003.

[3] IEEE std 802.11i, "Part11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements," July 2004.

[4] Jyh-Cheng Chen, Ming-Chia Jiang, and Yi-wen Liu, "Wireless LAN security and IEEE 802.11i," IEEE Wireless Communications, vol. 12,Issue 1, pp. 27-36, Feb. 2005.

[5] IEEE std 802.1X, "Port-Based Network Access Control," Dec. 2004.

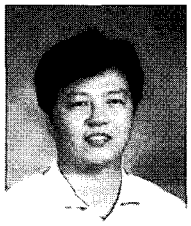
[6] P. Funk and S. Blake-Wilson, "EAP

Tunneled TLS Authentication Protocol (EAP-TTLS)," IETF Internet draft, draft-ietf-pppext-eap-ttls-05.txt, July 2004, work in progress.
[7] Borse, M. and Shinde, H., "Wireless security & privacy," *IEEE International Conference on* Personal Wireless Communications, pp.424-428, Jan. 2005.
[8] 강유성 외, "무선랜 보안 표준 IEEE 802.11i," TTA Journal No.99, pp123-129, 2005년 6월.
[9] Ramsdell B., "S/MIME Version 3 Message Specification," IETF RFC 2633, 1999.
[10] Baugher M., et al., "The Secure Real-time Transport Protocol (SRTP)," IETF RFC 3711, March 2004.
[11] Andreas Steffen, et al., "SIP Security," DFN-Arbeitstagung ber Kommunikationsnetze, pp.397-412, 2004.
[12] IEEE Std 802.1Q, "Virtual bridged local area networks," May 2003.
[13] Sharma, S., Ningning Zhu, and Tzicker Chiueh, "Low-latency mobile IP handoff for infrastructure-mode wireless LANs," *IEEE Journal on* Selected Areas in Communications, Vol. 22, Issue 4, pp643-652, May 2004.

〈著 者 紹 介〉

김 미 연 (Mi Yeon Kim)
정회원

1992년 2월 : 덕성여자대학교 전산학과 졸업
2000년 8월 : 고려대학교 컴퓨터과학기술대학원 공학석사
2005년 3월~현재 : 고려대학교 정보보호대학원 박사과정
1992년 3월~현재 : KT 컴버전스본부 책임연구원
〈관심분야〉 데이터베이스, 무선통신, 정보보호



김 계 진 (Kye Jin Kim)

1995년 2월 : 경북대학교 전자공학과 졸업
1996년 8월 ~현재 : KT 컴버전스본부 선임연구원
〈관심분야〉 무선통신, 정보보호

이 동 훈 (Dong Hoon Lee)
종신회원

1983년 8월 : 고려대학교 경제학사
1987년 12월 : Okahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1993년3월~1997년2월 : 고려대학교 전산학과 조교수
1997년3월~2001년2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술