무선랜 환경에서의 지문을 이용한 사용자 인증 프로토콜

정승환*, 이성주*, 신현섭*, 정용화*, 김태섭* 오룡*, 조충호*, 이남일+
*고려대학교 컴퓨터정보학과
+테스텍 주식회사

A Fingerprint_based User Authentication Protocol for Wireless LAN Environment

Seunghwan Jung*, Sungju Lee*, Hyunsup Shin*, Taesup Kim*, Ryong Oh*, Choongho Cho*, Namil Lee+, and Yongwha Chung*
*Department of Computer & Information Science, Korea University
+Testech Inc.

요 약

네트워크 기술이 발전함에 따라 유/무선 네트워크가 통합되기 시작하였고, 궁극적으로 언제/어디서나 컴퓨터를 사용할 수 있는 유비쿼터스 컴퓨팅 시대가 도래 할 것으로 예상된다. 최근에는 공공장소에서 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 관심이 많아지고 있다. 무선랜 환경에서 중요한 보안문제 중 하나는 승인된 사용자에게만 접속을 허용하는 것이다. 특히, 유선 네트워크와 다르게 무선 네트워크 환경에서는 Access Point(AP)가 설치되어 있는 곳이면 누구나 쉽게 AP를 통해 네트워크를 이용할 수 있기 때문에 접속에 관한 보안의 중요성이 강조되고 있다. 본 논문에서는 무선랜 환경에서 안전하게 사용자를 인증하고 서비스를 제공하기 위해 지문을 이용한 사용자 인증 프로토콜을 제안한다.

I. 서론

인터넷 및 이동통신 기술의 발전과 함께 사무실내에서 뿐만 아니라 자동차나 거리, 공항이나 지하철 역 등 다양한 환경에서 PDA 또는 휴대전화 등을 이용한 인터넷 사용이 증가하고 있다. 최근에는 우리에게 익숙한 이더넷 기술을 사용하는 무선랜(WLAN:Wireless Local Area Network) 서비스가 주목을 받고 있다. 무선랜은 무선랜 카드를 노트북이나 PDA 등에 장착하고 인터넷과의 접점이 되는 AP를 이용해 인터넷을 이용할 수 있게 해주는 기술이다. 즉, 이동전화를 이용해 인터넷을 이용할 경우에 비해 속도가 빠르고, 장비의 비용이 10배정도 저렴하기 때문에 무선인터넷 시장에서 경쟁력을 갖추고 있다고 보여지며, 향후 더 많은 이용이 예상되고 있다.

현재 무선랜 기술에서의 주요 문제점은 전송속도와 보안에 있다. 특히 보안 문제는 무선랜 기술의 보급과 사용에 커다란 장애 요소 중 하나이다[1]. 무선랜의 기지국 역할을 하는 AP는 유선 네트워크와 무선 네트워크를 매개해주는 역할을 하게 된다. 이 AP를 통한 접속은 비록 사용자가 네트워크의 외부에서 접속하는 것 같아 보이지만 실제로는 내부 네트워크(LAN:Local Area Network)안에서만 접근이 이루어진다. 따라서 외부망(WAN)과 내부망(LAN)사이의 보안 문제를 해결하는 기존 유선망의 보안 기술인 침입탐지시스템이나 방화벽등으로 무선랜의 보안 취약점을 해결하기 어렵다[2].

일반적인 무선랜의 보안문제는 크게 두 가지 측면에서 볼 수 있는데, 첫 번째는 승인된 사용자에게만 접속을 허용하는 접속에 관한 보

안이며, 다른 하나는 스니퍼 등을 이용해 무선랜을 통해 전송되는 내용 자체를 몰래 보는 도청 행위에 관한 보안이다. 특히 유선 네트워크와 달리 무선랜에서는 AP만 설치되어 있는 곳이면 누구나 쉽게 AP를 통해 네트워크를 이용할 수 있다. 이에 따라 무선랜에서의 중요한 보안문제는 접속에 관한 보안, 즉 사용자 인증 문제라고 할 수 있다.

일반적으로 정보시스템에 접근하기 위한 사용자 인증 수단으로 패스워드, PIN(Personal Identification Number) 또는 스마트카드 등의 전통적인 방법들이 널리 이용하고 있으나, 이러한 인증수단은 분실, 도난, 망각으로 인한 위험이 존재한다. 이러한 위험을 해결하기 위하여 개인의 고유한 생체정보를 이용하는 생체인식에 관한 연구가 활발히 진행되고 있다[3]. 본 논문에서는 생체인식을 위해 생체정보 중 가용성, 정확도, 경제성면에서 현재까지 가장 현실적인 대안으로 평가받고 있는 지문[4]을 이용한 무선랜 환경에서의 지문 인증 프로토콜을 제안한다. 즉, 지문을 이용하여 사용자를 인증하는 경우 지문정보가 무선 랜 환경에서 안전하게 전송되는 프로토콜을 제안한다.

2장에서는 본 논문에서 제안한 무선랜 환경에서의 지문을 이용한 인증 프로토콜과 키 분배 시나리오에 대해 설명하고, 3장에서는 제안한 프로토콜의 구현내용을 기술하며, 4장에서 결론을 맺는다.

II. 제안하는 인증 프로토콜

본 장에서는 무선랜 환경에서 지문을 이용한 인증 프로토콜에 대해 설명한다. 또한 지문 인증 프로토콜에서 사용되는 키를 효율적으로 분배하기 위해 KDC(Key Distribution Center)를 이용한 키 분배 시나리오를 설명한다.

본 논문에서 제안한 지문을 이용한 사용자 인증 시스템 환경은 그림 1과 같고, 사용자의 요청에 의해 사용자를 인증하는 인증서버, 기지국 역할을 하는 AP, 노트북이나 PDA 등의 무선랜 단말과 지문센서가 클라이언트로 구성된다. 인증서버와 AP는 유선으로 연결되어 있고, AP와 클라이언트는 무선으로 연결되어 있다.

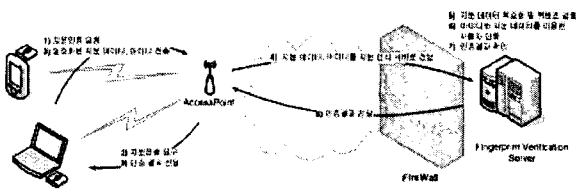

그림 1. 사용자 인증 시스템 환경

1. 키 분배

본 논문에서 제안하는 사용자 지문 인증 프로토콜 메커니즘에서 클라이언트, AP 그리고 인증서버에는 각각의 개인키 및 대칭키의 분배를 필요로 하고 클라이언트의 키 분배 요구에 따라 AP, 인증서버에 효율적인 키 분배가 이루어질 수 있도록 하는 구성이 필요하다.

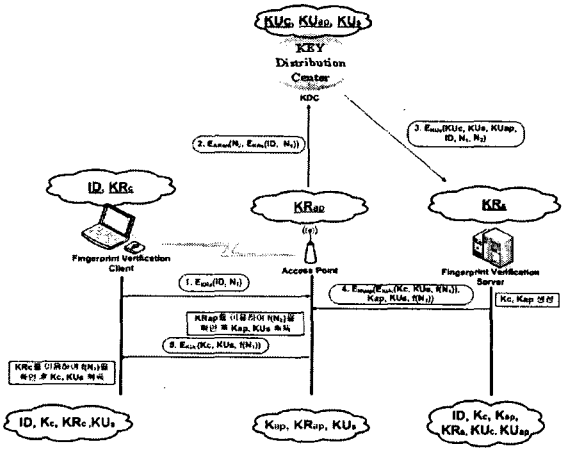

그림 2. 키 분배 시나리오

그림 2는 전체적인 키 분배 시나리오를 나타낸다. 키 분배를 효율적으로 하기위해 클라이언트, AP, 그리고 인증서버 이외에 KDC를 이용한다. 본 논문의 키 분배 시나리오에서는 클라이언트, AP, 인증 서버는 각각 자신의 개인키 KRx(x=c, ap, s)를 가지고 있고, KDC는 KRx를 미리 갖고 있다고 가정한다. 사용자가 클라이언트를 통하여 키 분배 요청을 하면, 클

라이언트에서는 ID와 Nounce값 N_1을 이용하여 $E_{KRc}(ID, N_1)$ 패킷을 생성하여 AP로 전송한다. 여기서 $E_{KRc}( )$는 비대칭 암호화 알고리즘인 RSA를 이용하여 암호화하며, 이때, 개인키 KRc를 사용한다. $E_{KRc}(ID, N1)$를 전송받은 AP는 Nounce값 N_2를 생성하고 N_2, $E_{KRc}(ID, N_1)$를 AP의 키 KRap로 암호화하여 KDC로 전송한다.

$E_{KRap}(N_2, E_{KRc}(ID, N_1))$를 전송받은 KDC는 공개키인 KUap, KUc를 이용하여 복호화 할 수 있으며, 클라이언트의 ID, N_1, AP에서의 N_2값을 얻어 $E_{KUs}(KUc, KUs, KUap, ID, N_1, N_2)$을 생성하여 인증서버로 전송한다. 인증서버에서는 개인키 KRs를 사용하여 $E_{KUs}(KUc, KUs, KUap, ID, N_1, N_2)$을 복호화하여 ID, KUs, KUap를 얻는다. 클라이언트의 ID를 이용하여 클라이언트와 인증서버 간의 대칭키인 Kc, 인증서버와 AP간의 대칭키인 Kap를 생성하고, $E_{KUap}(E_{KUc}(Kc, KUs, f(N_1)), Kap, KUs, f(N_2))$을 생성하여 AP로 전송한다. 여기서 N_1, N_2값에는 간단한 함수 f(N)이 적용되어 전송된다.

$E_{KUap}(E_{KUc}(Kc, KUs, f(N_1)), Kap, KUs, f(N_2))$을 전송받은 AP는 개인키 KUap를 사용하여 복호화 시켜 $E_{KUc}(Kc, KUs, f(N_1)), Kap, KUs, f(N_2)$를 얻는다. 여기서 얻은 $f(N_2)$는 이전에 KDC로 전송했던 N_2에 F(N)을 적용시켜 얻어진 결과와 비교하여 올바른 패킷인지 확인할 수 있다. Kap, KUs 등 AP에서 필요한 정보를 얻은 후 $E_{KUc}(Kc, KUs, f(N_1))$는 별도의 전처리 과정 없이 클라이언트로 전송되고 클라이언트에서는 KRc를 이용하여 복호화 하고 위의 AP에서와 같은 방법으로 N_1을 확인 후 Kc, KUs를 획득하게 되면 키 분배는 완료된다.

2. 지문을 이용한 사용자 인증

그림 3은 본 논문에서 구현한 전체적인 사용자 인증 프로토콜의 시나리오를 나타낸다. 사용자 지문 인증 프로토콜의 과정은 사용자가 ID를 입력하고 입력된 정보와 클라이언트에서 생성한 랜덤 값 R_1을 통하여 인증을 요청한다. 여기서 R_1은 세션키 Kc-s를 생성하기 위한 랜덤 값이다.

AP는 인증서버로 사용자 인증을 요청한다. 인증서버는 Nonce값 $f(R_1)$과 랜덤 값 R_2을 발생시켜 AP로 전송한다. Nonce값은 AP와 서버 사이의 프로토콜에서 사용될 세션키 생성을 위해 사용된다. AP는 클라이언트에게 사용자 인증 승인 메시지를 보낸다.

클라이언트는 센서로부터 획득한 지문정보를 해쉬함수를 적용한 뒤 클라이언트의 개인키 KRc를 이용하여 전자서명을 한 후 데이터를 세션키 Kc-s으로 암호화하여 AP로 전송을 한다. 여기서 전자서명은 전자서명에 작성자로 기재된 자가 그 전자문서를 작성하였다는 사실과 작성 내용이 송/수신 과정에서 위/변조되지 않았다는 사실을 증명하고, 작성자가 전자문서 작성 사실을 나중에 부인할 수 없게 하는 역할을 한다.

AP는 클라이언트로부터 받은 지문정보와 함께 암호화된 Authenticator를 인증서버로 전송한다. Authenticator는 AP와 인증 서버가 키 분배 시나리오에 의해 분배된 대칭키 K_{ap}와 인증서버로부터 받았던 랜덤 값 R_2에 의해 생성된 Nonce값를 이용하여 새로운 세션키 $K_{ap\text{-}s}$를 생성하고, 이 값을 MD5 해쉬 한 값으로 AP와 인증서버 사이의 데이터의 무결성을 위해 사용한다.

인증서버는 대칭키 K_{ap}와 Nonce를 이용하여 만든 $K_{ap\text{-}s}$ 값에서 Authenticator를 만들어 AP로부터 수신한 데이터의 Authenticator를 비교하여 유선 구간에서 데이터의 변조가 없음을 확인한다. 다음으로 AP로부터 받은 암호화된 데이터를 대칭키 K_c와 Nonce값을 이용하여 만든 $K_{c\text{-}s}$ 값으로 복호화 한 후 지문 정보의 해쉬 값과 클라이언트로부터 수신된 지문정보의 해쉬 값을 비교하여 지문정보의 무결성을 확인한다. 확인된 결과를 AP, 클라이언트로 전송한다.

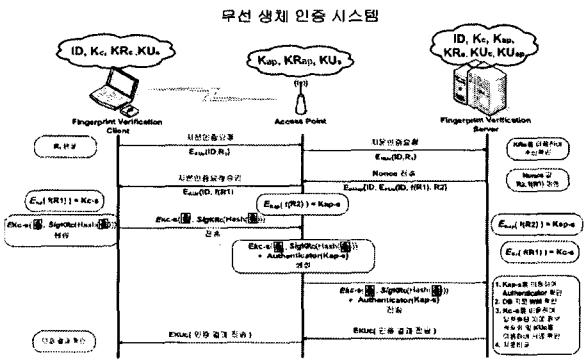

그림 3. 제안하는 사용자인증 프로토콜 메커니즘

Ⅳ. 구현

본 장에서는 무선랜 환경에서의 지문을 이용한 인증 프로토콜의 구현 환경 및 보안성에 대해 분석한다.

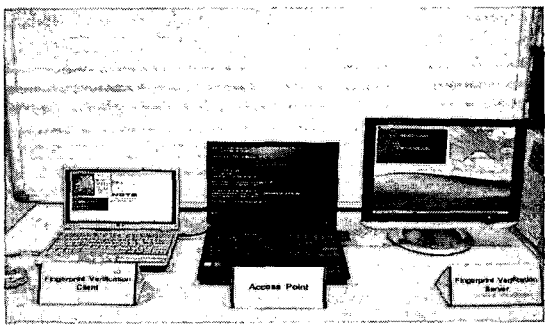

그림 4. 지문인증 서버와 지문인증 클라이언트 인증 시스템

그림 4는 본 논문에서 제안한 무선 랜 환경에서의 지문을 이용한 인증 프로토콜 시스템이다. 클라이언트는 지문 센서와 노트북을 이용하여 구축하였고 AP는 노트북을 이용하여 클라이언트와 무선 네트워크로 통신 할 수 있도록 하였다. 지문 인증 서버는 데스크탑 사양의 컴퓨터를 이용하여 AP와 유선으로 연결되어 통신 할 수 있도록 구축하였다.

기존의 IEEE802.1x의 EAP-MD5의 프로토콜의 취약점인 오프라인 사전 공격에 대해 제안한 프로토콜의 구성요소는 랜덤넘버 R_1과 R_2값을 이용하여 Nonce값, 일방향 해쉬값, 또는 암호화된 값으로 암호화되기 때문에 수동적 공격에 대해 안전하다.

제안한 프로토콜은 사용자와 AP 그리고 인증서버 간의 사용자의 지문정보가 노출되었다 하더라도 세션키가 사용자의 정보와는 독립적으로 생성된 Nonce값에 의해 결정되기 때문에 전송 중의 지문정보가 안전하다. 또한, Nonce값을 생성할 수 있는 랜덤넘버 R_1과 R_2가 공개키로 암호화되어 공격자가 이전에 세션 키를 획득하더라도 암호화된 정보를 알아 낼 수 없다.

Ⅴ. 결론

본 논문에서는 무선랜 환경에서 사용할 수 있는 지문 기반 인증 프로토콜을 제안하였다. 제안한 프로토콜은 랜덤하게 생성된 R_1과 R_2 값 그리고 시간함수에 의해 생성되는 Nonce값을 이용하여 세션 키 및 Authenticator를 생성하였고, 비대칭키 암호화 알고리즘을 이용하여 데이터의 기밀성을 확보하였다. 또한 전자서명 알고리즘을 사용하여 사용자 부인 방지 및 무결성을 확보하였다. 생체정보를 이용한 본인 인증은 기존의 패스워드에 비해 많은 사용상의 장점을 가지고 있다. 그러나, 일단 생체정보가 도용되면 이는 더 이상 바꿀 수 없다는 문제가 있다. 따라서 본 논문에서는 무선 랜 환경에서 지문을 이용하여 안전하게 사용자를 인증하는 프로토콜을 제안/구현하였다.

[참고문헌]

[1] 이종후, 서인석, 윤혁중, 류재철, "무선랜 환경에서의 PKI 구축", 한국정보보호학회 정보보호학회지, 2003.2, 13권 1호, pp77~92.

[2] 김동필, 강철범, 김상욱, "라디우스 인증 서버를 이용한 Rougue AP 차단 시스템 설계", 한국정보과학회 학술발표논문집 2004.4, pp316~318.

[3] A. Jain, R. Bole, and S. Panakanti, "*Biometrics: Personal Identification in Networked Society*", Kluwer Academic Publishers, 1999.

[4] D. Maltoni, et. al., "*Handbook of Fingerprint Recognition*", Springer, 2003.

[5] U. Uludag, *et al.*, "Biometric Cryptosystems: Issues and Challenges," *Proc. of IEEE*, 2004.