2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

무선랜 환경에서 로밍을 지원하는 효율적인 보안 방법론

송창열*, 오남호*, 안재영**, 조기환*
*전북대학교 전산통계학과
**한국전자통신연구원 무선접속모뎀연구팀
e-mail : {crsong, nhooh, ghcho}@cs.chonbuk.ac.kr, **jyahn@etri.re.kr

An Efficient Security Mechanism in Support of Roaming in Wireless LAN environment

Chang-Ryeol Song*, Nam-Ho Oh*, Jae-Young Ahn**, Gi-Hwan Cho*
*Dept of Computer Science & Statistics Chonbuk National Univ.
**Wireless Access Modem Research Team, ETRI

요 약

휴대용 컴퓨터의 폭넓은 보급으로 인해 사용자의 이동성을 살린 무선 정보망의 실현 수단으로서 무선 LAN 에 대한 관심이 급증하고 있다. 무선 LAN 이 향후 정보 통신 기반구조로 자리하기 위해서는 사용자의 이동성을 보장하기 위한 효과적인 로밍 기술이 절대적이다. 본 논문에서는 현재 표준화가 진행중인 IEEE 802.1X 를 기반으로 하여 무선 LAN 환경에서 사용자의 안전한 이동성 보장을 위한 서로 다른 도메인 간의 단말 이동을 지원하는 로밍 보안 방법론을 제안한다. 인증 및 키 교환 메커니즘은 EAP-TLS 를 기준으로 하며, 로밍이 발생할 때 TLS 의 핸드쉐이크 과정을 단순화하는 접근을 사용한다.

1. 서론

최근 무선 LAN 시장은 교육, 의료, 금융 등의 분야를 중심으로 빠르게 확대되고 있다. 무선 LAN(Wireless Local Area Network, WLAN)은 직접 선으로 연결하지 않고도 네트워크 망에 연결할 수 있도록 해주는 기술이다. 이는 개방된 공간 같은 물리적으로 선을 연결할 수 없는 장소에서, 또는 회의장 같은 한 꺼번에 여러 개의 장치의 연결이 필요한 장소에서 네트워크에의 접속을 가능하게 해준다.

무선 LAN 은 무선 전송 기술의 이동성, 휴대성 및 간편성 등의 장점으로 인해 그 응용 범위가 점차 확대되어 가고 있다. 또한 무선 LAN 기술의 발전으로 인해 전송속도가 빨라지고 가격이 저렴해짐으로써 무선 LAN 시장은 눈부신 발전을 이루고 있다.

이처럼 무선 LAN 이 미래 정보통신의 주류로 자리매김하는 시점에서 유선에서 제공되는 만큼의 보안성이 제공되지 않는다면 네트워크 관리자들은 무선 LAN 의 사용을 꺼리게 될 것이다.

이동 통신망에서 인접한 셀 사이의 이동에 대해 솔기 없는 네트워크 접속을 지원하는 것을 핸드오프(handoff)라고 하며, 서로 다른 관리 도메인 혹은 서로 다른 기술로 구현된 네트워크 간의 이음매 없는 이동을 지원하는 기술을 로밍(roaming)이라고 한다. 이동 통신망과 마찬가지로 무선 LAN 환경에서도 사용자의 이동성을 보장해주기 위해 단말의 로밍을 지원해주는 기술들이 연구되고 있다. 단말의 원거리 이동에서는 Mobile IP 가 근간 프로토콜로 적용되어 진다.

무선 LAN 의 표준 규격인 IEEE 802.11[1]은 무선 공간에서의 정보보호를 위해 인증(authentication)과 비밀성(privacy)의 보안 서비스를 제공한다. 인증은 무선 단말의 장치 인증을 의미하며, IEEE 802.11 에서는 open system 과 shared key 인증 등 두 가지 타입의 인증 메

커니즘을 제공한다. 그리고 비밀성을 제공하기 위해 WEP(Wired Equivalent Privacy) 알고리즘을 이용한다. 하지만 IEEE 802.11 프로토콜의 경우 장치 인증만을 제공한다는 점과 공유키 이용에 따른 키 분배와 관리 측면에 문제, 그리고 WEP 알고리즘 문제점 등이 있다[2].

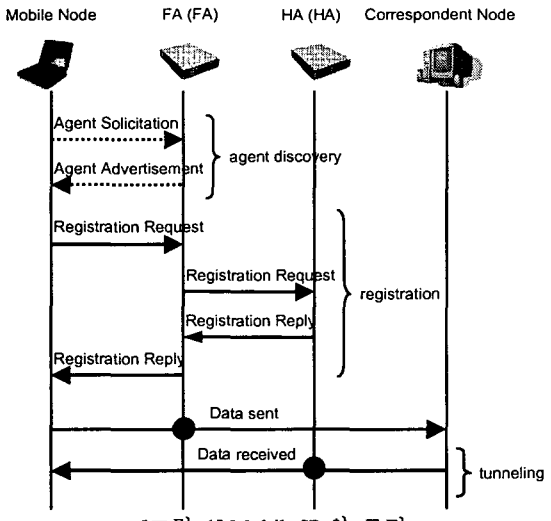
IEEE 802.11Tgi 에서는 무선 LAN 환경에서 이러한 문제를 해결하기 위해 port based access control 과 사용자 인증을 제공하는 IEEE 802.1X[3] 보안 프레임워크를 이용하여 무선 LAN 에서의 정보보호 서비스를 제공하고자 하고 있다. 현재 IEEE 802.11Tgi 에는 상호 인증, 안전한 키 관리 메커니즘 및 로밍 전략 등 향상된 보안 메커니즘을 제공하기 위한 여러 가지 방안이 제안되고 있다.

본 논문은 IEEE 802.1X 보안 프레임 워크와 IEEE 802.11Tgi 에 제안된 EAP-TLS(Extensible Authentication Protocol-Transport Layer Protocol)를 이용한 상호인증 및 키 분배 메커니즘을 토대로 무선 LAN 환경에서 서로 다른 도메인으로 로밍시에 이루어져야 하는 TLS 인증 과정에서 핸드쉐이크의 단순화된 방법으로 무선 단말의 이동성을 효과적으로 지원하는 보안 방법론을 제안한다.

본 논문은 구성은 다음과 같다. 2 장에서는 Mobile IP 의 로밍 전략에 대하여 설명하고, 3 장에서는 무선 단말과 AP 사이에서 상호인증과 공유 키 분배를 위한 EAP-TLS 메커니즘에 대하여 설명한다. 4 장에서는 2 장과 3 장의 내용을 토대로 무선 단말의 로밍을 지원하는 보안 방법론을 제시한다. 5 장에서는 결론을 내린다.

2. Mobile IP 의 로밍[4]

Mobile IP 는 인터넷에서 노드의 이동성을 지원하기 위한 IETF(Internet Engineering Task Force)의 표준 프로토콜이다. [그림 1]은 Mobile IP 에서의 로밍 지원을 설명하고 있다.

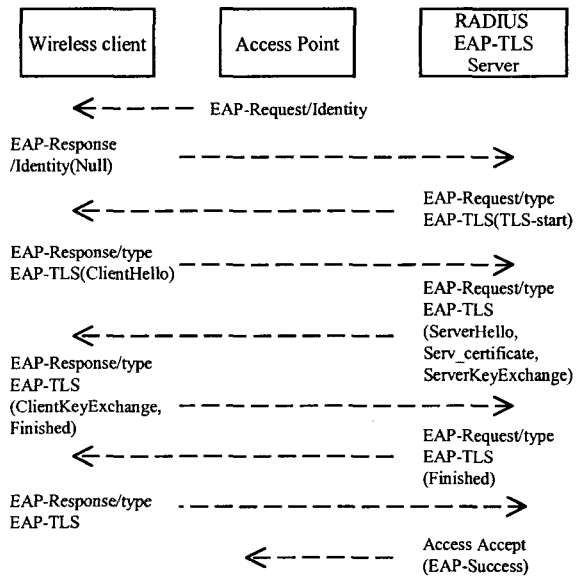


[그림 1] Mobile IP 의 로밍

이동 단말의 로밍은 단말이 이동성 에이전트인 HA 나 FA 가 전송하는 advertisement 메시지를 감지하거나, 자신이 solicitation 메시지를 브로드캐스트하여 FA 를 찾는 것으로 시작한다. 이와 같은 agent discovery 과정을 통한 FA 의 브로드캐스트 메시지로부터 이동 단말은 새로운 COA(Care-of Address)를 획득한다. 새로운 도메인으로 이동한 이동 단말은 이동성 에이전트에 등록 요청 메시지와 등록 응답 메시지를 교환하는 registration 과정을 수행한다. 이 때 이동 단말의 새로운 COA 를 HA 에 등록한다. HA 는 이동 단말과 이동 단말의 새로운 COA 를 짝지어 바인딩 테이블을 만들고 FA 에 등록 응답 메시지를 보냄으로써 tunneling 을 준비한다. HA 와 FA 사이에 등록이 성공적으로 이루어지면 외부에서 이동 단말의 홈 주소로 보내어지는 데이터그램은 HA 에 의해 이동 단말의 COA 로 tunneling 된다.

3. EAP-TLS 를 이용한 인증 및 키 분배[5]

EAP-TLS 를 이용한 인증 메커니즘은 이동 단말과 네트워크와의 상호 인증과 또한 무선 LAN 에서 비밀성 제공을 위해 사용되는 암호화에 필요한 키 분배 메커니즘을 기술하고 있다. EAP-TLS 를 이용한 인증 메커니즘은 [그림 2]와 같이 네트워크 인증과 클라이언트 인증의 수행에 의해 수행된다.



[그림 2] EAP-TLS 사용자 인증 절차

인증 서버는 TLS-Start 메시지를 통해 상호 인증 절차의 시작을 무선 단말에 알리고 무선 단말은 키 교환에 필요한 랜덤 넘버를 생성한 후 ClientHello 를 인증 서버에 보낸다. ClientHello 를 받은 인증 서버는 키 교환을 위한 랜덤 넘버 생성 후 단말의 서버 인증을 위하여 서버의 인증서를 포함하는 ServerHello 를 무선

단말에 전송한다. 서버의 인증서를 받은 무선 단말은 서버를 인증하고 자신이 생성한 랜덤 넘버와 서버의 랜덤 넘버 그리고 pre-master secret 을 이용하여 마스터 키를 생성한다. 그리고 나서 무선 단말은 서버로부터 받은 인증서의 public key 로 pre-master secret 를 암호화하여 ClientKeyExchange 메시지에 넣어 인증 서버에 전송한다. 인증 서버는 ClientKeyExchange 메시지에서 pre-master secret 를 추출하고 이것을 이용하여 서버에서도 마스터 키를 생성한다.

TLS 의 핸드쉐이크 메커니즘을 이용하여 무선 단말과 인증 서버 사이에 상호 인증을 완료한 후 인증 서버는 인증 성공 메시지와 함께 생성된 마스터 키를 AP 에게 전송한다. 무선 단말과 AP 는 마스터 키를 서로 공유하고 이를 이용하여 암호 키를 전송한다.

4. 로밍을 지원하는 보안 방법론

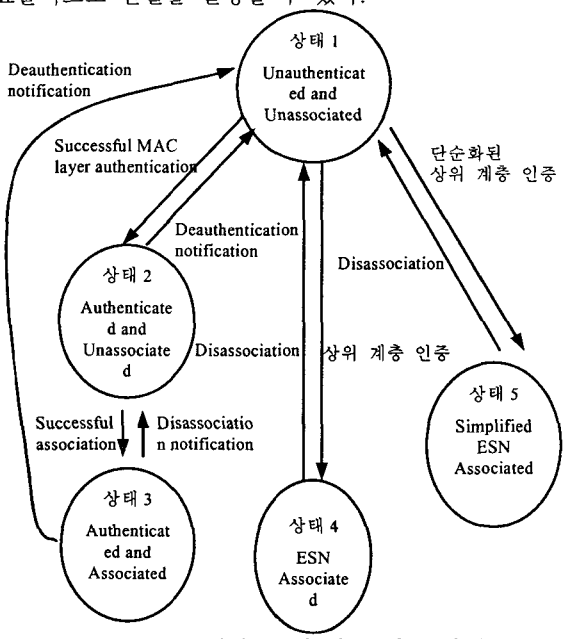
무선 LAN 에서 다른 도메인의 AP 로 이동하는 무선 단말의 이동성을 지원하기 위한 방법으로 Mobile IP 프로토콜을 사용한다. 이 때 새로운 AP 로 이동한 단말의 안전한 통신을 위해서는 단말의 등록이 이루어지기 전에 인증 과정을 거쳐야 한다. 하지만 새로운 도메인에서 또다시 기존의 EAP-TLS 의 핸드쉐이크 과정을 통하여 인증하는 과정은 로밍하는 단말의 인증에 많은 지연을 유발한다.

따라서 기존의 핸드쉐이크 인증보다는 간단하고 최적화된 TLS[6]의 단순화된 핸드쉐이크를 적용하여 절차의 간소화 및 메시지의 양을 줄이는 것이 절대적이다.

4.1 인증 절차가 포함된 무선 LAN 의 로밍

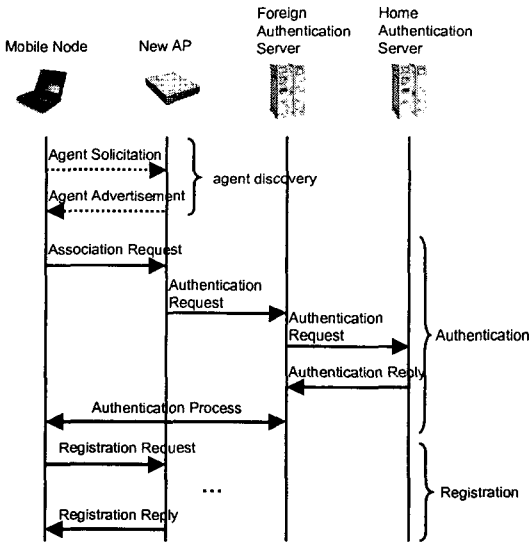
서로 다른 도메인으로 이동한 단말은 새로운 AP 의 advertisement 를 통해 새로운 도메인에 있음을 감지하게 된다. 그리고 난후 단말은 새로운 AP 에 associate 또는 re-associate 메시지를 보낸다. 이 때 associate 또는 re-associate 메시지에는 자신의 홈 도메인 ID 를 함께 실어 단말의 홈 도메인 영역을 AP 가 알 수 있도록 한다. 단말의 associate 또는 re-associate 메시지를 받은 AP 는 도메인 ID 에 따라 단말을 인증할 메커니즘을 선택하게 된다. [그림 3]은 도메인 ID 에 따라 선택될 수 있는 다른 인증 메커니즘들을 보여주고 있다.

도메인 ID 정보에 따라 현 도메인을 홈 도메인으로 하는 단말의 경우 상태 1 에서 상태 2, 상태 3 으로의 지역적인 장치 인증을 수행한다. 즉 하나의 도메인 내에서 핸드오프를 수행하는 단말의 경우 장치 인증만으로 단말의 빠른 인증을 수행한다. 처음 등록을 수행하는 단말의 경우 상태 1 에서 상태 4 로의 상위 계층 인증을 수행한다. 이것은 기존의 802.11 의 인증보다 향상된 보안 서비스를 지원하는 ESN(Enhanced Security Network)에서 802.1X 를 이용한 상호 인증 메커니즘을 의미한다. 이동 단말이 새로운 도메인으로 로밍할 경우에는 기존의 홈 도메인에서 수행했던 상태 1 에서 상태 4 로의 인증을 수행하지 않고, 홈 인증 서버를 이용한 상태 1 에서 상태 5 로의 단순화된 상위 계층 인증을 수행함으로써 단말의 로밍시에 좀 더 빠르고 효율적으로 연결을 설정할 수 있다.



[그림 3] 도메인 ID 에 따른 인증 선택

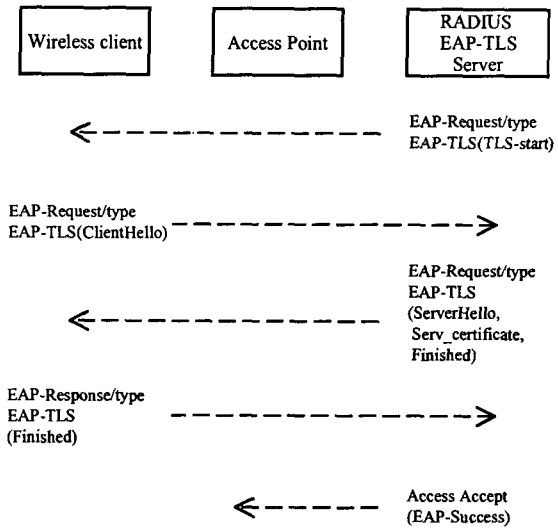
[그림 4]는 홈 도메인에서 다른 도메인으로 로밍한 이동 단말이 상태 1 에서 상태 5 로의 단순화된 상위 계층 인증을 수행하기 위해 홈 도메인의 인증 서버에 단말의 인증 정보를 요청하는 과정을 보여준다. 홈 도메인의 인증 서버는 단말의 인증 정보를 요청한 도메인의 인증 서버에 전송하고 그 인증 정보를 토대로 단말의 인증 과정을 수행한다. 인증이 성공하면 이동 단말은 등록 절차를 수행하고 인증이 실패하면 단말의 새로운 AP 에 대한 접근을 거부한다.



[그림 4] 인증 절차가 포함된 무선 단말의 로밍

4.2 단순화된 상위 계층 인증 및 키 관리

[그림 5]는 단말의 인증을 [그림 3]의 상태 1 에서 상태 5 로의 단순화된 상위 계층 인증을 통하여 수행할 경우에 사용되는 상호 인증과 키 분배 메커니즘을 보여주고 있다.



[그림 5] 단순화된 상위 계층 인증 절차

홈 도메인의 인증 서버로부터 단말의 인증 정보를 받은 현 도메인의 인증 서버는 이동 단말과의 상호 인증 과정 및 키 분배 과정을 수행하기 위해 EAP-TLS Start 메시지를 이동 단말에 전송한다. EAP-TLS Start 메시지를 받은 이동 단말은 ClientHello 메시지를 인증 서버에 전송한다. 인증 서버는 ClientHello 메시지의 client key id 의 정보로부터 이동 단말의 인증서를 획득한다. 이것은 단말과 인증 서버의 인증서에 공유키를 구할 수 있는 정보가 포함되어 있을 때 가능한데 이 단말의 경우 홈 도메인의 인증 서버와 이미 상호 인증을 통해 공유키를 가지고 있으며 현 도메인의 인증 서버는 홈 도메인의 인증 서버로부터 인증 정보를 넘겨 받을 때 이 정보를 넘겨 받기 때문에 이 절차를 수행할 수 있다.

인증 서버는 단말의 인증서로부터 단말을 인증하고 공유키를 pre-master secret 으로 사용하여 새로운 마스터 키을 생성한다. 그리고 서버 인증을 위해 서버에 자신의 인증서를 전송한다. 이동 단말은 서버의 인증서로부터 서버를 인증하고 서버와 마찬가지로 마스터 키를 생성한다.

이동 단말과 인증 서버와의 상호 인증이 성공하면 인증 서버는 AP 에 단말과의 인증과정에서 생성된 마스터 키를 전송하고 AP 는 단말과 무선 채널 상에서의 안전한 통신을 위한 암호키를 생성한다. 그리고 나서 암호키를 마스터 키로 암호화하여 단말에 전송한다. 이 후에 단말과 AP 사이에서의 전송되는 데이터는 암호키를 이용하여 암호화 되어진다.

이와 같은 인증 과정은 EAP-TLS 의 메커니즘의 핸드쉐이크에 의한 상호 인증에 비해 최적화된 인증 과정으로서 인증 절차를 간소화하고 메시지의 크기를 줄인다. 따라서 단말이 새로운 AP 에서 서비스를 받기 위한 전체 등록 과정에 이동 단말과 인증 서버 사이에 인증 과정이 미치는 영향을 줄이고, 무선 채널상에서 인증에 필요한 메시지의 양을 줄임으로써 좀 더 빠르고 효율적인 로밍을 지원해 줄 수 있다.

4.3 보안성 검토

단순화된 상호 인증은 기존의 핸드쉐이크를 거친 인증 주체들이 공유키를 가지고 있을 때 가능하다. 단말이 이동한 도메인의 인증 서버는 단말의 홈 인증 서버로부터 인증 정보를 요청하여 받을 때 이 정보를 획득하게 된다. 따라서 이동 단말과 인증 서버 사이에는 공유키를 가지게 되고 단순화된 상호 인증을 수행할 수 있다. 이는 홈 인증 서버와 새로운 도메인의 인증 서버 사이에 보안이 안전하다고 가정한다. 그러므로 무선 채널 상에 전송될 인증 정보의 양을 줄임으로써 외부의 위협으로부터 인증 정보의 유출로 인한 공격 가능성을 줄일 수 있다.

암호키의 오랜 사용을 방지하기 위해 이동 단말은 이동한 도메인의 인증 서버와 새로운 마스터 키를 공유하고 새로운 암호키를 생성해서 무선 채널상의 트래픽을 암호화하기 때문에 키 유출에 의해 발생할 수 있는 문제점을 극복할 수 있다.

5. 결론

본 논문에서는 서로 다른 도메인 영역을 이동하는 무선 단말의 로밍을 지원하기 위해 EAP-TLS 의 핸드쉐이크를 통한 상호 인증 절차가 아닌 홈 인증 서버를 이용한 단순화된 핸드 쉐이크 인증 절차를 수행한다. 이를 통해 이동 단말과 인증 서버 사이에 좀 더 빠르고 안전한 상호 인증과 키 분배를 수행한다.

이와 같이 인증 절차에 소요되는 시간의 단축과 무선 상에서 오가는 인증 정보의 양의 축소를 통해 이동 단말의 빠르고 안전한 로밍을 지원하게 된다.

향후 무선 LAN 이 본격적으로 활용되는 시점에서 단말의 로밍을 지원하기 위한 보안 방법론의 기초를 제공할 것으로 기대된다.

참고문헌

[1] Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications, *IEEE*, 1999

[2] S. Miller, "Facing the challenge of wireless security," *IEEE Computer*, vol 34(7), pp. 16-18, Jun., 2001

[3] "Standard for Local and Metropolitan Area Network: Standard for Port based Network Access Control," *IEEE draft P802.1X/D11*, Mar., 2001

[4] C. Perkins, "IP Mobility Support," *IETF RFC 2002*, Oct., 1996

[5] "Serial Authentication using EAP-TLS and EAP-MD5," *IEEE draft*, Jul., 2001

[6] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," *IETF RFC* 2246, Jan., 1999