무선랜 환경에서 Proactive Handoff를 위한 보안 방법론

오남호[0] 정병호* 조기환
전북대학교 전산통계학과
*한국전자통신연구원 무선인터넷보안연구팀
{nhooh, ghcho}@cs.chonbuk.ac.kr, *cbh@etri.re.kr

A Security Mechanism in support of Proactive Handoff in Wireless LAN Environment

Nam-Ho Oh[0] Byung-Ho Chung* Gi-Hwan Cho
Dept. of Computer Science & Statistics, Chonbuk National Univ.
*Wireless Internet Security Research Team, ETRI

요 약

휴대용 컴퓨터가 널리 보급됨에 따라 장소에 상관없이 네트워크 망에 연결시킬 수 있는 수단으로 무선 랜의 필요성이 증대되고 있다. 이에 따른 정보보호 문제 또한 중요한 현안으로 대두되고 있다. 현재 IEEE 802.1X를 중심으로 무선랜에서의 향상된 정보보호 솔루션을 제공하기 위한 노력이 진행 중에 있다. 하지만, 무선 랜 환경에서 안전하고 빠른 handoff를 지원해 주기 위한 방안은 부족한 상황이다. 이러한 필요성에 따라 본 논문에서는 무선 LAN환경에서 빠른 handoff를 제공하는 Proactive handoff를 지원하기 위한 안전한 보안 방법론을 제안한다. 이 때 키 교환 메커니즘으로 EAP-TLS를 이용한 방법을 토대로 한다.

1. 서 론

무선 전송 기술은 전파를 정보의 전송 매체로 이용하는 기술로, 사용자의 위치에 상관없이 용이하게 정보를 전송할 수 있는 이동성, 휴대성 및 간편성 등으로 인해 그 응용 범위가 점차 확대되어 가고 있다. 그 중에서도 무선 LAN (Wireless Local Area Network, WLAN)은 무선 전송 기술을 통해 기존의 유선 LAN에서의 미비점을 보완하고, 유선 LAN의 설치가 어려운 환경에까지 무선 채널을 통해 LAN을 확장하는 기술이라고 정의할 수 있다.

무선 LAN이 가지는 이점들과 휴대용 컴퓨터의 폭넓은 보급으로 인해 이동성을 살린 무선 정보망의 실현 수단으로서 무선 LAN에 대한 관심이 급증하고 있다. 그러나 무선 LAN은 데이터 전송 속도가 유선 LAN에 비해 느리고, 아직은 초기 설치 비용이 고가이며 정보의 전송 매체가 전파인 관계로 정보보호에 매우 취약하다는 단점이 있다.

이동 통신망과는 달리 무선 LAN은 현재 이동 단말의 로밍을 제대로 지원해주지 못하고 있다. 특히 local에서의 handoff의 경우 등록에 따른 delay가 많기 때문에 빠른 handoff를 지원하기 위해 Proactive handoff[1]와 같은 방법이 제안되고 있다.

무선 LAN의 표준 규격인 IEEE 802.11[2]에서는 무선 공간에서의 정보보호를 위해 인증(authentication)과 비밀성(privacy)의 보안 서비스를 제공한다. 인증은 무선 단말의 장치 인증을 의미하며, open system과 shared key 인증 등 두 가지 타입의 인증 메커니즘을 제공한다. 그리고 비밀성을 제공하기 위해 WEP(Wired Equivalent Privacy) 알고리즘을 이용한다.

하지만, IEEE 802.11 프로토콜의 경우 장치 인증만을 제공한다는 점과 shared key를 이용에 따른 키 분배와 관리 측면에 문제, 그리고 WEP 알고리즘 문제점 등이 있다.

IEEE 802.11Tgi에서는 이러한 문제를 해결하기 위해 port based access control과 사용자 인증을 제공하는 IEEE 802.1X[3]를 이용하여 IEEE 802.11에서의 정보보호 서비스를 제공하고자 하고 있다. 현재 IEEE 802.11Tgi에는 상호 인증, 안전한 키 관리 메커니즘 및 로밍 전략 등 향상된 보안 메커니즘을 제공하기 위한 여러 가지 방안이 제안되고 있다.

본 논문은 무선 LAN 환경에서 local에서 이동하는 단말의 빠른 handoff를 제공하는 Proactive handoff를 지원하기 위한 보안 방법론을 제안한다. 이에 필요한 키 관리 메커니즘은 IEEE 802.11Tgi에 제안된 무선 LAN에서의 향상된 키 교환 메커니즘인 EAP-TLS[4]를 토대로 한다.

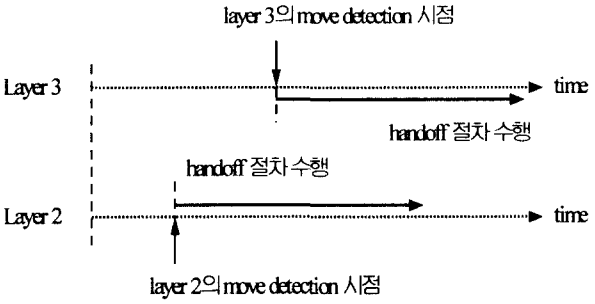
본 논문의 구성은 다음과 같다. 2장에서는 Proactive handoff 에 대해 설명하고, 3장에서는 EAP-TLS 메커니즘의 상호 인증 및 키 분배 방법을 설명한다. 4장에서는 2장과 3장에서 설명된 메커니즘을 이용하여 무선 LAN환경에서 이동하는 단말의 proactive Handoff를 지원하는 보안 방법론을 제시한다. 5장에서는 결론에 대해 논의한다.

2. Proactive handoff [1]

Proactive handoff는 local에서 이동하는 무선 단말의 빠른 handoff를 제공하기 위한 fast handoff 메커니즘이다.

기존의 handoff는 방법은 이동 단말이 local에서 이동할 때 layer 3에서의 move detection 전략에 의해 이동 단말의 이동 사실을 탐지하여 handoff 절차를 수행하였다. 하지만 단말이 handoff 절차를 마치고 새로운 AP에 등록될 때까지 많은 delay를 요구하기 때문에 서비스의 단절 현상이 발생하게 되어 단말의 빠른 handoff를 지원할 수 없었다.

Proactive handoff는 위와 같은 문제점을 해결하기 위해 [그림 1]과 같이 무선 단말의 이동에 대한 탐지를 layer 2에서 한다. Layer 2에서의 이동에 대한 탐지는 layer 3보다 빨리 이루어지기 때문에 layer 3에서의 handoff 절차가 수행되는 시점보다 좀 더 빠른 시점에서 단말의 handoff가 수행된다. 따라서 local에서 이동하는 단말의 빠른 handoff를 제공하여 서비스의 단절 현상을 줄일 수 있게 된다.

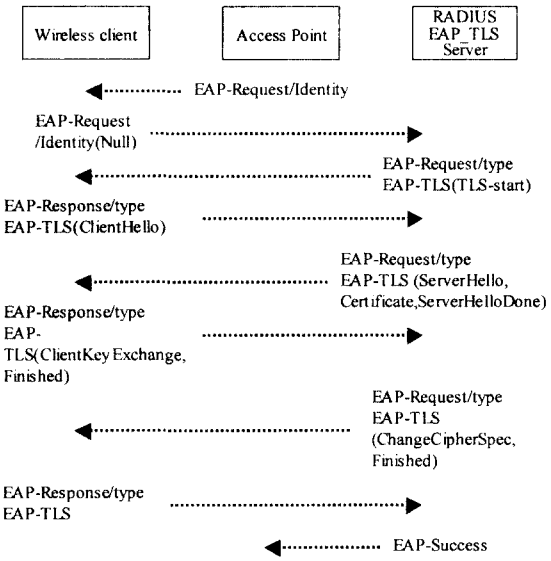


[그림 1] Proactive handoff 절차

3. EAP-TLS를 이용한 인증 및 키 분배 [4]

EAP-TLS를 이용한 인증 메커니즘은 이동 단말과 네트워크와의 상호 인증과 또한 무선 LAN에서 비밀성 제공을 위해 사용되는 암호화에 필요한 키 분배 메커니즘을 기술하고 있다.

EAP-TLS를 이용한 인증 메커니즘은 [그림 2]와 같이 네트워크 인증과 클라이언트 인증의 수행에 의해 수행된다. 인증 서버는 TLS-Start 메시지를 통해 상호 인증 절차의 시작을 무선 단말에 알리고 무선 단말은 키 교환에 필요한 랜덤 넘버를 생성한 후 ClientHello를 인증 서버에 보낸다. ClientHello를 받은 인증 서버는 키 교환을 위한 랜덤 넘버 생성 후 서버 인증을 위해 ServerHello와 서버의 인증서를 무선 단말에 전송한다. 서버의 인증서를 받은 무선 단말은 서버를 인증하고 자신이 생성한 랜덤 넘버와 서버의 랜덤 넘버 그리고 "master secret"라는 string을 pre-master secret으로 이용하여 master secret을 생성한다. 그리고 나서 무선 단말은 pre-master secret을 서버로부터 받은 인증서의 public key로 암호화 하여 ClientKeyExchange 메시지에 넣어 인증 서버에 전송한다. 인증 서버는 ClientKeyExchange 메시지에서 pre-master secret를 추출하고 이것을 이용하여 서버에서도 master secret



[그림 2] EAP-TLS 인증 메커니즘의 상호인증 절차

을 생성한다.

TLS(Transport Layer Security)의 handshake 메커니즘을 이용하여 무선 단말과 인증 서버 사이에 상호 인증을 완료한 후 인증 서버는 생성된 master secret를 AP에 Success 메시지와 함께 전송한다. 무선 단말과 AP는 master secret을 서로 공유하고 이를 이용하여 encryption 키를 전송한다.

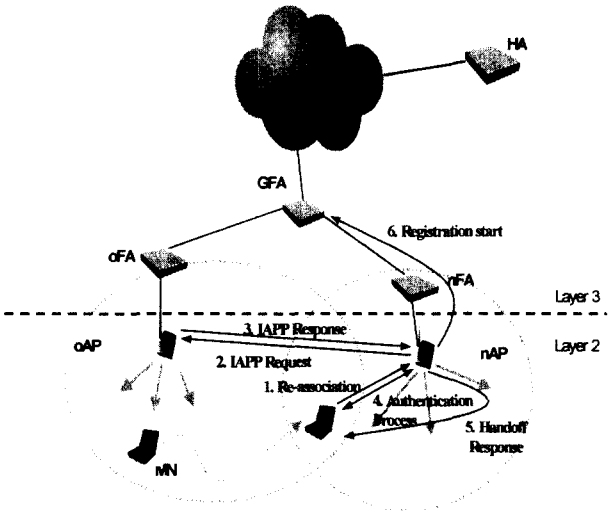
4. Proactive handoff를 지원하는 보안 방법론

Proactive handoff는 빠른 로밍을 위해 layer 2에서 단말의 이동을 탐지하여 handoff를 미리 진행하는 방법이다. 하지만 단말이 서비스를 받는 AP에서 수행된 EAP-TLS의 인증 절차를 그대로 수행할 경우 많은 registration delay를 유발하기 때문에 빠른 handoff를 지원하기 위해 Proactive handoff의 기본 취지에 위배된다. 따라서 이와 같은 Proactive handoff를 안전하게 수행할 수 있도록 하기 위해서는 단말의 인증 절차 또한 간소화되어야 한다.

4. 1. 인증 절차가 포함된 Proactive handoff

[그림 3]은 인증 절차가 포함된 Proactive handoff 과정을 설명하고 있다.

먼저, 무선 단말이 new AP의 서비스 영역과 old AP와의 서비스 영역 교차점으로 이동했을 때 new AP의 beacon을 통해 layer 2에서의 단말 이동을 탐지하게 된다. 이동 단말은 new AP로의 handoff를 위해 handoff request를 new AP에게 보낸다. new AP는 이동 단말의 request로부터 old AP의 주소를 얻어 old AP에게 이동 단말의 정보를 요청한다. 요구되는 정보에는 이동 단말의 인증 정보를 포함한다.



[그림 3] 인증 절차가 포함된 Proactive handoff

이 때 AP와 AP사이에서의 인증 정보 교환은 IAPP(Inter Access Point Protocol) [5]를 이용한다. IAPP는 서로 다른 AP 사이에서의 정보 교환을 위해 사용되는 프로토콜로서 layer 2에서의 사용자 정보를 교환한다. 이 때 AP와 AP 사이에서 이루어지는 정보의 교환은 안전하게 이루어진다고 가정한다.

old AP로부터 인증 정보를 넘겨 받은 new AP는 이 정보를 토대로 이동 단말을 인증한다. 인증이 성공하면 new AP는 이동 단말에게 handoff response를 전송하고 layer3의 등록을 시작한다.

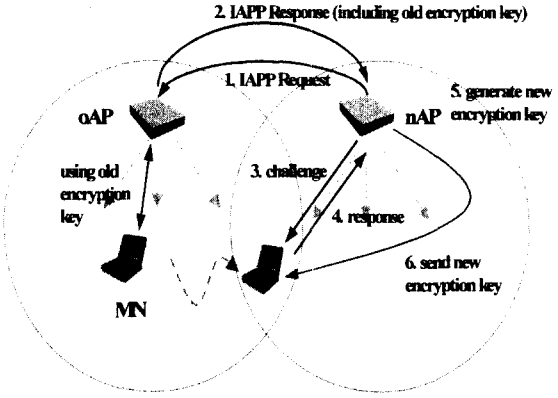
4. 2. 인증을 위한 키 교환 및 관리

Proactive handoff는 local에서 단말의 이동할 때 서비스의 단절 현상을 최소한으로 줄이기 위한 방법이므로 인증 절차 또한 간소해야 한다. 따라서 이동 단말이 old AP에서 3장에서와 같은 EAP-TLS를 이용한 상호인증 절차를 new AP에서 수행할 경우 많은 delay를 유발하기 때문에 바람직하지 못하다.

단말이 local에서 이동할 경우 이미 인증 서버와의 상호인증 절차를 수행하였기 때문에 이동 단말이 새롭게 인증 서버를 인증하지 않아도 된다. 따라서 이동 단말이 인증 서버를 인증하는 절차를 생략한다. 그리고 단말에 대한 인증은 old AP에서 AP와 단말사이에 비밀성 보장을 위해 사용한 encryption 키를 이용하여 shared key 인증을 수행한다.

[그림 4]와 같이 new AP가 old AP로 IAPP request를 보내면 old AP는 IAPP response에 이동 단말의 encryption 키를 포함시킨다. 이동 단말의 정보를 받은 new AP는 이동 단말에 challenge를 보내고 이동 단말은 old AP에서 사용한 encryption 키를 이용하여 response한다. new AP는 old AP로부터 받은 이동 단말의 encryption 키를 이용하여 단말을 인증하고 새로운 encryption 키를 생성하여 기존의 encryption 키로 암호화해서 이동 단말에게 전송한다.

EAP-TLS의 인증절차에서 단말과 AP 사이의 대칭키 전송



[그림 4] 인증 절차 및 키 분배

을 위해 session 키가 사용된다. 이 키는 EAP-TLS의 full handshake를 통해 얻어지기 때문에 이동 단말만의 인증 과정을 통해서는 shared secret을 얻을 수 없다. 따라서 old AP와 이동 단말이 공유하는 encryption 키를 new AP와 이동 단말 사이의 session 키로 사용한다. session 키는 AP와 단말 사이에서 encryption 키를 안전하게 전송하기 위해 서만 사용되기 때문에 new encryption 키를 전송하기 위해 사용된 old encryption 키는 폐기된다.

AP는 자신의 서비스 영역 안에 있는 모든 단말의 encryption 키를 관리하며 새롭게 등록한 단말과의 비밀성 유지를 위해 encryption 키를 새롭게 생성한다.

5. 결론

본 논문에서는 Proactive handoff를 지원하기 위해 local에서 이동 시에는 EAP-TLS을 통한 상호인증을 수행하지 않고 shared key 인증을 통한 단말의 인증만을 수행한다. 이와 같이 인증 절차에 소요되는 시간을 단축시킴으로써 단말의 빠른 handoff를 제공하기 위한 Proactive handoff를 안전하게 수행하게 된다.

향후 무선 LAN이 본격적으로 활용되는 시점에서 fast handoff를 지원하기 위한 보안 방법론의 기초를 제공할 것으로 기대된다.

참고 문헌

[1] P. Calhoun, et. al, "Foreign Agent Assisted Hand-off," *IETF draft*, draft-calhoun-mobileip-proactive-fa-01.txt , Jun., 2000

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

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

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

[5] "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," *IEEE draft*, Jan., 2001