이동 Ad-Hoc 네트워크에서 임시 인증서를 사용한 사용자 식별 및 인증 프로토콜

진병욱*, 조인희*, 한민기*, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
e-mail: Wlsquddnr@ssu.ac.kr

User Identification and Authentication Protocols Using a Temporary Certificate in Mobile ad-hoc network

Byung-Wook Jin*, In-Hee Jo*, Min-gi Han* ,Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

이동 Ad-Hoc 네트워크는 고정된 기반 망의 도움 없이 이동 노드들 간에 자율적으로 구성되는 망으로서, 모바일 노드 자체적으로 연결이 설정된 무선 네트워크이다. 이러한 이동 Ad-Hoc 네트워크는 유선 네크워크에 비해 보안에 매우 취약하여 네트워크 가입자에 대한 인증과 이동 Ad-Hoc 네트워크에 대한 인증이 매우 취약하다. 또한 사용자의 식별이 보호되지 않는다. 본 논문에서 제안하는 인증 프로토콜은 모바일 네트워크 인증서버가 분배한 임시 인증서를 사용하여 사용자의 식별하고 인증한다.

1. 서론

이동 Ad-Hoc 네트워크는 고정된 기반 망의 도움 없이 이동 노드들 간에 자율적으로 구성되는 망으로서, 네트워크에 자율성과 융통성을 부여한 네트워크이다[1]. 이동 Ad-Hoc 네트워크를 구성하는 노드들은 무선 인터페이스를 가지며, 이동 컴퓨팅 기능을 가진 호스트와 라우팅 기능을 가진 라우터를 동시에 만족하는 형상으로 흔히 모바일 노드로 불려진다.

이동 Ad Hoc 네트워크는 무선 인터페이스를 사용하기 때문에 유선 네트워크에 비해 훨씬 더 많은 위험에 노출되어 있다[2]. 그러므로, 기본적인 Ad-Hoc 네트워크의 보안 요구조건은 다른 통신 네트워크에서 요구되는 것과 동일하지만, 이동 Ad-Hoc 네트워크에서는 노드가 신뢰받은 인증기관을 통해 인증을 받는 형식이 아니기 때문에, 멀티홉 방식에 의해 라우팅을 수행할 경우 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 특히, 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로, 암호키에 크게 의존하게 된다. 한편으로, 보안 문제가 확실히 해결되다보면, 컴퓨팅 문제가 발생되어, 노드와 네트워크 전체에 심각한 부하를 주게 되므로, 이동 Ad-Hoc 네트워크에 적합하게 구현된 알고리즘, 키 분배 및 인증 프로토콜의 개발이 현실적으로 가장 필요하다[3]. 즉, 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 이동 Ad-Hoc 네트워크 전반에 분배하는 것이 주요 관심 사항이라 할 수 있다.

본 논문에서는 이동 Ad-Hoc 네트워크에서 무선 보안에서 사용되는 EAP-TLS 프로토콜을 개선하여 사용자의 식별을 보호하고 더욱더 안전한 인증을 위한 프로토콜을 제안한다. 본 논문은 사용자의 식별 값을 다른 모바일 노드에게 보내지 않고 임시 식별 값으로도 사용자가 인증이 되는 구조이며, 이동 Ad-Hoc 네트워크의 가입자 관리를 모바일 네트워크 인증 서버가 관리함으로써 더욱더 안전한 인증프로토콜을 제안한다.

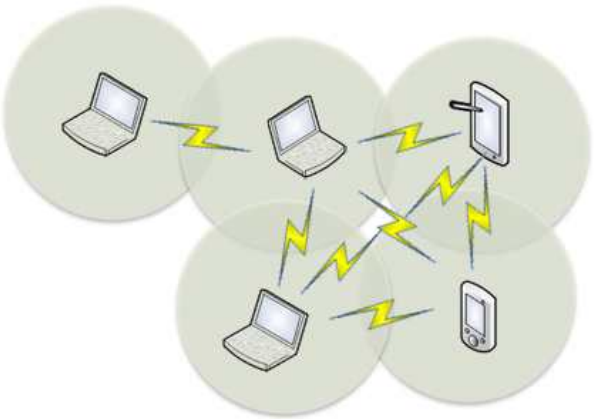
본 논문의 2장에서는 이동 Ad-Hoc과 모바일 네트워크의 구성 및 EAP-TLS 프로토콜에 대한 기술과 문제점에 대해 제시하고 이를 해결하기 위해 3장에서는 이동 Ad-Hoc 네트워크에서 임시 인증서를 사용한 사용자 식별 및 인증 프로토콜을 제안한다. 그에 따른 분석과 효과를 4장에서 제시하고 본 논문을 통하여 나온 결과를 분석하여 5장 결론을 맺는다.

2. 관련연구

2.1. 이동 Ad-Hoc 네트워크

기존의 유무선 네트워크와는 달리 이동 Ad-Hoc 네트워크는 주로 무선 네트워크에서 사용되는 기술이다. Ad-Hoc 네트워크는 BS나 AP와 같은 중재자가 없이 이동 노드들 간에 자체적으로 연결이 설정되어 있는 네트워크 구조이다[4]. 무선으로 통신이 가능한 노드들끼리 서로 통신을 하는 자율적인 구조의 네트워크로서 중간에서 제어하는 노드가 없으므로 각 노드들은 자신이 가질 수가 있는 정보를 최대한 활용하여 네트워크에서 통신해야 하고 먼 거리의 노드와의 통신에는 다른 노드를 경유하여 통신한다[5]. 특히, 기반망에서 계층적이고 수동적인 이동 노드는 이동 Ad-Hoc 네트워크에서는 대등하고 능동적인 망의 주체가 된다.

[그림 1]은 이동 노드 간에 자율적이고 즉흥적인 연결 설정을 가지는 이동 Ad-Hoc 네트워크를 나타낸다.



[그림 1] 이동 Ad-Hoc 네트워크

이동 Ad-Hoc 네트워크가 인터넷 또는 이동 통신망 등의 기반 망과 구별되는 가장 큰 특징은 고정된 중재자의 도움 없이 자율적으로 망의 구성이 가능하며, 고정된 라우터가 존재하지 않아 이동 노드간의 협력에 의한 라우팅 기능이 제공되며, 특정 서비스 제공자가 없이 단말에서 서비스가 해결되어야 한다는 점이다.

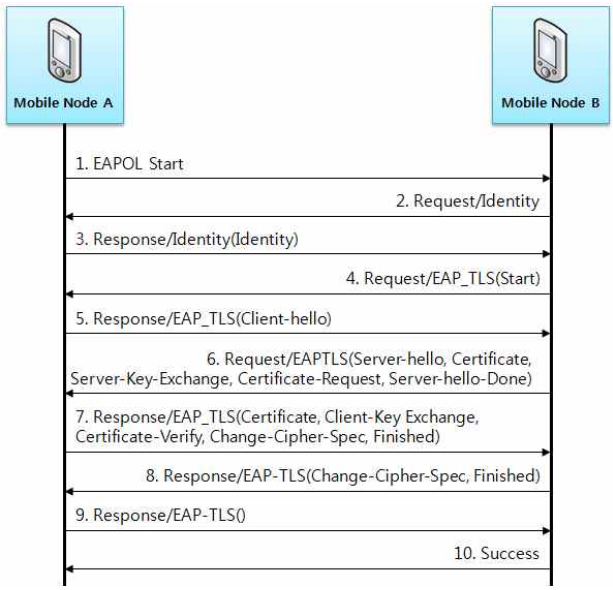
하지만 이러한 장점은 인증적인 문제에서는 단점으로 작용한다. 중앙적인 통제로부터 독립되어 있기 때문에 기존의 인증서비스를 접목시키는 것이 매우 어렵게 된다[2]. 또한 안전한 Ad-Hoc 네트워크인지에 대한 판단이 불확실해지고 새로운 Ad-Hoc 네트워크에 가입하려는 모바일 노드에 대한 검증하는 것이 매우 어렵다.

2.2. EAP-TLS 프로토콜

EAP(Extensible Authentication Protocol)은 IEEE에서 정의하는 보안 프레임워크 802.1X로 정의되어 있다[9]. EAP-TLS 표준은 PPP, 무선랜 서비스, 모바일 네트워크 서비스 등에서 널리 사용되는 인증 프로토콜로 제안된 EAP의 내부 인증 방식 중 하나로 TLS를 사용하기 위하여 제안되었다.

네트워크가 진화하고 다양한 공격방식이 시도됨에 따라, PPP, IEEE 802.11 기반의 무선랜, 3GPP등의 다양한 네트워크에 사용자가 안전한 접근을 할 수 있도록 상호 인증이 필요하게 되었으며, 네트워크상에서 주고받는 데이터에 대한 기밀성 및 무결성을 보장 받기 위해 키 교환 기능이 추가적으로 필요하게 되었다[6]. TLS는 기존의 인터넷에서 TCP 채널 보안을 위해 사용되어 왔으며 상호 인증 및 키 교환 기능을 지원하고 있다. 그러므로 EAP의 인증 방식으로 TLS를 사용하기 위해 TLS의 하위 프로토콜이 TCP가 아닌 EAP로 변경하면서 생키는 차이점을 반영하기 위해 표준을 구성하였다.

[그림 2]은 EAP-TLS 프로토콜의 동작과정을 나타낸다.



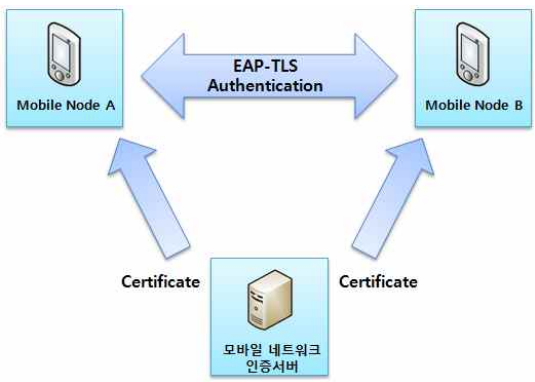
[그림 2] EAP-TLS 프로토콜

프로토콜 동작과정을 간단히 살펴보면 먼저 EAPOL(EAP over LAN)을 사용하여 모바일 노드 A(이하 MN_A)는 연결을 요청한다. 연결 요청을 받은

모바일 노드 B(이하 MN_B)는 MN_A의 식별 값을 요청한다. 요청에 대한 MN_A는 식별 값을 응답한다. 식별 값이 확인되면 MN_B는 EAP-TLS의 시작을 알리게 되고 두 모바일 노드는 EAP-TLS 과정을 시작한다. 먼저 MN_A가 Client-hello 요청 메시지를 보내게 된다. MN_B도 Server-hello, Certificate, Server-Key-Exchange, Certificate-Request, Server-hello-Done 메시지를 보낸다. 이 메시지를 받은 MNA는 MNB의 인증서를 검증하고 검증이 완료되면 Certificate, Client-Key-Exchange, Certificate-Verify, Change-Cipher-Spec, Finished 메시지로 응답한다. 다시 MN_B도 Change-Cipher-Spec, Finished 메시지로 응답한다. 위와 같은 과정이 끝나면 세션이 성공하게 된다. 하지만 EAP-TLS도 단점을 가지고 있다. 만약 두 노드 사이에 중간에서 공격자가 중간자 공격을 시도할 수 있다는 단점을 가지고 있다.

3. 제안하는 시스템

본 논문에서 제안하는 시스템의 모바일 노드는 듀얼인터페이스(USIM과 WLAN)카드를 가지고 있어야 하고 Ad-Hoc 네트워크에 연결되어 있는 모든 모바일 노드는 모바일 네트워크 인증서버(Mobile Network Authentication Server)에 등록되어 있어야 한다. 제안하는 시스템의 구성은 [그림 3]와 같이 구성되어 있다.



[그림 3] 제안 시스템 구성도

MN_A는 MN_B가 속한 이동 Ad-Hoc 네트워크에 가입하려고 한다. 이 경우 MN_A는 MN_B에게 EAP-TLS 인증 프로토콜을 통하여 인증절차를 수행하게 되며, 인증절차에서 필요한 MN_A의 인증서를 모바일 네트워크 인증서버로부터 부여 받는다. 이때 사용하는 MN_A의 인증서는 모바일 네트워크 인증서버가 부여하는 임시인증서를 사용하고, 임시 인증서를 통하여 MN_B가 검증과정을 수행한다.

3.1 사전 인증서 발급 과정

본 논문에서는 Ad-Hoc 네트워크에 가입하려는 모바일 노드는 모바일 네트워크 인증서버에 먼저 등록이 되어야한다. 등록된 모바일 노드는 Ad-Hoc 네트워크에 가입하기 전에 모바일 네트워크 인증서버로부터 임시 인증서를 발급받는다. [그림4]는 모바일 노드와 모바일 네트워크 인증서버 간의 사전 인증서 발급 과정이다.

[그림 4] 사전 인증서 발급 과정

먼저 단계 1에서 모바일 노드는 모바일 네트워크 인증서버에게 식(1)과 같은 인증서 요청 메시지를 보낸다.

$$MN\_Cert\_Req\_Msg = (Pub\_K_A, TempID_A, E_{Pub\_K_{as}}(ID_A, R_A), T, H) \quad (1)$$

이 인증서 요청 메시지에는 모바일 노드의 공개키와 노드가 Ad-Hoc 네트워크에서 사용할 임시 식별 값과 모바일 네트워크 인증서버의 공개키로 암호화된 식별 값과 랜덤넘버를 포함한다. 또한 타임스탬프와 해쉬 값도 포함한다. 해쉬 값은 식(2)와 같다.

$$H = Hash(Pub\_K_A, ID_A, TempID_A, T, R_A) \quad (2)$$

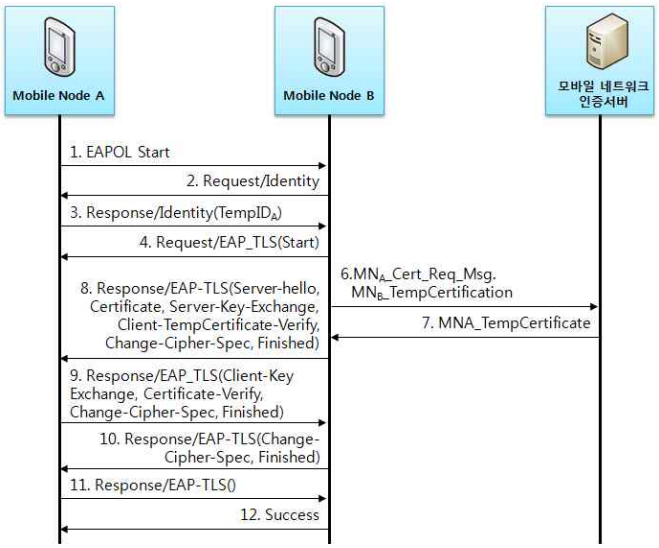
이 메시지를 받은 모바일 네트워크 인증서버는 모바일 노드의 식별 값과 임시 식별 값 랜덤넘버를 가지고 임시 인증서를 생성한다. 모바일 네트워크 인증서버는 모바일 노드에게 임시 인증서를 발급하고 발급 시에 식(3)과 같이 해쉬 값을 포함하여 전송한

다. 또한 모바일 노드는 서로 다른 식별 값으로 서로 다른 모바일 Ad-Hoc 네트워크에 가입이 가능하며, 그 때마다 모바일 네트워크 인증서버는 서로 다른 임시 인증서를 발급함으로써 모바일 식별자에 대한 보호가 강력하다.

$$H = Hash(Pub\_K_A, ID_A, TempID_A, T, R_A + 1) \quad (3)$$

3.2 사용자 식별 및 인증 프로토콜

본 논문에서는 제안하는 모바일 Ad-Hoc 네트워크에서 인증 프로토콜 동작은 [그림 5]과 같다.



[그림 5] 제안하는 프로토콜의 동작과정

제안하는 부분에 대해서만 설명하면, 단계 3에서 MN_B가 보내는 식별 값 요청에 대한 응답으로 MN_A는 자신의 식별 값으로 응답하는 것이 아니라 모바일 네트워크 인증서버에게 보냈던 임시 식별 값으로 응답한다. 이 과정을 통해 MN_A의 사용자 식별 값을 MN_B에게 알리지 않게 된다. 단계 5에서는 사전에 MN_A가 모바일 네트워크 인증서버에게 요청한 메시지를 다시 MN_B에게 보낸다. 단계 6에서 MN_B는 MN_A의 인증서 요청메시지와 자신이 이동 Ad-Hoc 네트워크에 가입 시 사용했던 임시 인증서를 모바일 네트워크 인증서버에게 보낸다. 이 경우 MN_B가 인증되지 않은 노드라면 모바일 네트워크 인증서버는 MN_A의 임시 인증서를 발급하지 않는다. 단계 7에서 MN_B의 검증이 완료되면 MN_B에게 MN_A의 임시 인증서를 발급한다. 단계 8에서 MN_A의 임시 인증서를 다시 보냄으로 하여, MN_A가 MN_B가 정상적으로 모바일 네트워크 인증서버에게 자신의 임시 인증서를 받아온 것을 확인할 수 있다. 이러므로 MN_A는 MN_B에 대한 검증을 할 수 있게 된다. 이 외의 나머지 과정은 EAP-TLS 프로토콜 과정과 동일하다.

제안하는 프로토콜 과정을 통해 모바일 Ad-Hoc 네트워크의 노드들에게 자신의 식별 값을 알리지 않아도 인증이 성립되며 공격자가 중간자 공격을 시행하더라도 모바일 네트워크 인증서버가 공격자를 인증하지 못하므로 제안하는 프로토콜은 중간자 공격을 방지할 수 있다.

4. 성능분석

본 논문에서 제안하는 프로토콜은 기존의 EAP-TLS 프로토콜과 모바일 네트워크간의 연결을 통해서 더욱 더 안전한 인증 프로토콜을 설계하였다. [표 2]에서와 같이 제안하는 프로토콜과 EAP-TLS 프로토콜을 비교해 보면 제안하는 프로토콜은 인증적인 측면에서 기존의 EAP-TLS 프로토콜은 Ad-Hoc 네트워크 내의 노드들의 각자의 인증서를 사용하는데 반해 제안하는 프로토콜은 모바일 네트워크의 인증서버가 발행한 인증서를 사용함으로써 더욱 더 안정된 인증을 수행한다.

[표 1] 비교 분석

구 분	제안하는 프로토콜	EAP-TLS 프로토콜
Ad-Hoc 인증	모바일 네트워크 인증서버가 발행한 인증서	인증서
가입자 인증	모바일 네트워크 인증서버가 발행한 인증서	인증서
가입자 관리	모바일 네트워크의 인증서버	없음
사용자의 식별 보호	강력함	없음
타 Ad-Hoc 가입	다른 임시 식별 값과 임시 인증서 사용	동일한 식별 값과 인증서 사용
중간자 공격 방지	탐지 가능	탐지 불가

또한 사용자 식별의 측면에서 보면, EAP-TLS 프로토콜은 사용자의 식별 값을 바로 받아 사용하기 때문에 사용자의 식별 값에 대한 보호가 전혀 되지 않지만, 제안하는 프로토콜의 사용자 식별 보호는 모바일 네트워크 인증서버에게만 식별 값을 보내고 다른 Ad-Hoc 사용자에게는 임시 식별 값만을 보내어 모바일 노드의 사용자 식별을 보호할 수 있다.

다른 Ad-Hoc 네트워크 가입 시 기존의 EAP-TLS

프로토콜은 동일한 식별 값과 동일한 인증서를 사용하여 공격자가 식별 값과 인증서를 얻어 다른 Ad-Hoc 네트워크에 접속하는 것이 용이하다. 하지만 제안하는 프로토콜에서는 다른 임시 식별 값과 다른 임시 인증서를 사용하기 때문서 서로 다른 Ad-Hoc 네트워크에서도 사용자의 식별이 분명해진다. 또한 중간자 공격에서도 EAP-TLS는 중간에 다른 공격자가 중간자 공격을 탐지하는 것이 매우 어려우나 제안하는 프로토콜은 중간자 공격을 공격자가 모바일 네트워크의 인증서버로부터 발행된 임시 인증서에 대하여 검증이 불가능하고 공격자 자신을 검증하지 못하기 때문에 중간자 공격을 방지할 수 있다.

5. 연구결과

본 논문에서는 이동 Ad-Hoc 네트워크에서 사용자의 식별 보호와 더욱더 안전한 인증을 하기위한 프로토콜을 제안하였다. 이동 Ad-Hoc 네트워크의 특성상 이동성을 가지고, 중앙 집중의 네트워크 체제로 이루어져 있지 않기 때문에 인증에 대해서는 많은 취약점들을 가지고 있다. 또한 공격자의 이동 Ad-Hoc 네트워크의 가입이 이루어질 경우 모든 노드들과 통신을 할 수 있기 때문에, 이러한 가입자를 막기 위해서는 더욱더 안전한 인증 프로토콜이 필요하다. 본 논문에서 제안한 인증 프로토콜은 모바일 네트워크 인증서버가 이동 Ad-Hoc 네트워크의 가입자에 대하여 인증서를 발급하고 그것을 확인함으로 인해 공격자의 네트워크 가입을 막고, Ad-Hoc 네트워크 안에서 임시 식별값을 사용함으로 인해 사용자의 식별 보호에도 강력하다. 또한 타 Ad-Hoc 가입 시 서로 다른 식별 값과 인증서를 사용하여 Ad-Hoc 네트워크마다 사용자의 식별보호가 강력해지고 공격자의 가장공격이나 중간자 공격을 방지할 수 있다.

제안된 인증 프로토콜은 다른 모바일 네트워크뿐만 아니라 센서 네트워크와 같은 유비쿼터스 환경에서도 많은 기여를 할 것으로 기대된다. 향후 모바일 노드가 아닌 비 모바일 노드와의 Ad-Hoc 연결 시에 대한 연구가 필요하다.

참고문헌

[1] 권혜연, 신재욱, 이병복, 최지혁, 남상우, 임선배, “이동 Ad Hoc 네트워크 기술 동향”, 한국전자통신연구원, [ETRI]전자통신동향분석 제 18권, 제 2호, 2003.4

[2] 김윤호, “Mobile Ad Hoc Networks에서 효과적인 인증서비스”, 한국전자거래학회, 한국전자거래학회지, 제 10권, 제 1호, pp. 310-317, 2005.6

[3] 신재욱, 권혜연, 남상우, 임선배, “이동 Ad Hoc 네트워크 실현을 위한 무선 접속 기술,”Telecom. Review, 제12권 3호, 2002, pp. 322 - 335.

[4] Charles E. Pekins, “Ad Hoc Networking”, Addson-Wesley, 2001.

[5] C.K. Toh, “Ad Hoc Mobile Wireless Networks : Protocols and Systems”, Prentice Hall PTR, 2002.

[6] Muhammad Agni Catur Bhakti, Azween Abdullah, Low Tan Jung, " EAP-BASED Authentication for Ad Hoc Network", Semina Nasional Aplikasi Teknologi Informasi 2007(SNATI 2007), 2007

[7] SANDIP VIJAY, S. C. SHARMA, "A Secure Gateway Solution Wireless Ad-Hoc Networks", International Journal of Computer Science and Applications, Vol. 5, No. 4, pp 26-44, 2008

[8] Yuh-Min Tseng, "USIM-based EAP-TLS Authentication Protocol for Wirelss Local Networks", Computer Standard & Interfaces 31, 128-136, 2009

[9] "The EAP TLS Authenticatioon Protocol", TTAE. IF-RFC5216, 2009