韓國 컴퓨터情報學會 論文誌
第10卷 第2號, 2005. 5.

2005-10-2-2-1

큐잉 모델을 이용한 핸드오버 시 인증 대기시간 분석

신승수*, 김덕술**

Analysis for Authentication waiting time in Hand-over using Queueing Model

Seung-Soo Shin*, Duck-Sool Kim**

요 약

본 논문에서는 기존의 무선 PKI에서 키 교환방식의 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 제안한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에 타원곡선을 적용하였다. 제안한 무선 PKI 구조 안에서의 핸드오버 방법은 CRL 검색시간을 단축시킬 수 있으므로 기존의 방법에 비하여 단축된 핸드오버 처리시간을 보여준다. 기존 알고리즘과 제안한 인증구조를 비교하여 실험해 보았을 때 인증 대기시간이 제안한 인증 기법이 모든 환경에서 기존 알고리즘보다 우수한 성능을 보였다.

Abstract

In this paper, a conventional key exchange method simply performs the key exchange setup step based on discrete algebraic subjects. But the mutual-authentication procedure of wireless PKI for reducing authentication time uses an elliptical curve for a key exchange setup step. Proposed hand-over method shows reduced hand-over processing time than conventional method since it can reduce CRL retrieval time. Also, we compared proposed authentication structure and conventional algorithm, and simulation results show that proposed authentication method outperforms conventional algorithm in authentication waiting time.

▸ Keyword : PKI, CRL, Hand-over, Authentication

• 제1저자 : 신승수
• 접수일 : 2005.03.10, 심사완료일 : 2005.05.13
* 동명정보대학교 정보보호학과 교수, ** 동명정보대학교 정보보호학과 교수

Ⅰ. 서 론

정보 유통시 안정성과 신뢰성 확보를 위해 공개키 암호 기술을 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 통신 시 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 사용 중인 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[2],[3].

Ⅱ 장에서는 공개키에 관련된 Jacobs의 공개키 기반의 인증방법[4]와 Sufatrio, K. Lam[5]의 공개키 기반의 인증방법에 대하여 살펴본다. Ⅲ 장에서는 제안한 무선 PKI 인증방법에 대하여 설명하고 Ⅳ 장에서는 기존방법과 제안한 방법을 비교 고찰한다. Ⅴ 장에서는 결론 및 향후 연구 과제를 제시한다.

Ⅱ. 기존 무선 PKI 인증 알고리즘

공개키를 사용하는 '사용자'는 공개키를 사용하기 전에 키에 대한 신뢰성을 제고하기 위해서 인증서 검증을 수행한다. 사용자의 인증서 검증은 사용자의 트러스트 도메인으로부터 인증서 소유자까지의 경로에 해당하는 모든 인증서를 검증하는 과정을 거쳐야 한다. 이러한 과정은 많은 자원을 사용하므로 시스템 성능에 영향을 미치게 된다. 특히, 이동통신 시스템과 같이 사용 가능한 리소스의 양이 상대적으로 적은 경우에는 큰 부담이 될 수 있다.

2.1 Jacobs의 공개키 기반 인증

비밀키를 기반으로 하는 현재의 모바일 IP 인증은 확장이 힘들다는 단점이 있다. 또한, 전자상거래에서 중요한 부인 봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Jacobs는 공개키 기반의 인증방법[4]을 제안하였다.

Jacobs는 모바일 IP 제어 메시지의 인증을 위하여 이동노드와 에이전트간에 X.509 디지털 서명(Digital Certificates), 공개키 그리고 디지털 서명을 사용하였다. 또한, 모든 제어 메시지에 추가되어야 하는 인증 정보를 전달할 새로운 Certificate Extension 메시지 형식을 정의하였다.

Jacobs 프로토콜은 비밀키 기반의 MAC값을 이용하는 대신 공개키를 생성한다는 것을 제외하고는, 기존의 모바일 IP 등록 프로토콜과 같은 동작을 취한다.

그러나 공개키 암호화방식을 사용하면서 Jacobs의 프로토콜은 여러 가지 문제점들이 도출되었다. 그 중 가장 큰 문제점은 이동노드에서의 공개키 암호화기법이 모바일 환경에 맞지 않는다는 것이다.

이동 단말기의 특성상 이동노드에서의 연산 능력에는 제한이 있다. 공개키 기반의 암호화기법을 사용하였을 경우 비밀키 기반의 암호화기법을 사용하였을 때보다 약 1000배의 비용이 증가하므로, 이동노드의 성능을 저하시키는 요인이 된다. 그리고 모바일 환경에서의 낮은 대역폭은 이동노드가 인증기관(CA)으로부터 인증서 폐지목록(CRL: Certification Revocation List)을 전송 받을 수 있을 만큼 충분하지 못

하다. 따라서 이동노드는 주기적으로 인증서 취소 목록을 업데이트 할 경우, 네트워크의 성능이 떨어지게 된다. 공개키를 사용함으로써 발생되는 또 다른 문제점은 이동노드의 시스템의 복잡해진다는 것이다. 공개키와 인증서를 생성하기 위해서는 이동노드에서의 하드웨어나 소프트웨어의 추가가 불가피해진다.

2.2 Sufatrio, K. Lam의 인증 프로토콜

비밀키를 기반으로 하는 현재의 무선 PKI 인증은 확장이 힘들다는 단점이 있다. 또한 전자상거래에서 중요한 부인봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Sufatrio, K. Lam[5]은 공개키 기반의 인증방법을 제안하였다.

Sufatrio, K. Lam은 Jacobs의 인증 프로토콜에서 공개키 기반 암호화의 사용을 줄이는 연구를 하였고, 이 프로토콜은 모바일 IP 등록 프로토콜에서 공개키와 비밀키를 병행하여 사용함으로써 Jacobs의 프로토콜에서 생기는 오버헤드를 줄이는 방법을 제시하였다.

<표 1>은 Sufatrio, K. Lam의 공개키 기반의 인증구조를 설명하기 위한 기본적인 용어를 나타낸 것이다.

표 1. 기존 프로토콜의 용어
Table 1. Definition of Protocol

CA	인증기관
K_{Agent}, K_{Server}, K_{CA}	에이전트, 서버 그리고 CA의 공개키
K^{-1}_{Agent}, K^{-1}_{Server}, K^{-1}_{CA}	에이전트, 서버 그리고 CA의 비밀키
$Cert_{Agent}$, $Cert_{Server}$	에이전트, 서버의 인증서
$<<M>>K^{-1}_{A}$	A의 비밀키를 사용한 메시지 M의 디지털 서명
N_{Agent}	에이전트에서 발행한 nonce
N_{Server}, N_{Agent}, N_{MN}	서버, 에이전트 그리고 모바일 노드의 nonce
MN_{HM}	모바일 노드의 홈 주소
MN_{COA}	모바일 노드의 Care-Of-Address
$Server_{ID}$, $Agent_{ID}$	서버와 에이전트의 IP 주소
$S_{MN-Server}$	모바일 노드와 서버의 비밀키
Advertisement	광고 메시지를 나타내는 비트패턴

기존 프로토콜은 아래와 같은 절차로 진행된다.

▸에이전트 광고 :

(AA) : Agent → MN : M_1, $<<M_1>>K^{-1}_{Agent}$, $Cert_{Agent}$

M_1 = [Advertisement, $Agent_{ID}$, MN_{COA}]

▸인증 과정 :

▪ 단계 1 : MN → Agent : M_2, $<M_2>S_{MN-Agent}$

M_2 = [Request, $Agent_{ID}$, MN_{HM}, MN_{COA}, N_{Server}, N_{MN}, [message in AA]]

▪ 단계 2 : Agent → Server : [message in step 1], N_{Agent}

▪ 단계 3 : Server : (upon receipt of step 2)

* validate $<M_2>S_{MN-Server}$ using $S_{MN-Server}$
* check whether $Agent_{ID}$ in AA1 = $Agent_{ID}$ in M_2
* validate $Cert_{Agent}$ based on existing PKI at $Server$
* validate $<<M_1>>K^{-1}_{Agent}$ using authenticated K_{Agent}

▪ 단계 4 : Server → Agent : M_3, $<<M_3>>K^{-1}_{Server}$, $Cert_{Server}$

M_3 = M_4, N_{Agent}

M_4 = [Reply, Result, $Agent_{ID}$, $Server_{ID}$, MN_{HM}, N'_{Server}, N_{MN}, $<M_4>S_{MN-Server}$]

▪ 단계 5 : Agent

* validate N_{Agent}
* validate $Cert_{Server}$ based on existing PKI at $Agent$
* validate $<<M_3>>K^{-1}_{Server}$ using authenticated K_{Server}
* log this message as a proof of serving

MN(perhaps used in conjunction with the billing protocol)

- 단계 6 : Agent → Server → CA
  : 인증서 검증 요구
- 단계 7 : CA → Server → Agent
  : (upon receipt of step 6)
  * Agent에게 인증서 유효성을 통보
- 단계 8 : CA → Server → Agent → MN
  : 신뢰 정보

III. 무선 PKI 인증구조

상호인증을 구현하기 위해 인증시간을 단축하기 위한 무선 PKI 기반의 인증구조를 제안하고자 한다. 제안한 무선 PKI 인증구조의 인증구조는 CA, 서버, 에이전트 그리고 모바일 노드(MN : Mobile Node)로 이루어지고, 에이전트는 CA으로부터 필요한 정보를 획득한 후에 CA 역할을 수행할 수 있다. 특히, 인증서 시간단축을 위한 무선 PKI 인증구조에서 상호 인증과정은 SRP(Secure Remote Password)[6] 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.

3.1 인증서 신청방법

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

MN ⇒ Agent ⇒ Server ⇒ CA

CA가 인증서를 발급할 때 발급과정은 다음과 같다.

CA ⇒ Server ⇒ Agent ⇒ MN

CA가 응답을 하면 CA안에 저장된 모바일 노드의 정보 중에서 필요한 인증서 정보를 서버와 에이전트를 경유하여 모바일 노드에게 전달한다. 여기서, 에이전트와 서버는 상위 기관으로부터 발급 받은 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 1)은 모바일 노드의 초기 인증서 신청과정에서 모바일 노드가 에이전트와 서버를 경유하여 초기 인증서를 신청하는 과정을 나타낸 것이다.

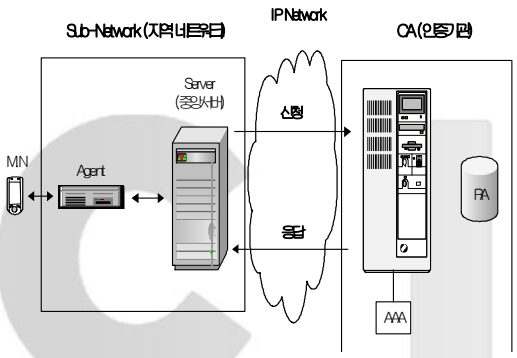

그림 1. 모바일 노드의 인증서 신청과정
Figure 1. Certificate request procedure of mobile node

3.2 상호 인증과정

상호 인증과정은 SRP[6] 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 이산대수 문제에 근거하여 수행되었지만 인증서 획득시간 단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 상호 인증과정은 (그림 2와 3)처럼 설정단계와 실행단계로 구성된다.

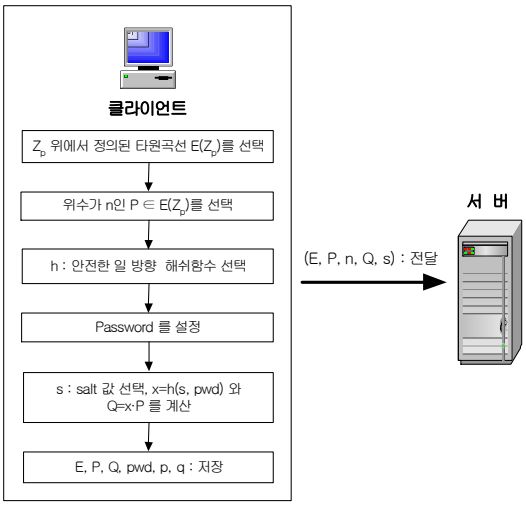

그림 2. 클라이언트와 서버간의 설정단계
Figure 2. Setup step between client and server

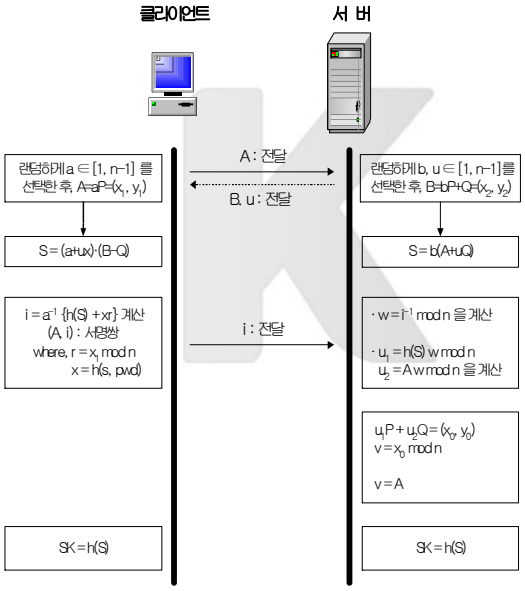

그림 3. 클라이언트와 서버간의 실행단계
Figure 3. Execution step between client and server

3.3 OCSP를 이용한 인증서 갱신 과정

OCSP(Online Certificate Status Protocol)는 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[7].

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 발생시킨다는 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 4)는 인증서 갱신과정을 나타낸 것이다. 인증서 갱신과정은 모바일 노드가 CA로부터 인증서를 발급 받은 후 모바일 노드가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이언트는 정해진 포맷으로 OCSP 서버에게 인증서 상태정보를 검색하여 전자서명을 수행한 후 수행 결과에 대한 응답을 OCSP 클라이언트로 넘겨줌으로써 실시간으로 인증서에 대한 유효성 검사를 수행한다.

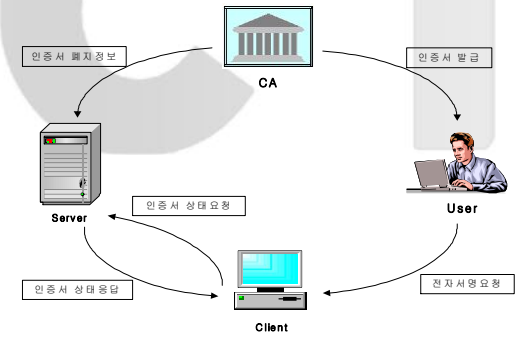

그림 4. OCSP 기반의 인증서 갱신과정
Figure 4. OCSP-based certificate renewal procedure

3.4 서명 및 검증과정

서명 및 검증방법은 ECDSA(Elliptic Curve Digital Signature Algorithm)을 이용해서 하나는 공개키를 구성하고 또 하나는 비밀키를 구성하는데 사용되는 두 세트의 수 체계를 유도하는 작업이 수반된다. 비밀키는 공개키에 의해 암호화된 메시지를 복호화 할 때 사용된다. 발신자는 중앙의 관리자로부터 수신자의 공개키를 찾은 다음, 그 공

개키를 사용하여 보내는 메시지를 암호화할 수 있다. 수신자는 그것을 받아서, 자신의 비밀키로 복호화 하면 된다. 프라이버시를 확실하게 하기 위해 메시지를 암호화하는 것 외에도, 자신의 비밀키를 사용하여 디지털 서명을 암호화해서 함께 보냄으로써, 그 메시지가 틀림없이 바로 발신자에게서 온 것임을 수신자에게 확신시켜줄 수 있다.

(그림 5)는 전자서명 과정을 나타낸 것이다.

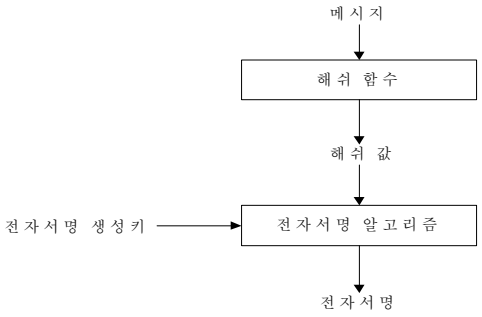

그림 5. 전자서명 과정
Figure 5. Electronic signature procedure

전자서명 검증과정은 우선 수신자는 송신자의 메시지와 함께 전송된 인증서에 포함된 전자서명 검증키를 사용하여 수신된 전자서명으로부터 메시지 해쉬값을 복원 후 수신자가 생성한 메시지의 해쉬값을 서명자가 서명하여 전송한 해쉬값과 비교하여 서명자의 신원 및 메시지의 변조 여부를 확인한다.

다음 (그림 6)은 전자서명 검증과정을 나타낸 것이다.

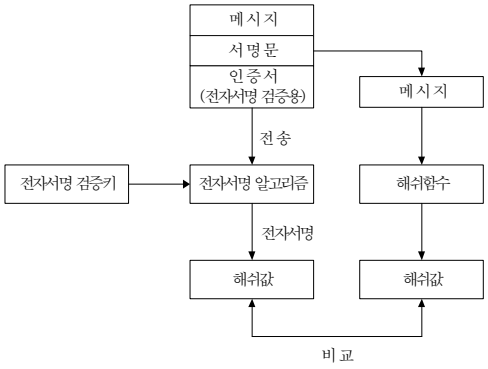

그림 6. 전자서명 검증과정
Figure 6. Electronic signature verification procedure

3.5 핸드오버 시 인증과정

공개키 기반 구조(PKI)를 사용하는 무선 환경의 사용자가 증가함에 따라 인증서 폐지 목록(CRL) 크기도 커질 것이며, 이는 곧 인증시간의 증가를 의미한다. 따라서 모바일 노드의 핸드오버 시 인증과정에서 CRL를 매번 검색하는 것은 많은 시간이 소비되어 효율적인 무선 서비스를 제공할 수 없다. 따라서 모바일 노드의 인증과정에서 CRL 검색과정을 얼마만큼 빠르게 처리하는지가 효율적인 서비스 제공에 중요한 영향을 미치게 된다.

모바일 노드가 이동할 때 에이전트의 SNR(Signal to Noise Ratio)값이 기준치 이하로 떨어지면 새로운 에이전트를 찾기 위하여 스캐닝을 시작하며 가장 큰 SNR을 갖는 에이전트를 선택한다. 이동할 에이전트를 결정한 후에는 모바일 노드와 이동할 에이전트간에 인증과정이 수행된다. 이전 에이전트와 이동할 에이전트는 이미 상호인증을 수행한 신뢰할 수 있는 객체들이기 때문에 이전 에이전트가 수행한 모바일 노드에 대한 인증과정이 끝나기 전까지는 이전 에이전트와 세션을 계속 유지한다.

지역 내에서 핸드오버 할 경우에 에이전트는 OCSP를 통해서 모바일 노드 인증서의 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 모바일 노드에게 서비스를 제공하고 있는 에이전트에게 사용자 인증 무효를 통보한다. 따라서 모바일 노드의 핸드오버 시 인증과정에서 CRL 검색에 소요되는 시간만큼 모바일 노드에게 빠른 핸드오버를 제공할 수 있게 된다. 이 때 사용자 인증은 에이전트와 모바일 노드간에 인증서를 통해 획득한 공개키를 사용하기 때문에 완전인증에 대응하는 안전한 인증과정을 수행하게 된다. (그림 7)은 지역 내에서 핸드오버 시 인증과정을 나타낸다.

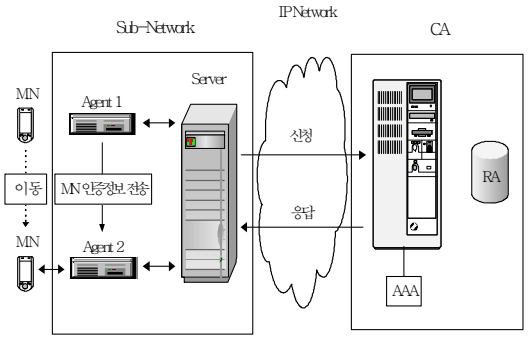

그림 7. 지역 내 핸드오버 과정
Figure 7. The intra-domain hand-over

지역 간에서 핸드오버 할 경우에 서버는 OCSP를 통해서 에이전트의 인증서 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 에이전트에게 서비스를 제공하고 있는 서버에게 사용자 인증무효를 통보한다. 따라서 에이전트의 핸드오버 시 인증과정에서 CRL 검색에 소요되는 시간만큼 에이전트에게 빠른 핸드오버를 제공할 수 있게 된다. (그림 8)은 지역 간에서 핸드오버 시 인증과정을 나타낸 것이다.

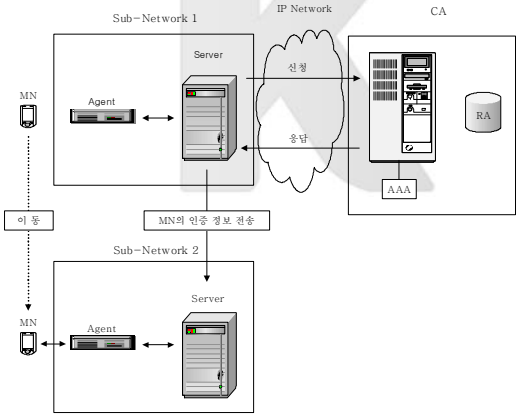

그림 8. 지역 간 핸드오버 과정
Figure 8. The extended intra-domain hand-over

Ⅳ. 실험 및 성능분석

4.1 실험

제안한 무선 PKI 인증구조의 성능을 평가하기 위해 이미 제안된 Jacobs 공개키 기반 인증 알고리즘, Sufatrio. K. Lam 인증 알고리즘들을 핸드오버 시 인증 대기시간에서 성능 분석을 진행하였다.

(그림 9)은 성능 분석을 위한 실험환경을 나타낸 것이다. 그림에서 볼 수 있듯이 초기 인증을 요청하는 단말기가 도착율 λ_2로 발생되고, 핸드오버를 요청하는 단말기는 도착율 λ_1로 발생된다. 특징 에이전트에게 초기 인증을 요청하는 무선 단말기와 핸드오버를 요구하는 무선 단말기의 요청이 모두 존재하는 경우, 에이전트는 우선순위 큐잉에 의해서 핸드오버 시 인증 서비스를 우선적으로 수행하게 된다.

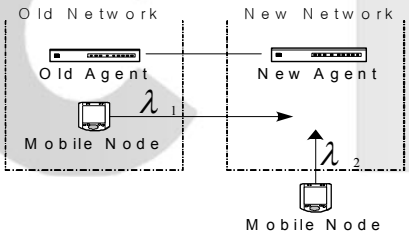

그림 9. 실험 환경
Figure 9. Experiment model

(그림 9)에서 각 에이전트의 큐잉 모델은 (그림 10)과 같이 Q_1, Q_2 두 개의 큐로 구성된다. Q_1는 Q_2보다 높은 우선순위를 가지는 큐로써 핸드오버 시 인증 서비스를 처리한다. Q_1에서 도착율은 λ_1으로 나타낸다. Q_2는 초기 로그인 과정의 인증 서비스를 처리하는 큐로 나타낸다. Q_2에서 도착율은 λ_2로 나타내며 Q_2의 처리 순위는 Q_1보다 낮은 우선순위를 갖는다. Q_1, Q_2는 FIFO(First In First Out)방식을 적용하며, Q_2에서 초기 인증 서비스가 처리중인 경우에 핸드오버 요청이 발생하면 현재 처리 중인 초기

인증 서비스가 끝난 후에 핸드오버를 위한 인증 서비스를 수행하는 비 선점 방식이 적용된다.

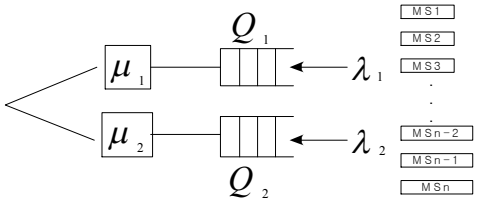

그림 10 큐잉 모델
Figure 10. Queueing model

이와 같은 큐잉 모델에서 각 큐에서의 평균대기시간은 다음 식과 같이 표현할 수 있다[8],[9].

$$E(W_k) = \frac{\sum_{i=1}^{2} \lambda_i E(q_i^2)}{2(1-\sum_{i=1}^{k-1} p_i)(1-\sum_{i=1}^{k} p_i)} \quad (k=1,2) \quad \cdots\cdots (1)$$

위의 식에서 W_1, W_2는 각각 Q_1, Q_2에서의 평균대기시간이고, q_1, q_2는 Q_1, Q_2에서 하나의 인증에 대하여 소요되는 처리시간을 나타내는 랜덤변수이다. p_1, p_2는 각각 초기 인증 및 핸드오버 시 인증으로 인한 서버의 이용률을 나타내는 변수로서 $p_1 = \lambda_1 E(q_1)$, $p_2 = \lambda_2 E(q_2)$의 값을 갖는다. 여기서 E(·)는 대기치를 나타낸다.

위의 식을 이용하여 큐잉 모델에서 핸드오버 시 인증을 위한 인증 대기시간 $E(W_1)$을 구하면 다음과 같다.

$$E(W_1) = \frac{\lambda_1 E(q_1^2) + \lambda_2 E(q_2^2)}{2(1-p_1)} \quad \cdots\cdots (2)$$

또한 초기 인증시 대기시간 $E(W_2)$을 구하면 다음과 같다.

$$E(W_2) = \frac{\lambda_1 E(q_1^2) + \lambda_2 E(q_2^2)}{2(1-p_1-p_2)(1-p_1)} \quad \cdots\cdots (3)$$

본 논문의 실험은 Intel Pentium IV 2G PC에서 Visual C#.NET 언어를 이용하여 수행하였으며, 제안된 인증 구조의 성능 향상 정도를 알아보기 위하여 특정 에이전트에 핸드오버를 요구하는 모바일 단말기의 도착율은 λ_1, 초기 인증을 요구하는 모바일 단말기의 도착율이 λ_2일 때에 이용률 변화에 따른 핸드오버 시 인증 대기시간을 알아보았다. 핸드오버 시에 모바일 대역폭은 2Mbps, 유선 대역폭은 10Mbps, 인증서 크기가 1KB, 공개키 암호/복호 처리 속도를 1.6Mbyte/s로 가정하였다.

새로운 인증 구조와 기존의 인증 구조의 성능 비교는 다음과 같다.

표 2. 인증모델의 성능 비교
Table 2. The result of comparing certificate model

	Jacobs 인증모델	K.Lam 인증모델	새로운 인증모델
상호인증	지원	지원	지원
신뢰도	높음	높음	높음
상호인증 시간	길다	길다	짧다
공개키의 신뢰정점	Root CA	Root CA	Root CA, Server , Agent
신뢰경로 구축	어려움 (Root로부터)	어려움 (Root로부터)	용이 (Server또는 Agent로부터)
적용 환경	유선환경	유·무선환경	유·무선환경
모델의 확장성	낮음	중간	높음
핸드오프시간	길다	중간	짧다
인증 시간	길다	중간	짧다
관리 용이성	어려움	어려움	용이
오버헤드 길이	크다	중간	짧다
처리효율	낮음	중간	높음
자원 사용량	낭비	중간	절약
복잡도	높음	중간	낮음
핸드오프시 CRL 검색 과정	필요	필요	불필요 (대신 OCSP를 사용)

4.2 결과 분석

핸드오버 시 인증 대기시간 결과 분석에 관한 실험은 CRL을 검색하는 시간을 각각 600ms와 900ms로 구분하여 분석한 것이다. 핸드오버 시 인증을 처리하는 Q_1의 이용률이 p_1, 초기인증을 처리하는 Q_2의 이용률이 p_2이므로, 전체 큐의 이용률 p는 $p = p_1 + p_2 < 1$의 관계를 갖는다.

(그림 11)과 (그림 12)는 초기 인증 서비스를 수행하는

p_2가 각각 30%, 50%로 정의하였을 때 CRL 검색시간에 따른 핸드오버 시 기존알고리즘의 평균인증 대기시간과 새로이 제안한 구조의 인증 대기시간과 비교한 결과를 보여준다.

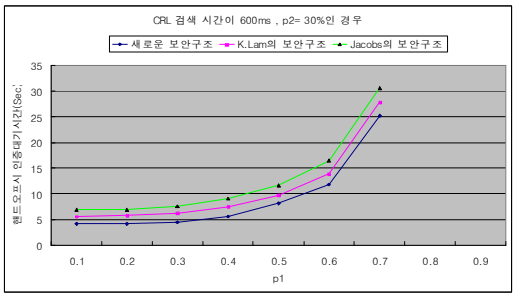

그림 11 (a) CRL 검색 시간이 600ms, p_2=30%인 경우
Figure 11. (a) CRL search time 600ms, in case of p_2=30%

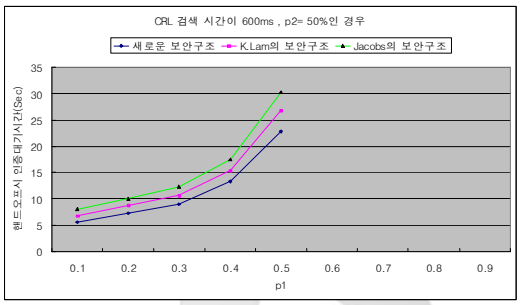

그림 11 (b) CRL 검색 시간이 600ms, p_2=50%인 경우
Figure 11. (b) CRL search time 600ms, in case of p_2=50%

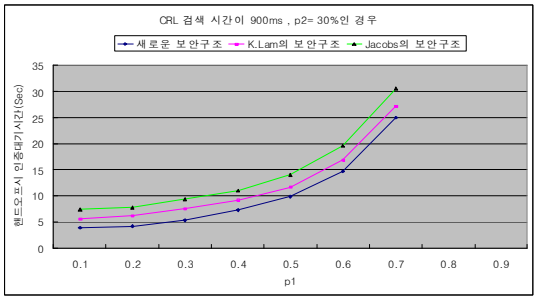

그림 12 (a) CRL 검색 시간이 900ms, p_2=30%인 경우
Figure 12. (a) CRL search time 900ms, in case of p_2=30%

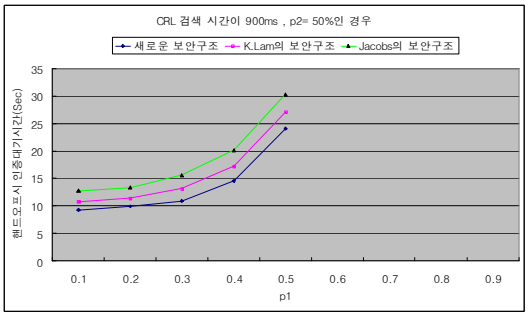

그림 12 (b) CRL 검색 시간이 900ms, p_2=50%인 경우
Figure 12. (b) CRL search time 900ms, in case of p_2=50%

핸드오버 시 인증 대기시간을 살펴보면 기존방법의 경우에는 CRL 검색시간이 증가함에 따라 인증 대기시간도 증가함을 알 수 있다. 그러나 제안된 핸드오버 방식을 사용하였을 경우에는 CRL을 직접 검색하지 않기 때문에 CRL 검색시간 변화에 별다른 영향을 받지 않음을 알 수 있다. 또한 핸드오버 요청이 증가할수록 기존 방법과 제안한 방법의 인증 대기시간 차이가 점차 커짐을 알 수 있다.

V. 결 론

비밀키를 기반으로 하는 현재의 모바일 IP 인증은 확장이 힘들다는 단점이 있다. 또한, 전자상거래에서 중요한 부인 봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Jacobs는 공개키 기반의 인증방법을 사용하였다. 비밀키를 기반으로 하는 현재의 무선 PKI 인증은 확장이 힘들다는 단점이 있다. 또한 전자상거래에서 중요한 부인 봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Sufatrio, K. Lam은 공개키 기반의 인증방법을 사용하였다.

제안한 무선 PKI 인증구조의 성능을 평가하기 위해 이미 제안된 Jacobs 공개키 기반 인증 알고리즘, Sufatrio. K. Lam 인증 알고리즘들을 핸드오버 시 인증 대기시간에서 성

능 분석을 기존방법의 경우에는 CRL 검색시간이 증가함에 따라 인증 대기시간도 증가함을 알 수 있다. 그러나 제안된 핸드오버 방식을 사용하였을 경우에는 CRL을 직접 검색하지 않기 때문에 CRL 검색시간 변화에 별다른 영향을 받지 않음을 알 수 있다. 또한 핸드오버 요청이 증가할수록 기존 방법과 제안한 방법의 인증 대기시간 차이가 점차 커짐을 알 수 있다.

참고문헌

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

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

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

[4] 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.

[5] S. Bellovin and M. Merritt, Augmented Encrypted Key Exchange", in Proceedings of the First ACM Conference on Computer and Communication Security, pp. 244-250, 193.

[6] 신승수, 서정만, "핸드오버시 인증 대기시간 단축을 위한 성능 분석", 한국컴퓨터정보학회, 제9권 3호, pp. 163-169, 2004, 9.

[7] 고병수, 장재혁, 최용락, "디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현". OA학회, 제8권 3호, 2003.

저 자 소 개

신 승 수

2001년 2월 충북대학교 수학과 (이학박사)

2004년 8월 충북대학교 컴퓨터공학과(공학박사)

2005년 3월~현재 동명정보대학교 정보보호학과 교수

김 덕 술

1992년 2월 동아대학교 화공학과 (공학석사)

1996년 3월 일본 오사카대학 생체제어학과(공학박사)

1999년 3월~현재 동명정보대학 정보보호학과 교수