3G-WLAN 통합 네트워크에서 지역적인 인증 프로토콜 제안

유진희* 송주석
*연세대학교. 컴퓨터과학과

Locally Stabile Authentication Protocol In 3G-WLAN Integration Networks

Jin-Hee You* Joo-Seok Song
*Computer Science Department, Yonsei University.

요 약

최근 다양한 무선 네트워크의 사용이 일반화 되면서 이종의 네트워크 간의 연동의 필요성이 대두되고 있다. 이는 서로 다른 특징을 갖는 네트워크간의 연동을 통해 개별 네트워크가 갖는 장점을 혼합하여 질 좋은 서비스를 제공하기 위함이다. 본 논문은 많이 사용되어지고 있는 3G 네트워크와 WLAN 네트워크의 연동을 고려한다. 또한 연동 시 발생하는 기술 문제들 중에서 중요성이 높은 인증 방법에 초점을 맞춘다. 본 논문은 3G-WLAN 연동 네트워크상에서 일반적으로 많이 쓰이는 인증 방법의 문제점을 보완한 새로운 인증 프로토콜을 제안한다.

Ⅰ. 서론

최근 무선네트워크의 사용이 일반화 되면서 다양한 특징을 갖는 네트워크 간의 연동의 필요성이 대두되었다. 또한 사용자가 이종 네트워크에 추가적인 비용 없이 편리한 방법으로 빠르게 접근 할 수 있도록 효과적인 연동 구조를 제안하는 연구가 활발히 진행 중이다[1]. 특히 현존하는 무선 네트워크에서 특징이 상반되는 3G 이동 통신 네트워크와 WLAN 네트워크 간의 연동은 큰 관심을 갖고 있다. 이때 3G의 장점과 WLAN의 장점을 혼합하여 최적의 서비스를 제공받을 수 있는 좋은 연동 구조가 필요하다.

3G 서비스는 서비스의 영역이 넓지만 사용 요금이 비싸고 데이터 전송 속도도 느리다. 반면 WLAN 서비스는 서비스 영역이 좁지만 전송 속도가 빠르고 요금이 싸다는 장점이 있다[2]. 이 두 네트워크의 장점을 혼합하여 질 좋은 서비스를 사용자에게 제공하기 위한 노력이 필요하다.

3G-WLAN 연동에는 많은 고려사항이 필요하다. 모바일 IP의 이동성, 주소 매핑 및 로밍 방법, QoS, 인증 기술, 과금 기술 등의 지원이 이루어 져야 한다[3]. 그 중 본 논문은 3G-WLAN의 연동을 위한 효과적인 보안 기술을 제안한다.

연동 네트워크상에서의 보안 구조는 연동된 한 네트워크가 가지는 취약한 보안 구조를 다른 네트워크가 강화시켜 줌으로써 보다 나은 보안 기술을 개발해야 한다. 이를 위해 필요한 기술로는 사용자와 네트워크간의 상호 인증방식, 안전한 키 관리 기법, 데이터의 기밀성 및 무결성 보장, 보다 안전한 암호화 기술 등이 있다[3].

본 논문은 현재 3G-WLAN 연동 네트워크상에서 사용되고 있는 일반적인 인증 방식인 EAP-AKA(Extensible Authentication Protocol - Authentication and Key Agreement) 방식을 소개하고 이 방식의 문제점을 보완하는 새로운 인증 프로토콜을 제안한다[4].

대부분의 3G-WLAN 연동 방식은 3G 네트워크 상에 있는 이동 단말기가 어떠한 지점(hot-spot)에 들어갔을 때 WLAN 서비스를 받는 것이다. 이때 이동 단말은 WLAN에게 사용 인증을 받아야 한다[3]. 대부분의 연동 보안 프로토콜은 이동 단말이 WLAN의 인증을 받기 위해서 3G의 인증 서버를 통해 인증을 받아야 WLAN의 서비스를 받을 수 있는 방식을 사용한다[4].

마찬가지로 EAP-AKA 인증 방식도 WLAN을 접근하기 위해서 3G의 인증 서버인 AAA (Authentication , Authorization and Accounting)로의 접근을 통해 인증을 허락받아야 한다. 이러한 과정은 이동 단말이 새로운 망에 접근하는 단계에서 패킷의 교환 횟수가 많아지고 복잡한 인증 절차로 인해 오버헤드가 증가한다는 단점이 있다.

또한 EAP-AKA 방식은 이동 단말의 인증을 위해 Home Location Register(HLR)와 이동 단말 사이의 비밀키 암호화 방식을 사용한다. 이는 WLAN에게 사용자의 정보를 노출시킬 가능성이 크다는 단점을 가지고 있다. 그러므로 이를 보완하기 위해서 본 논문은 공개키 암호화 방식 기반의 공개키 인증서를 통해 보다 강화된 암호화 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로써 3G-WLAN 연동 네트워크상에서 사용되는 기존의 인증 프로토콜을 소개한다. 3장에서는 기존의 인증 방식을 보완한 새로운 인증 프로토콜을 소개한다. 4장에서는 결론을 내리고 향후 연구 방향을 제시한다.

Ⅱ. 관련연구

3G-WLAN 연동 네트워크상에서 일반적으로 사용되는 인증 프로토콜은 EAP-AKA 방식이다[4]. 이는 AKA 인증에 다양한 인증 방법들을 지원하는 점 대 점 프로토콜(Point-to-Point Protocol)인 EAP 개념을 도입함으로써 사용자의 단일 인증을 통한 편의성, 호환성이 한층 강화될수 있다는 장점을 가지고 있다. 또한 3G 네트워크의 표준 인증 방식인 EAP-AKA를 WLAN 네트워크 상에서도 동일하게 인증될 수 있도록 함으로써 연동 인증 프로토콜로 대두되었다.

3G-WLAN 연동 네트워크에서 사용되는 EAP-AKA 방식은 그림 1과 같다[6]. MS가 WLAN 네트워크에 접속하기 위해 필요한 인증 절차는 우선 WLAN은 EAP 요청을 통해 시작된다. 요청을 받은 이동 단말기(Mobile Station(MS))는 Access Point(AP)로 EAP 응답을 보내고 인증을 받기 위해 3G 네트워크의 AAA 서버에 등록한다. 3G 네트워크의 AAA 서버는 HLR에 접속하여 가입자의 인증 정보 및 프로파일(Profile)을 조회한다. 인증이 성공되면 AAA 서버는 해당 WLAN AP에게 접속 승인 메시지를 전송하고 AP는 이동 단말기에게 EAP 인증 성공 메시지를 전달한다. 이러한 과정이 끝나면 이동 단말기는 WLAN의 서비스를 받을 수 있게 된다.

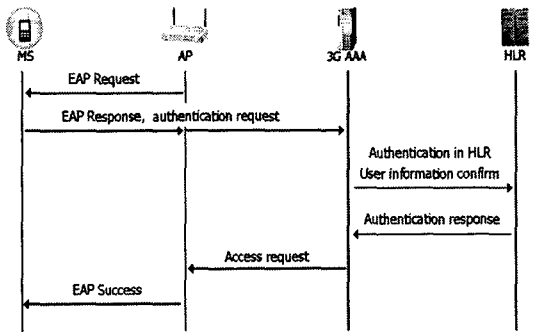

그림 1. EAP-AKA 인증 절차

이와 같은 EAP-AKA의 문제점은 이동 단말기가 WLAN에 접속할 때 마다 3G 네트워크에 접속하여 위와 같은 인증 절차를 거쳐야 한다는 것이다, 즉, 3G 네트워크의 동의하에 WLAN의 서비스를 받을 수 있다. 이는 인증 절차가 복잡하고 인증 과정에서 많은 메시지 전송으로 인한 오버헤드가 발생할 뿐만 아니라 이동 단말기의 이동성이 심해지면 병목현상(bottleneck)이 발생할 가능성이 높아진다는 단점을 가지고 있다. 그러므로 본 논문은 이러한 오버헤드를 줄이기 위해 WLAN상에서의 지역적인 인증 절차를 통해 WLAN의 서비스를 제공받을 수 있는 인증 프로토콜을 제안한다.

EAP-AKA의 또 다른 문제점으로는 MS와 HLR이 공유하는 비밀키(secret key) 암호화 방식을 통해 HLR 에서의 인증이 수행되는데 이는 사용자의 프로파일이 WLAN에게 공개될 가능성이 높다는 것이다. 이를 보완하기 위해 본 논문은 공개키 암호화 알고리즘을 사용하는 EAP-TLS 인증 방식을 도입한다.

EAP-TLS(Transport Layer Security) 방식은 안전한 웹 애플리케이션 트랜잭션을 위해 대부분의 웹 브라우저

에서 사용하는 SSL(Secure Socket Layer)의 최신 버전이다[5]. TLS는 TCP/IP 연결을 위해 안전한 인증 및 암호화를 제공하도록 설계되었다. TLS의 인증 방식은 우선 SSL 클라이언트가 서버에 연결하여 인증 요청을 수행하면 서버가 클라이언트로 전자 인증서를 전송한다. 그 후 클라이언트가 인증서의 유효성 및 전자 서명을 검사한다. 다음으로 서버가 클라이언트에게 인증을 요청하면 클라이언트가 서버로 전자 인증서를 전송하다. 서버가 인증서의 유효성 및 전자 서명을 검사하고 무결성이 검증되면 인증이 완료된 것이다. TLS의 공개키 기반 구조(Public Key Infrastructure(PKI))방식을 도입하여 본 논문은 기존의 취약한 인증 방법을 보완한다.

Ⅲ. 본론

본 논문은 기존의 인증 절차인 EAP-AKA방식에서 두 가지 문제점을 보완한다.

(1) 이동 단말기가 WLAN에 접근 시 3G 네트워크의 연결 없이 WLAN 네트워크에 있는 인증 시스템을 통해 인증을 받는다.

(2) 공개키 인증서를 통해 강화된 암호화 방식을 지원한다.

우선 첫 번째 보완된 부분은 이동 단말기가 WLAN에 접근 하였을 때 WLAN 네트워크에서 인증 철자가 진행되는 방식이다. 이는 이동 단말기가 WLAN 서비스를 받기위해서 항상 3G의 AAA 서버와 HLR을 통한 인증이 이루어져야 하는 기존 EAP-AKA방식의 오버헤드를 줄이기 위한 것이다. 이는 WLAN에서 이루어지는 지역적인 인증 프로토콜로써 기존의 3G의 AAA와 HLR이 필요가 없다. 단지 WLAN에서 인증을 위한 인증 시스템(Authentication System (AS))이 필요하다. 그러므로 본 논문은 이동 단말기인 MS와 AS사이의 새로운 인증 절차를 제안한다.

다음으로 두 번째 보완된 부분은 기존의 암호화 방식에서 보안이 더욱 강화된 공개키 인증서 방식을 사용한다. 이때 3G는 인증기관(Certification Authority(CA)) 역할을 한다. 이동 단말기는 자신의 프로파일과 공개키를 3G의 인증기관에 전송함으로써 인증서를 발급 받고 WLAN 네트워크의 AS는 CA의 공개키를 3G로부터 받아 후에 이동 단말기가 WLAN에 접근할 때 이동 단말기의 인증서의 유효성을 증명할 때 사용한다. 즉, 본 논문이 제안하는 인증 프로토콜은 3G와의 접근이 초기에 한번 이루어지고 그 후에는 이동 단말기가 WLAN에 접근할 때 WLAN와 이동 단말기간의 인증 절차만 진행된다.

그림 2는 본 논문이 제안하는 지역적인 공개키 인증서 기반의 인증 과정을 보여준다.

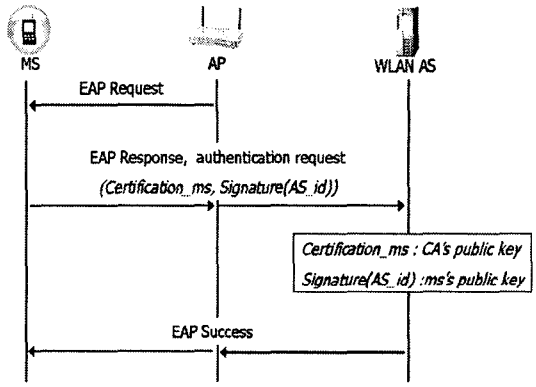

그림 2. 공개키 인증서 기반의 지역적인 인증 절차

인증서를 받은 이동 단말기는 WLAN 네트워크에 접근 한 즉시 WLAN의 AP로부터 EAP 요청 메시지를 받는다. 이동 단말기는 인증을 위해 자신이 가지고 있는 인증서와 자신이 접근하기 원하는 WLAN의 AS의 아이디를 자신의 개인키로 서명하여 WLAN의 AS에게 전송한다. 이 메시지를 받은 AS는 이전에 CA로부터 받은 CA의 공개키를 통해 이동 단말기의 유효성을 검증하고 이 인증서에 포함된 이동 단말기의 공개키를 사용하여 AS의 아이디 서명을 복호화 하여 자신의 아이디와 일치하는 지를 증명한다. 그 값이 증명이 되면 WLAN은 이동 단말기가 인증에 성공했음을 알리고 성공 메시지를 전송하여 서비스를 제공 받도록 한다.

위와 같은 본 논문이 제안하는 인증 프로토콜을 기존 EAP-AKA방식의 복잡성과 보안의 취약성을 해결해준다. 3G에 접근을 최소화 하여 지역적인 인증을 수행하고 전송하는 인증 메시지를 줄임으로써 이동 단말기가 WLAN 네트워크에 접근 시 지연시간을 줄여준다.

Ⅳ. 결론 및 향후 연구

본 논문은 3G-WLAN연동 네트워크상에서 수행되어야 할 효과적인 인증 프로토콜을 제안하였다. 이는 기존의 인증 프로토콜일 EAP-AKA방식에서 발생되는 많은 메시지 전송과 복잡한 인증 절차, 사용자 프로파일이 WLAN에 공개되는 보안상의 취약점등의 문제점을 보완하였다. 또한 이동 단말기가 WLAN에 접근할 때 3G의 AAA 서버와 HLR을 통해 이동 단말기의 인증을 수행하려하는 비효율적인 인증 방법을 보완하기 위해 3G의 접근을 최소화하고 WLAN 네트워크상에서 인증을 수행할 수 있는 인증 시스템을 생성하였다.

향후 연구로는 본 논문에서 제안한 인증 프로토콜과 EAP-AKA방식의 성능을 비교하여 본 논문의 효율성을 증명하려 한다.

[참고문헌]

[1] R. G Cheng and S. L. Tsao, "3G-based access control for 3GPP-WLAN interworking." in IEEE 59th Vehicular Technology , VTC 2004-Spring, vol. 5, pp. 2967-2971, May 2004.

[2] 3GPP TSG Services and System Aspects, Feasibility Study on 3GPP System to Wireless Local Area(WLAN) Interworking (release 6), Technical Report, 3GPP TS 33.102 V6.2.0 (2003-09), Sept. 2003

[3] G. M. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking." IEEE communications vol. 41, no. 11, pp.82-88, 2003

[4] J. Arkkp and H. Haverinen, Extensible Authentication Protocol Method for UMRS Authentication and Key Agreement(EAP-AKA), Technical Report, draft-arkko-pppext-eap-aka-14, 2004

[5] G. Kormentzas, G. Kambourakis, A. Rouskas, and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking." IEEE Proceeding-Communications, 2004

[6] Y. M. Tseng, C. C. Yang, and J. H. Su. " Authentication and billing protocols for the integration of WLAN and 3G networks." Wireless Personal Communications, 2004