인증시간 단축을 위한 무선 PKI

Wireless PKI for Reduction of Authentication Time

신승수*, 최승권**, 조용환**
(주)시그마정보기술*, 충북대학교**

Shin Seung-Soo*, Choi Seung-Kwon**,
Cho Yong-Hwan**
Sigma Information Technology Co., Ltd.*,
Chungbuk National University**

요약

본 논문에서는 기존의 무선 PKI에서 개선되어야 할 여러 가지 사항 중에서 인증서 획득 시간을 단축하기 위한 새로운 인증구조를 제안하고자 한다. 기존의 키 교환방식에서 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 인증서 시간단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다.
인증 시간을 Sufatrio, K. Lam[4]가 제안한 인증구조와 제안한 인증구조를 실험을 통해 비교· 분석하였다.

I. 서 론

정보 유통시 안정성과 신뢰성 확보를 위해 공개키 암호기술을 적용한 인증서 기반의 공개키 기반 구조(PKI : Public Key Infrastructure)가 현재 각종 분야에 가장 보편화되어 있는 방법이다. PKI에서는 사용자의 신상정보와 공개키를 확인할 수 있도록 제 3자인 인증기관(CA : Certificate Authority)으로부터 인증서를 발급 받는다. 그러나 기존의 잦은 인증서 발급으로 통화량의 증가와 비용 및 시간의 소모, 키 관리 등 복잡한 문제가 발생하고 있다. 따라서 사용자간에 실질적인 통신시 제 3자의 신뢰기관의 접촉 없이 독립적으로 안전한 사용자 인증 및 키 분배가 가능한 시스템에 대한 연구가 필요하다[1].

현재의 무선 PKI 프로토콜에서는 라우터 최적화, Ingress 필터링, 이동노드의 이동 관리와 데이터 전송 기법 등과 같은 기술적인 문제와 구현상의 문제들이 여전히 남아 있다. 그러나 무선 PKI의 가장 큰 당면 과제는 상호인증 문제이다. 모든 통신에서 상호인증 문제는 필수적으로 해결해야 할 부분이다. 무선 PKI에서도 전자상거래, 데이터통신, 전자메일 등 다양한 서비스가 원활하게 제공되기 위해서는 상호인증 문제가 해결되어야 한다. 특히 인터넷에서 사용중인 다양한 인증구조들과 무선 PKI가 공존할 수 있도록 하기 위한 연구가 계속 진행되고 있다. 무선 PKI의 보안성을 증대시키기 위해서는 강력한 인증절차와 데이터 보호를 위한 상호 인증기능이 필요하다. 무선 PKI에서는 호스트들의 이동성 지원을 위해 무선 환경을 사용하게 되므로 무선 환경에 적합한 인증 프로토콜이 구축되어야 한다.

II. 인증시간 단축을 위한 무선 PKI 설계

상호인증을 구현하기 위해 인증시간을 단축하기 위한 무선 PKI 기반의 인증구조를 제안하고자 한다.

제안한 무선 PKI 인증구조의 인증구조는 CA, 서버, 에이전트 그리고 모바일 노드로 이루어지고, 에이전트는 CA으로부터 필요한 정보를 획득한 후에 CA 역할을 수행할 수 있다. 특히, 인증서 시간단축을 위한 무선 PKI 인증구조에서는 상호 인증과정은 SRP[2] 프로토콜을 바탕으로 실행된다. SRP 프로토콜은 Diffie-Hellman 키 교환 방식에 기반 한 프로토콜로 서버와 에이전트 사이에 키 교환 설정단계에서 이산대수 문제를 이용하여 구성하고, 서버와 에이전트 사이에 상호인증은 해쉬함수를 이용하여 구성된다.

기존의 SRP는 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 인증서 시간단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 상호 인증과정은 설정단계와 실행단계로 구성된다.

1. 인증서 신청방법

서브네트워크 안에 있는 서버와 CA사이에 항상 서로 신뢰관계가 있다고 가정한다. 모바일 노드가 인증서를 신청할 때 신청과정은 다음과 같다.

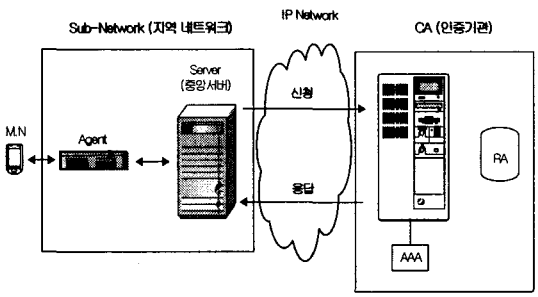
$$MN \Rightarrow Agent \Rightarrow Server \Rightarrow CA$$

CA가 인증서를 발급할 때 발급과정은 다음과 같다.

$$CA \Rightarrow Server \Rightarrow Agent \Rightarrow MN$$

CA가 응답을 하면 CA안에 저장된 모바일 노드의 정보 중에서 필요한 인증서 정보를 서버와 에이전트를 경유하여 모바일 노드에게 전달한다. 여기서, 에이전트와 서버는 상위기관으로부터 발급받은 인증서 1부를 저장하여 보관한다. 만약 인증서 유효기간 동안에 모바일 노드가 인증서를 재신청할 때에는 CA까지 보내지 않고 에이전트에서 인증서 사본을 발급 받는다. 발급된 인증서 유효기간 동안 서버나 에이전트가 CA의 역할을 수행할 수 있다.

그림 2.1은 모바일 노드의 초기 인증서 신청과정에서 모바일 노드가 에이전트와 서버를 경유하여 초기 인증서를 신청하는 과정을 나타낸 것이다.



▶▶ 그림 2.1 모바일 노드의 인증서 신청과정

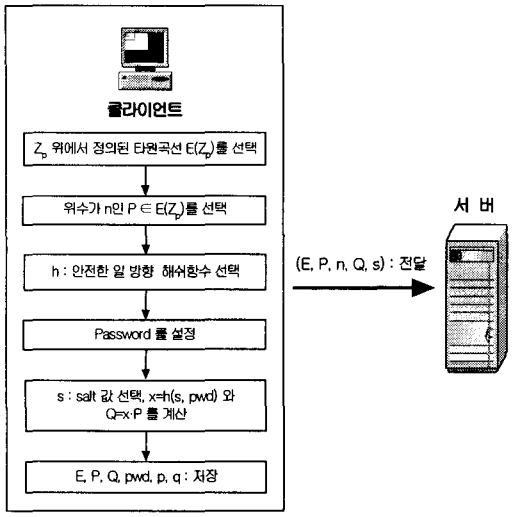
2. 상호 인증과정

상호 인증과정은 SRP[2] 프로토콜을 바탕으로 실행된다. SRP 프로토콜은 Diffie-Hellman 키 교환 방식에 기반 한 프로토콜로 서버와 에이전트 사이에 키 교환 설정단계에서 이산대수 문제를 이용하여 구성하고, 서버와 에이전트 사이에 상호인증은 해쉬함수를 이용하여 구성된다.

기존의 SRP는 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 인증서 획득시간 단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 상호 인증과정은 그림 2-2와 2-3처럼 설정단계와 실행단계로 구성된다.

3. OCSP를 이용한 인증서 갱신 과정

OCSP는 CRL 기반의 인증서 검증 방식의 문제점인 인증서에 대한 실시간 상태검증을 할 수 없는 것을 해결하기 위해 제안된 인증서 상태 검증방식으로 1999년 6월 IETF RFC2560 문서에 의해 공포되었다[3].

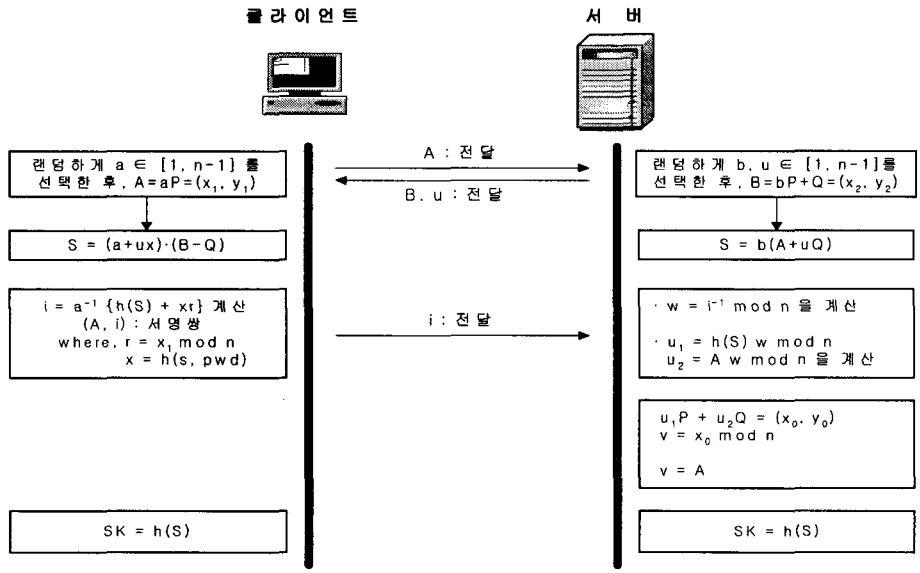


▶▶ 그림 2.2 클라이언트와 서버간의 설정단계

다는 것과 네트워크 상태에 따라 인증서 유효성 검사의 수행시간이 달라진다는 단점이 있다.

OCSP 인증서 상태 검증방식은 클라이언트가 인증서 검증 작업을 수행하기 위한 인증서를 저장한 장소 URL에게 인증서 검증을 요청하고 그 결과만 클라이언트가 받아 작업을 수행하는 방식이다. 클라이언트는 받은 인증서를 OCSP 서버에게 보내서 그 인증서의 정확성 여부를 묻게 된다. 그러면 OCSP 서버가 해당하는 인증서의 검증작업을 해서 클라이언트에게 인증서의 정확성 여부를 알려 주게 된다.

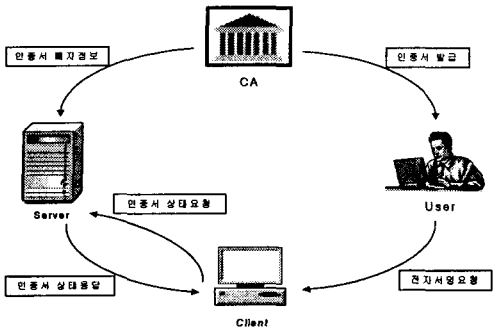
그림 2.4는 인증서 갱신과정을 나타낸 것이다. 인증서 갱신과정은 모바일 노드가 CA로부터 인증서를 발급 받은 후 모바일 노드가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이



▶▶ 그림 2.3 클라이언트와 서버간의 실행단계

OCSP 기반의 인증서 검증방식은 OCSP 클라이언트가 CRL을 요청하지 않고 인증서의 현재 상태를 검증하기 때문에 실시간으로 인증서에 대한 상태검증을 할 수 있다는 장점이 있는 반면 실시간으로 인증서에 대한 유효성 검사를 수행해야 하기 때문에 많은 통신량으로 인한 네트워크 과부하 문제를 발생시킨

언트는 정해진 포맷으로 OCSP 서버에게 인증서 상태정보를 검색하여 전자서명을 수행한 후 수행 결과에 대한 응답을 OCSP 클라이언트로 넘겨줌으로써 실시간으로 인증서에 대한 유효성 검사를 수행한다.



▶▶ 그림 2.4 OCSP 기반의 인증서 갱신과정

III. 제안한 무선 PKI의 실험 및 결과

본 논문에서 인증시간 단축을 위한 무선 PKI 인증구조의 성능을 평가하기 위해 기존의 Sufatrio, K. Lam[4] 인증구조를 실험을 통해 비교·분석하였다.

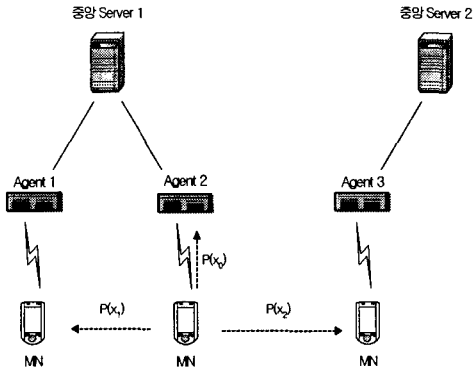
인증 경로길이에 따른 인증서 획득시간에 관하여 실험을 하기 위해서 표 3.1과 같이 파라미터를 정의한다.

[표 3.1] 파라미터의 정의

기호	정의	값
BW_w	유선 링크의 대역폭	1Gbps
BW_{wl}	무선 링크의 대역폭	1Mbps
L_w	유선 링크의 지연	0.5ms
L_{wl}	무선 링크의 지연	7ms
S_{data}	데이터 패킷의 최대 크기	1024byte
S_{reg}	등록 요청 패킷의 크기	50byte
T_{acq}	MN이 무선 채널을 획득하는 시간	20ms
T_{Int}	인터넷에서 노드간 패킷 전달시간	3ms
T_{prot}	등록 패킷을 프로토콜이 처리하는 시간	3ms
T_{reg}	현재 에이전트로부터 등록 패킷을 생성하는 시간	5ms
T_{tun}	프로토콜이 패킷을 터널링하기 위해 소요되는 시간	7ms
T_{wait}	MN이 핸드오버 중 발생되는 평균 패킷 인증시간	400ms

인터넷에서 노드간 패킷 전달시간은 서버가 서로 이웃하고 있을 경우 일정하게 $3ms$라 가정한다.

실험환경은 그림 3.1에서처럼 $P(X_0)$, $P(X_1)$ 그리고 $P(X_2)$은 각각 모바일 노드가 에이전트에 위치할 확률, 모바일 노드가 에이전트에서 다른 에이전트로 이동할 확률, 그리고 모바일 노드가 서버에서 다른 서버로 이동할 확률을 나타낸 것이다.



▶▶ 그림 3.1 모바일 노드의 이동

계층적인 인증서 검증구조를 갖는 X.509 기반의 인증 체계에서는 인증경로가 길어질 경우 인증경로 검증에 대한 지연은 매우 중요한 의미를 갖게 된다.

인증서 획득에 소요되는 총 소요 시간은 모바일 노드 내부의 처리시간을 포함한 무선 구간과 에이전트를 포함한 상위계층의 유선 구간에서 소요되는 시간을 더한 것이다. 무선 구간은 모바일 노드의 무선 채널 획득시간 (T_{acq}), 모바일 노드의 등록 패킷 생성시간 (T_{reg}), 등록 패킷의 전송시간 (S_{reg}/B_{wl}) 그리고 무선 링크의 지연 (L_{wl})과 같은 요소로 이루어진다.

이 요소들을 이용하여 무선 채널을 이용한 에이전트에 인증서 획득을 하기 위한 대기시간을 T_1이라고 하면 다음과 같다.

$$T_1 = T_{acq} + (S_{reg}/BW_{wl}) + L_{wl} + T_{reg} \quad (3\text{-}1)$$

무선 구간에서 패킷 전송에 소요되는 대기시간은 다음과 같다.

$$T_2 = (S_{data}/BW_w) + L_{wl} \quad (3\text{-}2)$$

유선으로 연결된 에이전트 사이의 인증서 획득을 하기 위한 패킷 처리대기시간은 다음과 같다.

$$T_3 = ((S_{reg}/BW_w) + L_w) \times \text{노드의 수} + T_{prot} \quad (3\text{-}3)$$

유선으로 연결된 에이전트 사이의 패킷 전송시간은 다음과 같다(터널링하기 위해 소요되는 시간).

$$T_4 = ((S_{data}/BW_w) + L_w) \times \text{노드의 수} + T_{tun} \quad (3\text{-}4)$$

여기서, 인증서를 획득하기 위한 패킷의 ACK 패킷에 대한 시간은 고려하지 않는다. 서브네트워크 내에서 노드의 수를 l은 4, m은 2, 그리고 s는 1로 한다. 인증서 획득 시간은 다음과 같다. T_{old}은 기존의 인증서 획득시간, T_{new}은 제안한 인증서 시간단축을 위한 인증구조에서의 인증서 획득시간이다.

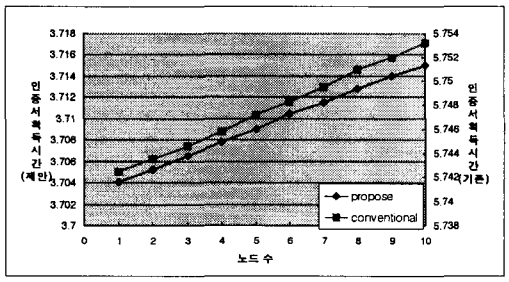
$$T_{old} = (P(X_0) \times (T_1 + T_3 m + 2D)) + (P(X_1) \times (T_1 + T_3 l + 4D)) + (P(X_2) \times (T_1 + 2 \times T_3 m + 4D + k \times D \times T_{Int})) \quad (3\text{-}5)$$

$$T_{new} = (P(X_0) \times (T_1 + T_3 s + D)) + (P X_1) \times (T_1 + T_3 m + 2D)) + (P(X_2) \times (T_1 + T_3 m + 2D + k \times D \times T_{Int})) \quad (3\text{-}6)$$

여기서, $0 < P(X_i) \leq 1$, $i = 0, 1, 2$이고, $\sum_{i=0}^{2} P(X_i) = 1$이다. 그리고 $P(X_0) \geq P(X_1) \geq P(X_2)$이고 $0.3 \leq P(X_0) \leq 1.0$이다.

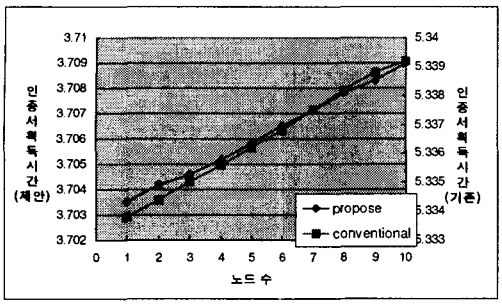
$P(X_0)$, $P(X_1)$ 그리고 $P(X_2)$은 각각 모바일 노드가 에이전트에 위치할 확률, 모바일 노드가 에이전트에서 다른 에이전트로 이동할 확률 그리고 모바일 노드가 서버에서 다른 서버로 이동할 확률을 나타낸 것이다. D는 각 노드에서 발생하는 평균 핸드오버시 인증 대기시간을 의미한다. k는 서브네트워크간의 노드의 수이고, k의 크기는 $1 \leq k \leq 10$이다.

그림 3.2는 모바일 노드가 에이전트 2에 위치할 확률이 $P(X_0) = 0.4$이고, 모바일 노드가 에이전트 1에 위치할 확률이 $P(X_1) = 0.3$이고, 모바일 노드가 다른 서버에 위치할 확률이 $P(X_2) = 0.3$로 정의하였을 때 노드의 수에 따른 기존의 인증서 획득시간과 새로운 인증구조에서의 인증서 획득시간과 비교한 결과를 보여준다.



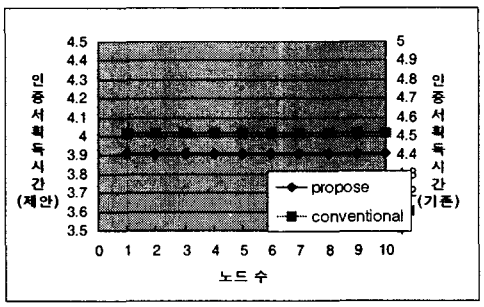
▶▶ 그림 3.2 인증서 획득시간

그림 3.3은 모바일 노드가 에이전트 2에 위치할 확률이 $P(X_0) = 0.5$이고, 모바일 노드가 에이전트 1에 위치할 확률이 $P(X_1) = 0.3$이고, 모바일 노드가 다른 서버에 위치할 확률이 $P(X_2) = 0.2$로 정의하였을 때 노드의 수에 따른 기존의 인증서 획득시간과 새로운 인증구조에서의 인증서 획득시간과 비교한 결과를 보여준다.



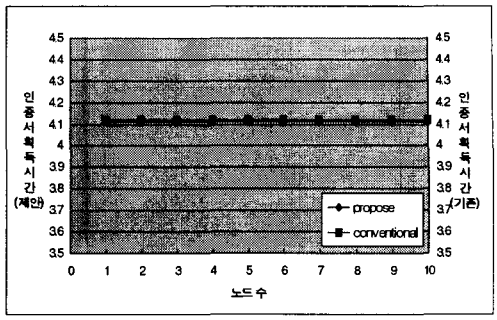
▶▶ 그림 3.3 인증서 획득시간

그림 3.4는 모바일 노드가 에이전트 2에 위치할 확률이 $P(X_0)=0.8$이고, 모바일 노드가 에이전트 1에 위치할 확률이 $P(X_1)=0.1$이고, 모바일 노드가 다른 서버에 위치할 확률이 $P(X_2)=0.1$로 정의하였을 때 노드의 수에 따른 기존의 인증서 획득시간과 새로운 인증구조에서의 인증서 획득시간과 비교한 결과를 보여준다.



▶▶ 그림 3.4 인증서 획득시간

그림 3.5는 모바일 노드가 에이전트 2에 위치할 확률이 $P(X_0)=1.0$이고, 모바일 노드가 에이전트 1에 위치할 확률이 $P(X_1)=0.0$이고, 모바일 노드가 다른 서버에 위치할 확률이 $P(X_2)=0.0$로 정의하였을 때 노드의 수에 따른 기존의 인증서 획득시간과 새로운 인증구조에서의 인증서 획득시간과 비교한 결과를 보여준다.



▶▶ 그림 3.5 인증서 획득시간

IV. 결 론

본 논문에서 제안한 인증서 획득시간 단축을 위한 무선 PKI 인증구조의 성능을 평가하기 위해 기존의 Sufatrio, K. Lam 인증구조를 인증경로 길이에 따른 인증서 획득시간 실험을 통해 비교·분석하였다. 실험 결과 제안한 무선 PKI 인증구조가 기존의 인증구조보다 인증경로 길이에 따른 인증서 획득시간이 우수하다는 사실을 알 수 있었다. 향후 무선 PKI 인증구조에서는 모바일 노드가 사용되는 인증서에 대한 검색시간을 최소화할 수 있는 효율적인 무선 인터넷 서비스를 제공하기 위한 핸드오버를 지원하는 인증구조를 연구하여야 할 것이다.

▌참고문헌▐

[1] R. Anderson and T. Lomas, "Fortifying Key negotiation schemes with poorly chosen passwords," Electronics Letters, 1994, Vol. 30, No. 13.

[2] Thomas Wu, "The Secure Remote Password Protocol", Internet Society Symp., Network and Distributed Systems Security Symposium, 1998, pp. 97-111.

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol -OCSP," RFC2560, 1999.

[4] Sufatrio, K. Lam, "Mobile IP Registration Protocol : A Security Attack and New Secure Minimal Public-Key Based Authentication," I-SPAN'99, June 1999.