Mobile-IP망에서의 효율적인 인증 방안
(An Efficient Authentication Mechanism in Mobile-IP Network)

정 선 이 † 채 기 준 †† 장 종 수 ††† 손 승 원 †††
(Sunnie Chung) (Kijoon Chae) (Jongsoo Jang) (Sungwon Sohn)

요 약 무선 네트워크의 사용이 증가함에 따라 IETF에서는 Mobile-IP 프로토콜을 이용하여 이동성을 제공하기 위한 방안을 제시하고 있는데, 무선 환경은 외부에 노출되기 쉽기 때문에 안전한 통신을 보장할 수 있어야 한다. IETF의 워킹 그룹은 비밀키 기반 인증 메커니즘, 공개키 기반 인증 메커니즘, 최소 공개키 기반 인증 메커니즘을 제안하고 있으나 각각 확장성, 효율성, 부인방지 서비스 문제로 실제 적용되기에 어려운 상황이다. 본 논문에서는 인증을 위하여 공개키를 사용하되 공개키를 최소로 사용하여 전체 인증 시간을 줄였으며, 이동 노드에게 전자서명을 함으로써 전자상거래와 같이 보안이 중요한 시스템이 있는 네트워크에서 위치 등록에 대한 부인방지 서비스를 제공하였다. 시뮬레이션을 위해 SDL을 이용하였으며 시뮬레이션 결과를 통해 제안된 인증 메커니즘의 전체 등록 시간이 짧다는 것을 확인할 수 있었다. 특히 이동 노드에서의 계산 비용 감소는 이동 노드가 가진 전력 제약 문제를 해결하였다. 제안된 인증 메커니즘은 Mobile-IP가 실제로 사용되는 매크로 셀 환경에서 보다 효율적으로 작동한다.

Abstract The explosive growth in wireless networking increasingly urges the demand to support mobility within the Internet which is what Mobile-IP aims to provide. Because the transmission of signals through open-air is easy to be attacked, it is important to provide secure transmission for mobile users and make them responsible for what they have done in networks. Although IETF provides a secret-key based security mechanism, a public-key based security mechanism and minimal public-key based security mechanism, those mechanisms suffer from scalability, efficiency and non-repudiation service problem.. The proposed mechanism uses public-key based authentication optimizing the performance. It includes non-repudiation service on the side of mobile for airtight security in wireless network. The simulation results show that the proposed authentication reduces the total registration time. It especially minimizes the computation cost on the side of the mobile node and solves the power problem. In practice, the proposed authentication is feasible with reasonable performance and security service in macro mobility that Mobile-IP is intended to solve.

1. 서 론

최근에 인터넷 사용과 무선 네트워크의 성장이 두드러짐에 따라 기존의 유선 사용자뿐만 아니라 이동 사용자도 어디에 위치하던 전자상거래와 같은 다양한 서비스에 자유롭게 접근하고 싶어한다. Mobile-IP는 이런 이동성을 제공하기 위해 제시된 IP 프로토콜로 이동 사용자가 일시적으로 다른 서브넷으로 이동해도 지속적인 서비스를 제공해줄 수 있다. 그러나 무선 네트워크에서의 시그널 전송은 공격 당하기 쉬워 이동 사용자에게 안전한 데이타를 전송하는 것이 어렵기 때문에 보안은 Mobile-IP 구조에서 빼놓을 수 없는 중요한 요소이다.

Mobile-IP에서는 이동 사용자가 새 위치 정보를 등록한 후 모든 데이타가 그 경로로 전송된다는 점에서 등록 과정은 무척 중요한 과정이 아닐 수 없다. 또한 이동 사용자가 전자상거래와 같은 시스템에서 행한 행동에는 책임이 크기 때문에 이동 사용자가 네트워크에서 한 행

† 비 회 원 : Lucent Technologies 연구원
sunnie@lucent.com
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
kjchae@cwha.ac.kr
††† 비 회 원 : 한국전자통신연구원 정보보호기술연구본부 연구원
jsjang@etri.re.kr
swsohn@etri.re.kr
논문접수 : 2001년 2월 19일
심사완료 : 2001년 5월 24일

동에 대하여 책임을 질 수 있는 서비스가 있어야 한다.

IETF의 RFC2002에서는 Mobile-IP망에서 비밀키 기반 인증 메커니즘을 제시하고 있으나 키 분배에 있어서 확장성이 떨어지며, 이 문제를 해결하기 위하여 draft로 제안된 공개키 기반 인증 메커니즘은 공개키 동작이 복잡하다는 면에서 전체적인 인증시간이 길다는 단점이 있다. 또한 최근에 논문에서는 공개키 사용을 최소로 줄여 효율성을 높인 최소 공개키 기반 인증 메커니즘이 제시되었으나 이동 노드가 공개키를 이용한 전자서명을 하지 않기 때문에 부인방지 서비스가 결여되어 있다.

본 논문의 목적은 이동 사용자가 네트워크를 사용하기 위하여 Mobile-IP 상에서 이동성을 제공하는 것으로, 원활한 네트워크 이용을 위하여 안전하고 효율적인 인증 메커니즘을 제안하는 것이다. Mobile-IP가 이용되기 위해서는 이동 노드에 부인방지 서비스가 제공되어야 하며 부인방지 서비스는 공개키를 기반으로 한 전자서명을 할 때 가능하다. 그러나 공개키 사용에 있어서 공개키 계산이 복잡하여 전체 인증 시간이 증가한다는 점과 공개키 확인을 위하여 인증 기관에 접근하는 시간이 길다는 점을 고려하여 전체 인증이 효율적으로 이루어질 수 있도록 해야 한다. 따라서 제안된 인증 메커니즘에서는 공개키 사용을 최소로 하여 인증 시간을 줄이면서도 이동 노드에게 전자서명을 함으로써 부인방지 서비스를 제공하고자 한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 이동성 제공을 위하여 IETF에서 제안한 Mobile-IP 동작에 대하여 알아보고, Mobile-IP에서 새로운 위치 정보를 등록시키는 기존 인증 메커니즘에 대하여 설명한다. 3장에서는 기존 인증 메커니즘의 장단점을 인증 참여자, 인증 서비스, 암호 알고리즘 면으로 비교분석하여 새로운 인증 메커니즘에서 필요한 서비스를 제안하도록 한다. 4장에서는 제안된 인증 메커니즘의 모델링 구조에 대하여 상세히 설명하고, 기존 인증 메커니즘을 시뮬레이션하여 성능을 비교분석한다. 마지막으로 5장에서는 본 논문의 연구 결과와 향후 연구 계획에 대하여 기술한다.

2. Mobile-IP에서의 기존 인증 메커니즘 고찰

초기에는 모든 컴퓨터의 위치가 고정되어 있다는 가정 하에 네트워크를 구성하였으나 점점 많은 수의 컴퓨터들이 고정되지 않은 상태로 네트워크에 접속하게 되었다. 모든 컴퓨터는 항상 통신을 할 수 있는 상태를 유지해야 하기 때문에 컴퓨터 통신 기술에서 이런 이동성까지 지원해야 한다.

IP에서 이동성을 제공하는 방법으로 IETF에서는 1992년 Mobile-IP 워킹그룹을 결성하여 접속되는 위치가 반드시 고정적으로 지정되어 있던 기존 IP 프로토콜에 단말기의 이동성을 제공하는 Mobile-IP를 제안하였다. Mobile-IP 프로토콜은 IETF의 RFC2002에 기술되어 있으며, 이동 노드가 인터넷에서 연결지점을 바꾸는 동안에도 이동 노드와 통신 노드 사이에 IP 데이타그램을 전달하도록 하는 프로토콜이다.

● Mobile-IP 용어

- 이동 노드(Mobile Node: MN) : 자신의 IP 주소를 바꾸지 않고, 한 네트워크 또는 서브 네트워크에서 다른 네트워크로 이동한 호스트나 라우터로 어디에 위치하든 자신의 IP 주소를 사용해서 인터넷과 통신을 계속할 수 있다.
- 홈 네트워크(Home Network) : 이동 노드가 연결을 처음 시작한 네트워크로 이동 노드는 여기서 고정된 IP 주소를 받는다.
- 외부 네트워크(Foreign Network) : 이동 노드가 이동하여 방문한 다른 네트워크나 서브 네트워크로 여기서 임시 IP 주소를 부여 받는다.
- 고정 IP 주소 : 이동 노드가 처음으로 연결을 시작한 홈 네트워크에서 받은 주소로 이동 노드와 통신하고자 하는 송신자가 목적지 주소로 이용하는 고정된 IP 주소이다.
- COA(Care-of-Address) : 이동 노드가 외부 에이전트에 등록시 얻는 새로운 주소로 이동 노드로 향하는 터널의 종료 지점이다. 이동 노드는 자신의 홈 네트워크에서 부여 받은 고정 IP 주소를 가지고 있으며, 멀리 이동하였을 때에는 새로 연결된 네트워크에서 임시 COA를 얻는다.
- 홈 에이전트(Home Agent: HA) : 이동 노드의 홈 네트워크의 라우터로 이동 노드에 대한 현재 위치 정보를 유지하면서 이동 노드가 홈 네트워크를 떠났을 때, 이동 노드로 향하는 데이타그램을 전송해 준다.
- 외부 에이전트(Foreign Agent: FA) : 이동 노드가 방문해 있는 네트워크에 위치하는 라우터로 이동 노드가 멀리 떨어져 있는 동안 홈 에이전트와 협력해서 이동 노드에 데이타그램을 전송해 준다.
  에이전트 광고(Agent Advertisement) : 외부 에이전트는 라우터 광고 메시지에 특별한 광고 메시지를 붙인 메시지를 통해 자신의 존재를 알린다.
- 통신 노드(Correspondent Node: CN) : 이동 노드가 통신하는 상대로 이동하는 노드이거나 위치가 고정된 노드이다.

- 이동성 결합(Mobility binding) : 홈 주소와 COA를 결합시키는 과정을 의미한다.
- 터널(Tunnel) : 이동 노드가 홈 네트워크를 떠났을 때 이동 노드로 향하는 데이타그램을 보내기 위해서 홈 에이전트와 외부 에이전트 사이에 생성되는 길로서, 이때 데이타그램은 인캡슐레이트되어 터널을 따라 전송된 후 외부 에이전트에서 디캡슐레이트되어 최종 이동 노드로 전송 된다.

Mobile-IP에서는 두개의 IP 주소를 이용하는데, 먼저 이동 노드는 처음 연결을 시작한 홈 네트워크에서 고정 IP 주소를 할당 받고 외부 네트워크로 이동함에 따라 외부 네트워크에 위치하는 외부 에이전트로부터 COA라는 임시 IP 주소를 할당 받는다. 이 두개의 IP 주소가 결합되어 사용되며, 데이타가 전송되는 과정은 통신 노드가 홈 네트워크에 의해 제공되는 고정 IP 주소로 데이타를 보내면 홈 네트워크에 위치한 라우터가 이 데이타를 외부 네트워크의 임시 IP 주소로 재전송해주는 과정으로 이루어진다.

이동 노드가 홈 에이전트에게 새 위치정보를 등록하는 과정은 에이전트 광고, 등록 요청, 등록 대답의 3단계로 나뉜다.

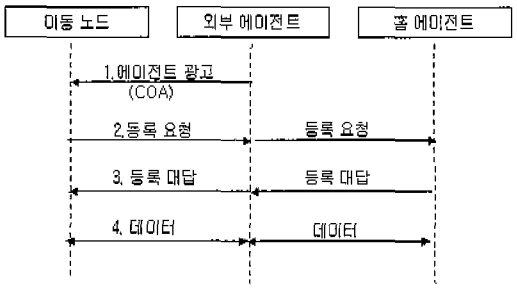


그림 1 Mobile-IP 등록 과정

1단계에서 외부 에이전트는 에이전트 광고를 이용하여 이동 노드에게 COA를 제공한다. 이동 노드는 이 메시지가 홈 네트워크로부터 온 것인지 외부 네트워크로부터 온 것인지 결정하여, 외부 네트워크에서 받은 것이면 에이전트 광고에 들어있는 COA를 새로운 임시 IP 주소로 부여 받는다[1]. 2단계와 3단계에서는 이동 노드가 외부 에이전트에게서 받은 새 COA를 홈 에이전트에게 등록하기 위하여 등록 요청을 하고 결과로 등록 대답을 받는다. 등록 과정을 마치면 이동 노드와 데이타그램을 주고 받을 수 있다[2]. 홈 에이전트는 이동 노드의 고정 IP 주소와 COA를 결합시켜 registration lifetime이 끝날 때까지 보관한다. 다른 노드는 이동 노드가 홈 네트워크에서 떠나간 것을 모르기 때문에 고정 IP 주소로 보내게 되고 홈 에이전트가 전송된 데이타그램을 가로채 임시 COA로 터널링한다[3].

모든 데이타가 홈 네트워크에서 새로 이동한 외부 네트워크로 재전송된다는 점을 생각할 때 이동 노드의 새로운 위치 정보를 홈 네트워크에 등록하는 과정은 중요한 부분이 아닐 수 없다. 만약 악의를 가진 사용자가 이동 노드임을 가장하고 등록을 시도할 경우 틀린 COA를 홈 에이전트의 라우팅 테이블에 잘못 등록시키게 된다. 따라서 홈 에이전트는 등록 메시지가 올바른 이동 노드에서 왔다는 확신이 있어야 한다. 이동 노드의 인증 부분을 다루는 기존의 메커니즘으로는 비밀키를 기반으로 한 인증 메커니즘과 공개키를 기반으로 한 인증 메커니즘, 공개키를 최소로 사용하는 인증 메커니즘이 있다. 인증 메커니즘을 설명하기 위한 표기법은 다음과 같다.

● 인증 메커니즘 표기법

- MN, FA, HA : 각각 이동 노드, 외부 에이전트, 홈 에이전트
- CA : 인증 기관(Certificate Authority)
- S_{MN-HA} : MN와 HA 사이 공유하는 비밀키
- K_{MN}, K_{HA}, K_{FA}, K_{CA} : MN, HA, FA, CA 각각의 공개키
- K^{-1}_{HA}, K^{-1}_{FA}, K^{-1}_{CA} : MN, HA, FA, CA 각각의 개인키
- MN_{HM} : MN의 고정 IP 주소
- MN_{COA} : MN의 COA
- HA_{id} : ID로서 HA의 IP 주소
- FA_{id} : ID로서 FA의 IP 주소
- N_{MN}, N_{HA} : MN, HA 각각의 넌스(Nonce)
- {M}K : 메시지 M을 키 K로 암호화한 값
- <M>K : 메시지 M에 대하여 키 K로 얻은 MAC (Message Authentication Code)
- $<<M>>K^{-1}_{A}$: 메시지 M에 대하여 A의 개인키로 서명한 전자서명
- $Cert_{HA}$, $Cert_{FA}$: HA, FA 각각의 인증서

2.1 비밀키 기반 인증 메커니즘

Mobile-IP에서는 인증과 제어 메시지의 무결성을 보장하기 위하여 MAC을 의무로 한다. 등록 요청을 안전하게 전송하기 위하여 각 메시지에 유일한 데이타를 포함시킴으로써 다른 등록 요청이 같은 해쉬값을 가지지 못하도록 한다. 이동 노드는 홈 에이전트와 미리 나누어 가진 비밀키를 가지고 등록 요청에 대해 MD5(Message Digest 5) 해쉬 함수를 수행하여 다이제스트 메시지를

얻어 요청에 덧붙여 전달하면 홈 에이전트는 같은 비밀키를 이용하여 전달받은 등록 요청에 대해 해쉬 함수를 수행하여 덧붙어온 내용과 일치하는지 확인한다. 이와 같은 과정으로 이동 노드는 홈 에이전트에게 인증을 받으며 홈 에이전트에서 이동 노드로 보내는 등록 대답의 경우에도 같은 방법으로 인증 받는다.

또한 재공격(Replay Attack)을 막기 위해서는 이동 노드와 홈 에이전트 사이에 난수를 발생시켜 주고 받거나 타임스탬프(Timestamp)를 이용하여 제한된 시간 내에만 사용할 수 있도록 한다. 이와 같은 방법으로 악의를 가진 사용자가 돌아다니는 유효한 등록 메시지를 가로채 등록정보를 빼낸 후 재등록 하는 것을 방지할 수 있다. 아래는 임의의 수인 넌스를 이용한 비밀키 기반 인증 메커니즘을 표기한 것이다.

● From previous HA's reply

HA → MN : N_{HA}

● Registration

MN → FA : M_1, $<M1>S_{MN-HA}$

where M_1 = Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}

FA → HA: M_1, $<M_1>S_{MN-HA}$

- verify $< M_1>S_{MN-HA}$ using S_{MN-HA}

HA → FA: M_3, $<M_3>S_{MN-HA}$

where M3 = Reply, Result, FAid, HAid, MNHM, N'HA, NMN

FA → MN: M_3, $<M_3>S_{MN-HA}$

- verify $< M_2>S_{MN-HA}$ using S_{MN-HA}

이 방법은 간단하게 등록 메시지의 보안을 제공하는 듯 보이지만 실제로는 이동 노드와 홈 에이전트 사이의 인증만 보장한다. 외부 에이전트는 단지 수동적으로 받은 등록 요청과 등록 대답을 전달해주는 역할 외에는 하지 않는다.

2.2 공개키 기반 인증 메커니즘

비밀키 기반 인증 메커니즘은 상대와 통신을 하기 전에 안전한 방법으로 상대방과 비밀키를 나눠 가져야 한다. 그러나 비밀키는 키 분배 방법에 있어서 유연성이 떨어지고 특히 많은 사용자를 수용하기에는 적당하지 못하다는 한계점이 있다. 또한 상업적인 면에서 필요한 부인방지 서비스가 없다는 면을 극복하기 위하여 공개키를 기반으로 한 인증 메커니즘이 제시되었다.

비밀키 기반 메커니즘이 MAC 값을 사용하는 반면 공개키 기반 메커니즘은 공개키를 이용한 전자서명을 사용한다. 공개키 기반 인증 메커니즘에서는 인증과 관련된 내용을 담은 certificate extension을 모든 제어 메시지 뒤에 붙도록 정의하여 인증과 관련된 정보를 주고 받는다.

● Agent Advertisement

FA → MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$

MN
- validate $Cert_{FA}$ using K_{CA}
- verify $<<M_1>>K^{-1}_{FA}$ using K_{FA}

● Registration

MN → FA : M_2, $<<M_2>>K^{-1}_{MN}$, $Cert_{MN}$

FA
- validate Cert $_{MN}$ using K_{CA}
- verify $<<M_2>>K^{-1}_{MN}$ using K_{MN}

FA → HA
- delete $Cert_{MN}$

: M_3, $<<M_3>>K^{-1}_{FA}$, $Cert_{FA}$

HA
- validate $Cert_{FA}$ using K_{CA}
- verify $<<M_3>>K^{-1}_{FA}$ using K_{FA}
- verify $<<M_2>>K^{-1}_{MN}$ using K_{MN} (from $Cert_{MN}$ already has)

HA → FA : M_4, $<<M_4>K^{-1}_{HA}$, $Cert_{HA}$

FA
- validate $Cert_{HA}$
- verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}

FA → MN
- delete $Cert_{HA}$

: M_5, $<<M_5>>K^{-1}_{FA}$

MN
- verify $<<M_5>>K^{-1}_{FA}$ using K_{FA} (from $Cert_{FA}$ already has)
- verify $<<M_4>>K^{-1}_{HA}$ using K_{HA} (from $Cert_{HA}$ already has)

여기서는 이동 노드, 외부 에이전트, 홈 에이전트 간에 서로에 대한 인증을 한다. 메시지를 새로 만들거나 받은 메시지를 전달하는 경우 메시지 뒤에 전자서명을 추가함으로써 메시지가 변하지 않았다는 것을 확인시키고, 또한 자신이 메시지를 만들었음을 증명할 수 있다.

2.3 최소 공개키 인증 메커니즘

최소 공개키 인증 메커니즘은 공개키 기반 인증이 가진 단점을 줄인 방법으로 공개키 암호화를 최소로 사용한다.

● Agent Advertisement

FA → MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$

● Registration

MN → FA : M_2, $<<M_2>>S_{MN-HA}$

where M_2=Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}, [message in agent advertisement]

FA → HA : [message in MN FA step], N_{FA}

HA
- validate <M2> S_{MN-HA} using $S_{MN\ HA}$

- check whether FA_{id} in M1 and FA_{id} in M_2 is identical
- validate $Cert_{FA}$ based on existing PKI at HA
- validate $<<M_1>>K^{-1}_{FA}$ using authenticated K_{FA}

HA → FA : M_3, $<<M_3>K^{-1}_{HA}$, $Cert_{HA}$
where $M_3=M_4$, N_{FA}
M_4=Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}, $<M_4>S_{MN-HA}$

FA
- validate N_{FA}
- validate $Cert_{HA}$ based on existing PKI at FA
- validate $<<M_3>>K^{-1}_{HA}$ using authenticated K_{HA}
- log this msg as a proof of serving MN (perhaps used in conjunction with the billing protocol)

FA → MN : M_4

MN
- validate $<M_4>S_{MN-HA}$ using S_{MN-HA}
- verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}(from $Cert_{HA}$ already has)

이동 노드는 모든 암호화 동작을 비밀키 기반으로 수행하며, CRL(Certificate Revocation List) 접근과 인증서 증명과 같은 무거운 작업에 대해서 벗어난다. 이동 노드는 홈 에이전트를 비밀키로 인증하며 외부 에이전트에 대해서는 홈 에이전트로부터 등록 대답을 받음으로써 외부 에이전트의 인증서가 유효하다는 것을 간접적으로 보장 받게 된다. 인증서를 캐쉬에 저장하여 후에 사용할 때 효율을 높일 수 있다. 그러나 만약 이동 노드가 공개키 기반 암호화를 수행할 수 있을 정도로 자원이 풍부하다면 홈 에이전트가 제공하는 서비스와 무관하게 선택적으로 공개키 기반 인증을 할 수도 있다. 외부 에이전트는 이동 노드에 대해 홈 에이전트가 이동 노드에게 돌려준 등록 대답에서 간접적으로 인증 받으며 홈 에이전트와는 직접적으로 공개키 기반 인증을 수행한다. 이동 노드는 홈 에이전트와 언제나 비밀키 기반 보안 조합(Security Association)을 유지하기 때문에 이동 노드와 홈 에이전트 사이에 부인 방지서비스가 제공되지 않는다.

3. 제안하는 Mobile-IP 인증 메커니즘

본 장에서는 기존 인증 메커니즘의 장단점을 비교하고 사용 암호 알고리즘에 대하여 분석하여 새로운 Mobile-IP 인증 방안을 제시하고자 한다.

3.1 기존 인증 메커니즘의 문제점 및 분석

안전하고 효율적인 인증을 위하여 인증 참여자, 인증 서비스, 암호 알고리즘에 대하여 기존 인증 메커니즘을 분석하여 본다.

3.1.1 인증 참여자

비밀키 기반 인증 메커니즘에서의 인증은 기본적으로 이동 노드와 홈 에이전트 둘 사이에서 이루어진다. 이동 노드는 등록 요청시 비밀키와 보호된 필드에 대한 MAC을 첨부시켜 홈 에이전트에게 인증 받고, 홈 에이전트도 등록 대답시 동일한 방법으로 이동 노드에게 인증 받는다. 그러나 인증에 참여하는 외부 에이전트의 역할은 전달 받은 메시지를 전달해주는 소극적인 역할만을 수행하여 보안이 완전하지 못하다.

공개키 기반 인증 메커니즘은 세 참여자 서로에 대한 인증을 메시지를 받고 전달할 때마다 수행한다. 등록과정에 참여하는 세 참여자가 모두 서로에 대한 신뢰있는 인증을 할 수 있기 때문에 보안면에서 이상적이나 반복되는 인증은 성능의 저하를 가져온다.

최소 공개키 기반 인증 메커니즘 역시 세 참여자 모두 인증에 참여하되 간접적인 인증을 통해 인증 횟수를 줄이고 비밀키 인증의 사용하여 인증에 필요한 오버헤드를 줄였다. 외부 에이전트는 이동 노드로부터 등록 요청을 받으면 인증 작업을 수행하지 않고 자신이 보냈던 에이전트 광고의 값이 유효한 것인가만 검사한다. 이동 노드가 외부 에이전트를 직접 인증하지 않고 홈 에이전트가 인증한 결과를 받음으로써 간접적으로 공개키 인증 효과를 가짐으로써 모든 인증 참여자에 대한 인증이 가능하다. 이 방법은 외부 에이전트의 인증까지 유지하는 동시에 외부 에이전트의 공개키 인증 부분은 홈 에이전트에게 넘겨 성능 저하를 감소시켰다.

따라서 안전한 인증을 위하여는 인증 참여자 모두를 인증하여야 하고 동시에 효율을 높이기 위하여 기본적으로 반복되는 공개키 인증의 횟수를 줄이고 이동 노드에게는 계산이 비교적 간단한 비밀키 인증을 시키는 방법으로 이루어져야 한다.

3.1.2 인증 서비스

문서의 전자적인 교환이 일반화되면서 문서의 인위적인 변조나 여러 가지 결함 때문에 문제가 많다. 따라서 일반적인 종이문서에 상호 서명이나 도장을 찍는 것과 같이 전자문서의 송신자와 수신자간에 문서내용에 전자서명을 하는 방식이 필요하다.

비밀키 기반 암호 메커니즘에서는 넌스나 타임스탬프를 사용하여 재사용하지 못하게 하며 원문에 대해 유일

하게 생성되는 인증 코드를 덧붙여서 인증 받고 문서 내용이 변경되지 않음을 증명할 수 있다. 그러나 암호화하는 키와 복호화하는 키가 동일하여 비밀키가 누설되었을 경우 누구든지 MAC을 생성해낼 수 있어 MAC에는 부인방지 기능이 없다.

공개키 기반 인증 메커니즘에서 역시 넌스나 타임스탬프로 재사용하지 못하게 하며 원문에 대하여 전자서명을 함으로써 인증 받고 내용이 변경되지 않음을 증명한다. 공개키 기반 시스템은 개인키와 공개키의 쌍으로 이루어져 이 중 공개키만 외부에 노출되어 있고 개인키는 어떠한 경우에도 개인키 소유자에게만 알려져 있다. 따라서 개인키 소유자가 개인키를 노출시키지 않는 한 누구도 올바로 암호화할 수 없다. 암호화를 할 수 있는 자가 유일하다는 특성은 자신이 제공한 서비스에 대하여 후에 부인할 수 없게 한다. 이것을 전자서명이 제공하는 부인방지 서비스라고 하며 이동하는 노드가 책임을 가지고 네트워크 자원을 사용하도록 한다.

최소 공개키 기반 인증 메커니즘은 공개키를 사용하여 확장성을 높이면서도 이동 노드가 해야 하는 인증 관련 관리와 이동 노드에게 부여된 공개키 계산을 최소로 줄였다. 그러나 이동 노드와 홈 에이전트 사이에는 비밀키를 이용하여 MAC을 생성하였기 때문에 부인방지 서비스가 결여되어 있다. 외부 에이전트와 홈 에이전트 사이에서는 공개키를 이용한 전자서명을 교환하기 때문에 네트워크에서 제공한 것에 대하여 부인할 수 없다. 다만 홈 에이전트는 외부 에이전트에게 공개키로 전자서명을 보냄으로써 이동 노드에게 제공한 서비스에 대하여 부인할 수 없다. 그러나 전자상거래와 같이 보안이 중요한 환경에서 이동 노드의 위치 등록에 대한 부인방지 서비스가 결여되어 있다.

3.1.3 암호 알고리즘의 분석

현재 IETF RFC2002에서 지정해 놓은 표준 Mobile-IP의 인증 메커니즘은 비밀키 기반으로 RFC 1321에 정의된 해쉬 함수 MD5를 이용한다. 해쉬 함수는 임의의 입력 비트 열에 대하여 일정한 길이의 안전한 비트 열을 출력하는 것이다. 입력 데이타 스트링을 고정된 길이의 출력인 해쉬 코드로 대응시키는 함수로서 주어진 해쉬 코드에 대하여 이 해쉬 코드를 생성하는 데이타 스트링을 찾아내는 것은 계산상 실행 불가능하며, 주어진 데이타 스트링에 대하여 같은 해쉬 코드를 생성하는 또 다른 데이타 스트링을 찾아내는 것은 계산상 실행 불가능하다. MD5는 Ron Rivest가 1990년 개발한 MD4 알고리즘을 개선한 것으로 충돌률이 일어날 가능성이 적은 크기인 128 bits 의 해쉬를 만든다. 적은 계산 비용과 빠른 계산 속도면에 있어서 공개키에 비하여 우수하지만 RFC2002에 따라 동작하는 비밀키가 이동 노드와 홈 에이전트 사이에 미리 분배되어야 한다는 문제로 확장성이 떨어진다[4].

이에 반하여 공개키 인증 메커니즘에서는 이동 노드가 인증서를 기반으로 한 공개키 암호작동을 하도록 요구한다. 공개키 기반 인증 메커니즘은 IETF의 draft로 제시되어 있으며 마찬가지로 어떤 알고리즘이든 사용할 수 있으나 기본적으로 512 bits 키를 사용한 RSA를 제안한다. 보안상의 강점에도 불구하고 암복호화의 비용이 높아 인증서를 증명하기 위한 인증서 검증 작업과 함께 이동 노드에게 성능 저하를 가져온다. 특히 공개키 동작이 일반적으로 비밀키 동작에 비하여 100 ~1,000배 이상 복잡하다는 것을 생각할 때 공개키 방식은 상당히 부담스럽다. 일반적으로 자원이 제약되어 있는 이동 노드에게는 인증서를 발급하는 동작은 상당히 무거운 작업이다. 인증서 발급으로 인하여 공개키 기반 인증 메커니즘의 경우 등록 단계에서만 X.509로 정의된 인증 기관에 4번이나 접근하여 인증서 확인 결과를 기다려야 한다. 그런데 이동 노드가 일반적으로 자원이 한정되어 있어 계산할 수 있는 파워가 부족하다는 점과 홈 네트워크에서 멀어질수록 인증 기관에서 메시지를 주고 받는 시간이 길어진다는 면에서 이러한 동작은 손쉬운 것이 아니다.

최소 공개키 기반 인증 메커니즘에서는 이동 노드가 인증 기관에 접근하여 인증서를 발급 받고 유효한 인증서인지 확인하기 위하여 CRL에 접근해야 하는 복잡한 작업에서 해방되었다. 이동 노드는 홈 에이전트와 비밀키를 이용하여 인증하며 자원이 풍부한 외부 에이전트와 홈 에이전트는 공개키를 사용하여 인증한다.

따라서 자원에 제약되어 있는 이동 노드는 계산이 간단한 해쉬 함수를 사용하는 방법으로 인증하는 것이 효율적이며 자원이 풍부한 외부 에이전트나 홈 에이전트는 공개키 암호 시스템을 사용하여 보안을 강화시키는 것이 좋다.

3.2 제안하는 인증 메커니즘

여기서는 기존 인증 메커니즘의 분석에 따라 보다 효율적이고 안전한 인증 메커니즘을 제시하고자 한다. 앞에서 분석한 것과 같이 비밀키 기반 인증 메커니즘에서는 가벼운 비밀키 계산으로 인증의 효율성은 높으나 모든 인증 참여자에 대한 인증이 이루어지지 못하고 생성하는 MAC의 특성상 부인방지 서비스가 부족하다는 단점이 있다. 공개키 기반 인증 메커니즘은 모든 인증 참여자에 대하여 공개키를 기반으로 부인방지 서비스가 제공되는 인증을 수행하나 실제로 적용할 수 없을 만큼 시간이 오래 걸린다. 최소 공개키 기반 인증 메커니즘에

서는 이동 노드와 홈 에이전트 사이에는 비밀키를 기반으로 신뢰성 있는 관계를 유지하며, 외부 에이전트와 홈 에이전트는 공개키를 기반으로 인증한다. 보안을 유지시키면서 동시에 성능을 높이는 효과가 있으나 이동 노드와 홈 에이전트 사이에는 전자서명을 사용하지 않아 부인방지 기능이 없다. 전자상거래와 같이 이동 노드 행동의 책임성이 질을 경우에는 위치 등록에 대한 부인방지 서비스가 있어야 한다. 따라서 인증은 사용자가 네트워크에서 사용한 자원과 행동에 대하여 부인을 못하도록 하며 동시에 사용자의 편의와 원활한 네트워크 이용을 위해 등록 과정이 짧아야 한다.

제안된 방법은 공개키 기반 인증 메커니즘과 최소 공개키 기반 인증 메커니즘의 혼합 형태이다. 이동 노드가 등록 요청에 전자서명을 추가하는 것 외에는 최소 공개키 기반 인증 메커니즘과 동일하게 작동한다.

외부 에이전트가 보낸 에이전트 광고를 이동 노드는 홈 에이전트에게 그대로 전달시키고 홈 에이전트가 인증한 내용은 결과를 통해 간접적으로 인증한다. 이동 노드는 홈 에이전트에게 전자서명을 보내고 홈 에이전트는 인증 기관에 접근하여 공개키의 진실 여부를 확인한 후 전자서명을 증명한다. 이로써 홈 에이전트는 이동 노드와 외부 에이전트 모두를 인증할 수 있다. 여기서 이동 노드의 전자서명은 자신이 등록한 위치정보에 대한 중요한 부인방지 기능을 제공하여 네트워크 자원 사용을 관리제어할 수 있다. 홈 에이전트의 경우에는 외부 에이전트에게 전자서명을 보내 인증 받고 이동 노드에게는 MAC을 생성시킴으로써 직접 인증 받는다. 이로서 새로운 위치 등록과정에 관계하는 모든 참여자에 대한 인증을 할 수 있다. 아래 표시된 메시지 부분만 제외하고 최소 공개키 기반 인증 메커니즘과 동일하다.

● **Registration**

MN → FA : M_2, $<<M_2>>K^{-1}_{MN}$, $Cert_{MN}$
where M_2=Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}, [messge in agent advertisement]

HA
- validate $Cert_{MN}$ using K_{CA}
- verify $<<M_2>>K^{-1}_{MN}$ using K_{MN}
- check whether FA_{id} in M1 and FA_{id} in M_2 is identical
- validate $Cert_{FA}$ based on existing *PKI* at *HA*
- validate $<<M_1>>K^{-1}_{FA}$ using authenticated K_{FA}

이동 노드는 자신의 개인키를 사용해서 전자서명을 생성하고 그 전자서명을 등록 요청에 포함시킨다. 이동 노드는 원문에 전자서명과 인증서를 포함시키지만 미리 인증서를 발급해 놓기 때문에 서명시마다 인증 기관에 접근할 필요가 없다. 홈 에이전트는 전자서명을 받아 증명하고 이동 노드의 서비스 요청에 대한 증거로 보존한다. 등록 요청은 전자서명을 이용하지만, 등록 대답은 MAC에 의존하기 때문에 이동 노드가 등록 대답을 받았을 때에도 미리 나눠 가진 비밀키로 인증함으로써 인증시 인증 기관에 접근할 필요가 없다. 이런 구조는 특히 이동 노드의 공개키 사용을 최소로 한다.

제안된 방법이 공개키 기반 인증 메커니즘에 비하여 가지는 장점은 첫째, 홈 에이전트가 보내는 등록 대답은 비밀키를 사용한 MAC을 포함시켜 이동 노드의 성능 저하를 줄였다는 것이다. 이동 노드와 같이 계산을 최소로 줄여야 하는 환경에서 해쉬 함수가 주는 이점은 크다.

둘째, 이동 노드는 에이전트 광고를 받은 때 외부 에이전트를 증명할 필요가 없고 등록 과정 중 외부 에이전트와 직접 상호 인증을 할 필요도 없다. 홈 에이전트가 등록 요청을 받아 외부 에이전트를 인증하고 인증이 성공이라면 등록 대답을 이동 노드에게 보낸다. 이동 노드는 등록 대답을 받음으로써 외부 에이전트에 대한 내용을 간접적으로 인증한다.

셋째, 이동 노드는 한번의 공개키 동작을 수행하여 전자서명을 생성해낸다. 자신의 개인키로 전자서명을 만들고 보내므로 인증 기관의 CRL에 접근할 필요가 없다. 일반적으로 전력을 아껴서 사용해야 하는 이동 노드에게 계산을 줄여준다. 또한 홈 에이전트로부터 등록 대답을 받아도 미리 받은 비밀키로 인증하기 때문에 인증 기관에 접근할 필요도 없고 계산 비용이 매우 적다.

이렇게 새로 제시된 전자서명을 이용한 최소 공개키 인증 방안은 이동 노드가 위치를 바꾸었을 때, 이후에 이루어질 데이타 통신 경로를 열기 위한 새 위치 등록 단계에 해당된다. 따라서 새 통신 경로를 만드는데 있어서 인증 과정에 관계하는 모든 참여자를 인증한다는 면에서 악의를 가진 사용자의 공격을 방지할 수 있으며, 동시에 비밀키공개키에서 사용되는 MD5와 RSA와 같은 인증 알고리즘을 통하여 인증의 무결성을 보장할 수 있다. 특히 RSA는 이동 사용자만이 비밀키를 보유한다는 점에서 새 위치 등록과정 행위를 부인을 할 수 없게 한다. 이 방법은 보안을 중요시하는 네트워크에서 새로운 네트워크 경로 설정할 때 네트워크 자원 사용에 대한 부인방지 기능을 부여하는 것으로, 이것은 어플리케

이션에서 전자서명을 이용한 문서, 데이타에 대한 부인방지 기능과는 다르다. 이로써 인증 참여자 모두에게 인증을 수행하면서도 공개키를 최소로 사용하여 성능을 높였으며 부인방지 서비스를 이동 노드에게도 포함시킴으로써 보안이 높은 시스템을 가진 네트워크에서 사용될 수 있는 이동 프로토콜로 제안될 수 있다. 그 외에도 등록되어 있던 이동 노드가 오프라인이 되었다가 다시 같은 외부 에이전트에게 재등록 하려고 한다면 최적화하여 구현할 수 있다. 이동 노드가 할 일이 없는 동안 먼저 전자서명을 만들어 놓았다가 재등록시 즉시 사용함으로써 전체 인증시간의 단축을 더 가져올 수 있다. 기존의 세가지 인증 메커니즘과 제안된 인증 메커니즘을 비교하면 표 1과 같다.

표 1 인증 메커니즘의 비교

	SK	PK	MinPK	minPKds
인증방식	MAC	MAC	MAC, 전자서명	MAC, 전자서명
알고리즘	MD5	RSA	MD5, RSA	MD5, RSA
키 종류와 키 길이	비밀키	공개키 (512bits)	비밀키, 공개키 (512bits)	비밀키, 공개키 (512bits)
인증 코드길이	16bytes	64 bytes	16bytes, 64bytes	16bytes, 64bytes
MAC 사용	HN, HA	·	MN, HA	HA
전자서명사용	·	MN, FA, HA	FA, HA	MN, FA, HA

(SK : 비밀키 기반 인증 메커니즘, PK : 공개키 기반 인증 메커니즘 , minPK : 최소 공개키 기반 인증 메커니즘, minPKds : 제안하는 전자서명을 첨부한 공개키 기반 인증 메커니즘)

4. Mobile-IP 인증 모델링 및 성능 평가

4.1 모델링 도구 : SDL

통신 시스템 개발용 명세 언어인 SDL(Specification and Description Language)은 시스템을 명세화하고 기술하는 표준화된 언어이다. 현재 ITU-T로 명칭이 바뀐 CCITT에 의해 개발되었으며 ITU-T Recommendation Z.100으로 표준화되었다. 전기통신 분야에서 분석 및 개발에 많이 쓰이며, 통신 시스템들이 복잡해짐에 따라 시스템의 동작(Behavior)을 명시하는데 사용된다. SDL은 시스템을 계층적으로 표현하기 위해 제안되어 동시 작업과 상호 동작이 중요시되는 사건 중심의 실시간 시스템을 기술하는데 적합하다. 이에 따라 통신 시스템의 동작을 기술해 주는 사용자와 개발자들의 공통언어로 사용되고 실시간 시스템의 구조, 동작 기능 및 데이타를 표시할 수 있는 장점을 보유하며 시스템 분석과 설계에 적용이 가능하다.

4.2 시뮬레이션 환경

4.2.1 망구성

물리적으로 망은 무선랜으로 IEEE 802.11를 따르고 시뮬레이션 구성은 그림 2와 같다[5].

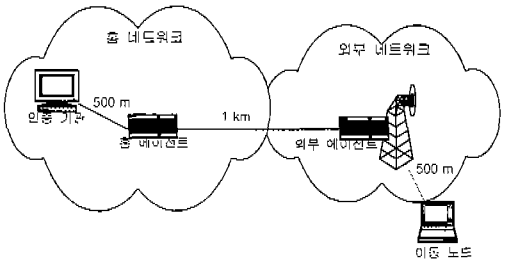


그림 2 망구성

이동 노드는 홈 네트워크에서 시작하여 홈 에이전트로부터 고정 IP를 부여받고 외부 네트워크로 이동하여 외부 에이전트에게서 에이전트 광고를 통해 새로운 COA를 받아 홈 에이전트에게 등록시킨다. Mobile-IP는 매크로 셀에서 작동하기에 알맞으므로 서브넷은 반경 500m로 하며 외부로 이동함에 따라 홈 네트워크와 외부 네트워크 사이의 거리는 1km에서 40km까지 벌어진다. 새로운 서브넷에 들어가 IP가 바뀔 때마다 홈 에이전트에 새 위치 정보를 등록하고 데이타그램을 터널링 받는다. 시뮬레이션에 사용된 고정 파라미터는 표 2와 같다.

표 2 시뮬레이션 고정 파라미터 값

거리	이동 노드 ~ 기지국 (무선 링크의 거리)	500m
	외부 에이전트 ~ 홈 에이전트 (유선 링크의 거리)	1km
	외부 에이전트 ~ CA (유선 링크의 거리)	1.5km
	홈 에이전트 ~ CA (유선링크의 거리)	500m
지연시간	무선 링크의 지연	7ms/km
	유선 링크의 지연	5ms/km
대역폭	무선 링크 대역폭	2Mbps
	유선 링크 대역폭	10Mbps

4.2.2 인증 메커니즘의 작동

인증 동작은 먼저 UDP 계층에서 UDP checksum 필드를 계산한 뒤 재공격을 방지하기 위해 삽입된 식별자(Identification)를 검사한다. 임의의 수인 넌스를 삽입하거나 등록 메시지가 사용될 수 있는 lifetime을 명시한 타임스탬프를 삽입할 수 있는데 여기서는 넌스를 포함시키며 상대방의 답변을 받으면 자신이 전 단계에서 삽입시킨 넌스가 제대로 들어있는지 검사한다.

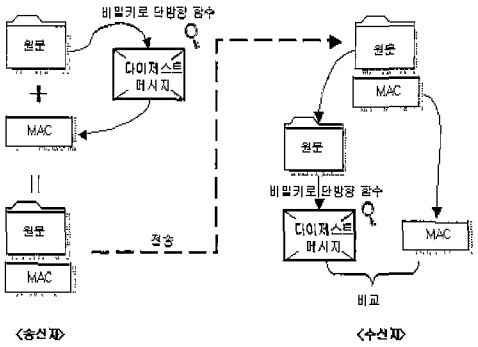


그림 3 MAC 동작

마지막으로 인증 코드가 삽입된 경우에는 MAC을 증명하고 전자서명이 첨부된 경우에는 인증서를 확인하고 전자서명을 증빙한다. 그림 3은 MAC을 검사하는 동작을 보여준다. 이 때 사용하는 해쉬 함수는 어떤 종류도 사용할 수 있으며, 본 시뮬레이션에서는 RFC 2002에서 기본으로 하는 MD5를 사용한다. 등록 대답에 대하여 prefix-suffix 모드로 128 bits의 다이제스트 메시지를 생성한다. 방법은 먼저 공유한 비밀키에 대하여 해쉬 함수를 수행하고 보호하고자 하는 원문 메시지에 대하여 다시 해쉬 함수를 수행하고 다시 한번 비밀키에 대하여 해쉬 함수를 수행한다. 이 때 보호하고자 하는 원문 메시지는 다음과 같다.

- UDP payload (등록 요청이나 등록 대답 데이타)
- 모든 전에 위치하는 extension

  해당 extension의 type과 length 필드[6]

MD5는 RFC1321에 제시된 소스 코드를 따르며, 본 시뮬레이션에서는 앞에서 설명된 해쉬 함수 MD5를 사용한다. 이 때 입력 값은 512 bits이고 결과로 나오는 해쉬 값은 16 bytes이다.

전자서명을 인증하는 경우에는 그림 4와 같이 공개키를 사용한 부가형 전자서명(Digital signature with appendix)을 이용한다. 보호하는 원문 메시지는 해쉬 함수와 동일하다. 부가형 전자서명은 원문 이외에 서명을 따로 전송해야 하므로 전송량이 조금 늘어나는 반면, 메시지가 아무리 길더라도 단 한번의 서명 생성 과정만이 필요하므로 효율적이다. 임의의 길이의 메시지를 일정한 길이로 압축해 주는 해쉬 알고리즘은 입력 메시지가 조금만 변하더라도 그 해쉬 결과로 전혀 다른 값을 출력하여 서명의 위조나 서명된 메시지의 변조를 막을 수 있다[8].

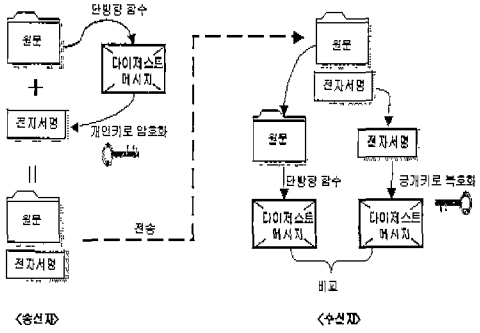


그림 4 전자서명의 작동

여기서는 전자서명을 인증하기 위하여 공개키가 필요한데, 송신자는 자신의 공개키가 삽입된 인증서를 인증기관으로부터 먼저 발급받아 원문에 전자서명과 함께 첨부시키면 수신자는 받은 인증서를 확인한 후 유효한 경우 수신 받은 공개키가 올바르다고 확신하고 전자서명을 검증하는데 사용한다. 인증 기관을 통한 전자서명의 인증절차 과정은 그림 5와 같다[8][9].

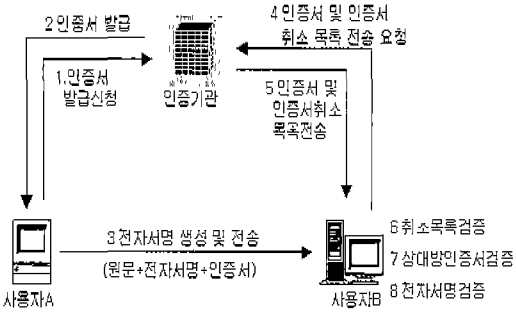


그림 5 인증기관을 통한 전자서명 인증절차

Draft에 따라 여기서 공개키 기반 전자서명은 X.509를 기반으로 하며 표준으로 특정한 알고리즘을 명시하지는 않지만 RSA를 권고한다. 그 외에도 RSA가 가진

단점으로 지적되는 속도를 대폭 향상시킨 타원곡선 암호 알고리즘과 DSA(Digital Signature Algorithm)를 제시하여 키 길이와 전자서명 길이를 명시하고 있다[10]. 타원곡선 암호 시스템은 수학적인 복잡도 때문에 동일한 키 크기의 정수 위에서 구현하는 것보다 훨씬 강도가 세다. 본 시뮬레이션에서는 RSA Laboratory의 RSA 암호 시스템을 시뮬레이션한다[11]. RSA에서 사용한 키길이는 512 bits이고 결과로 나오는 전자서명은 64 bytes이다.

4.3 시뮬레이션 결과 분석

본 절에서는 시뮬레이션 결과를 분석한다. 모델링은 이동 노드가 새로운 서브넷으로 들어가 에이전트 광고와 같은 특별한 메시지를 받았을 때 새 이동 정보를 홈 에이전트에게 등록하는 과정에 해당한다[12]. 시뮬레이션은 기존의 등록을 위한 3가지 인증 메커니즘과 제안된 인증 메커니즘으로 나누어 수행된다. 본 모델링은 Ultrasparc SUN OS 5.6 버전의 운영체제를 사용하고, CPU가 167 MHz, RAM이 132M인 워크스테이션에서 실행되었다.

4.3.1 암복호화 횟수 및 인증 평균시간

인증 메커니즘에서 암복호화가 차지하는 비중이 크기 때문에 각 수행 횟수와 인증 평균시간을 계산하여 인증 메커니즘에서 차지하는 영향을 분석할 수 있다.

표 3 암복호화 횟수

		해쉬 함수		공개키 전자서명	
		암호화	복호화	암호화	복호화
SK	전체	2	2		
	이동 노드	1	1		
PK	전체			10	11
	이동 노드			1	4
MinPK	전체	2	2	4	4
	이동 노드	1	1		
MinPKds	전체	1	1	6	5
	이동 노드		1	1	

표 3을 통해 먼저 각 인증 메커니즘에서 요구되는 암복호화 횟수를 계산하였다. 이 때 시뮬레이션 결과를 수치로 계산하기 위하여 사용된 수식은 다음과 같다. 전체 등록 시간(T)은 등록 요청, 등록 대답을 만드는 시간과 각 에이전트가 자신이 가진 테이블을 갱신하는 시간을 포함한 노드 프로세싱 시간(Operation), 노드와 에이전트 사이에 메시지가 전달되는데 걸리는 전달지연시간(Delay), MAC이나 전자서명을 만드는데 필요한 암호화 복호화 시간(EncrypDescrypTime)을 합친 시간이다.

$$T = Operation + Delay + EncrypDecrypTime \quad (1)$$

$$Delay = PropDelay + TransDelay \quad (1\text{-}1)$$

$$EncrypDecrypTime = EncrypTime + DecrypTime \quad (1\text{-}2)$$

$$EncrypTime = SecretEncryp + PublicEncryp \quad (1\text{-}3)$$

$$DecrypTime = SecretDecryp + PublicDecryp \quad (1\text{-}4)$$

전달지연시간(Delay)은 인증 참여 노드사이의 거리와 미디어에 따른 Propagation Delay와 Transmission Delay를 합친 것이고, 암호화복호화에 사용되는 시간(EncrypDecrypTime)은 각각 암호화 시간(EncrypTime)과 복호화 시간(DecrypTime)으로 나뉜다. 암호화 시간은 다시 비밀키 기반 암호화 시간(SecretEncryp)과 공개키 기반 암호화 시간(PublicEncryp)으로 나누어진다. 비밀키로는 MD5가 사용되었고 공개키로는 RSA가 사용되었다. 마찬가지로 복호화 시간도 비밀키 기반 복호화 시간(SecretDecryp)과 공개키 기반 복호화 시간(PublicDecryp)으로 나누어져 계산된다.

SK에서는 해쉬 함수 계산이 4번인데 비하여 PK에서는 공개키 계산 횟수가 21번으로 5배 이상 증가하였다. 공개키 계산 자체가 일반적으로 100~1,000배 정도 오래 걸린다는 것을 고려할 때 PK는 SK에 비하여 상당한 시간과 계산 비용을 요구함을 알 수 있다. minPK에서처럼 공개키 계산을 최소로 할 경우 비싼 공개키 계산이 반 이하로 줄며 특히 이동 노드에서는 비밀키 계산만 수행하도록 하였다. 제안된 minPKds에서는 부인방지 서비스를 위해 전자서명을 추가시킴으로써 공개키 계산이 조금 증가하였으나 이동 노드에서의 공개키 계산 횟수 증가는 1번으로 최소로 하였다.

표 4 인증 코드의 평균 시간

(단위 : ms)

	MAC		전자서명	
	생성	증명	생성	증명
평균 시간	0.21	017	80.38	10.08

표 4는 인증 코드를 생성하고 검증하는데 필요한 평균 시간을 보여준다. MAC을 생성하기 위하여 평균 0.208 ms가 걸리고 증명하기 위하여 0.167 ms가 걸리는데 실제로 MAC을 만들고 증명하는 메커니즘이 동일하므로 차이가 거의 없다. 전자서명에서는 전자서명을 생성하는데 80.38 ms이 걸려 증명하는데 걸린 10.08 ms보다 오래 걸린다. 전자서명은 MAC을 만드는 과정

에 비해 48~473배 걸리는데 해쉬 함수에 비하여 공개키 함수 자체가 복잡한 구조를 가졌기 때문이다. 공개키 계산은 더 계산 비용이 많이 들어 자원을 많이 필요로 하고 전력을 소모시킨다. 또한 암복호화 시간이 오래 걸리고 자신의 공개키를 발급하여 키관리소에 맡기고 상대방의 공개키를 배급받아 복호화에 사용하는 과정을 생각하면 단순한 비밀키 계산에 비하여 계산 비용이 상당히 높은 이유를 알 수 있다. 인증 평균 시간을 통하여 보안을 보장하는 범위 내에서 공개키 사용을 최소로 줄여야 함을 확인시켜준다.

4.3.2 전체 등록시간과 이동 노드에서의 등록시간

전체 등록 시간은 이동 노드가 자신이 속해 있던 네트워크를 떠나 새로운 네트워크에 들어갔을 경우 외부 에이전트를 통해 홈 에이전트에게 새로운 위치 정보를 등록시키는 실제 네트워크 계층에서 걸리는 시간이다. 전체 등록 시간은 등록 요청, 등록 대답을 만드는 시간과 각 에이전트가 자신이 가진 테이블을 갱신하는 시간을 포함한 노드 프로세싱 시간, MAC이나 전자서명을 만드는데 필요한 암복호화 시간, 노드와 에이전트 사이에 메시지가 전달되는데 걸리는 전달 지연시간 3가지로 구성된다.

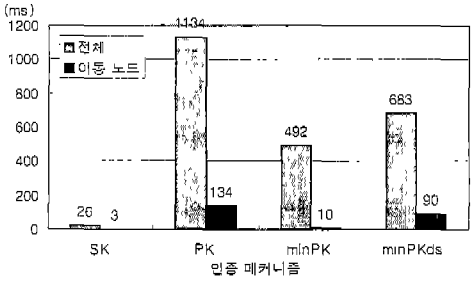


그림 6 전체 등록 시간

그림 6은 인증 메커니즘별 전체 인증시간과 이동 노드에서의 인증시간을 보여준다. 전체 등록 시간은 SK일 경우에 비하여 PK의 경우 37배가 되어 1,134 ms가 걸린다. 이 시간은 새로운 등록과정이 네트워크 계층에서 이루어진 후 핸드오프 서비스나 TCP/UDP 계층에서의 서비스가 이어질 경우 상당히 긴 시간이다. 공개키는 보안을 높여준다는 사실에도 불구하고 사용이 어렵다는 것을 알 수 있다. 보안을 그대로 유지하면서 공개키 사용을 최소로 줄이는 minPK는 PK에 비하여 전체 등록 시간이 43%밖에 걸리지 않는다. 이 방안은 공개키 암복호화 과정이 반으로 줄어든 것으로 그 외에도 이동 노드, 외부 에이전트, 홈 에이전트가 인증 기관에게서 인증서를 발급 받고 공개키를 구하는 횟수가 많고 노드들 사이에 데이타그램을 많이 주고 받아 전달 지연시간이 길어졌기 때문이다. 그러나 여기에는 부인방지 서비스가 결여되어 있기에 제시된 minPKds의 경우에는 이동 노드가 전자서명을 하도록 하였다. minPKds는 PK에 비하여 등록시간을 60%로 줄여 성능을 향상시켰고 부인방지 서비스를 위한 전자서명을 추가시키면서minPK에 비하여는 139% 증가 폭을 보였다. 필요한 서비스를 제공하면서도 효율성을 최대한 떨어뜨리지 않는 동시에 부인방지 서비스를 제공한다.

이동 노드에서의 등록 시간은 전체 등록시간 중에서 이동 노드에서 수행된 시간만을 계산한 것이다. SK의 경우 3 ms로 수행 시간이 무척 적은데 반하여 PK는 44.7배가 넘는 134 ms가 이동 노드에서만 걸렸다. PK에서 이루어지는 공개키 기반 암복호화가 매우 오래 걸린다는 점에서 수행 시간이 길 수 밖에 없다. 또한 SK에서는 이동 노드와 홈에이전트 사이에서만 있던 상호 인증이 PK에 오면 이동 노드, 홈 에이전트, 외부 에이전트 사이에 서로 이루어지기에 인증 횟수가 늘어났으며 공개키를 사용하기 위하여 인증 기관에 접근하는 시간과 여기서 인증서를 발급 받는 시간이 추가로 걸린다. PK는 이동 노드에게는 너무 많은 비용을 요구하며 인증 시간 자체가 길다. 이에 반하여 계산 비용이 높은 공개키를 최소로 사용하고자 하는 minPK는 꼭 필요한 부분에만 공개키를 사용하고 나머지를 비밀키로 바꾸는 방식을 이용하였다. 특히 이동 노드에서는 비밀키만을 사용하여 암복호화를 수행한 결과 SK와 비슷한 10 ms의 시간이 걸렸다. 새로 제시된 minPKds의 경우에는 이동 노드가 자신의 개인키로 암호화한 전자서명을 추가시켜 등록 요청을 보내고 홈 에이전트는 이동 노드의 공용키로 복호화 해 이동 노드가 보낸 메시지임을 확인할 수 있다. minPKds는 이런 개선된 부인방지 서비스에도 불구하고 이동 노드에서의 등록시간이 90 ms로 적게 유지된다. 이 시간은 PK에 비하여 67%로 줄어든 것으로 이동 노드가 외부 에이전트에게 에이전트 광고를 받았을 때 수행하여야 할 인증 과정을 홈 에이전트가 대신 수행하기 때문이며, 또한 홈 에이전트에 대한 인증에서는 전자서명 대신 비용이 적은 MAC을 이용하여 인증을 했기 때문이다. minPK에 비해서는 8.8배의 시간이 걸리는데 전자서명을 하기 위하여 이동 노드가 개인키를 이용하여 전자서명에 서명하는 시간이 증가하였기 때문이다. 또한 홈 에이전트로부터 받은 등록 대답에서는 비밀키를 이용한 MAC 인증을 했기 때문에 홈

에이전트에 대하여 인증기관으로부터 공개키를 받아 인증서를 증명하는 시간이 걸리지 않는다.

4.3.3 전체 등록시간, 노드프로세스시간 그리고 암호화시간

전체 등록과정에 있어서 노드와 에이전트, 인증기관 사이에 메시지를 주고 받는 전달 지연시간을 제외한 시간은 순 노드 프로세스 시간이 되며, 여기서 등록 요청, 등록 대답을 생성하는 시간, 이동 노드나 에이전트가 가진 정보테이블을 갱신하는 시간, 넌스나 타임스탬프를 검사하는 시간, 아이디를 검사하는 시간을 제외한 시간은 암복호화에 들어가는 주요 계산 시간이다. 계산 비용이 높은 암복호화 과정은 노드의 자원을 대부분 사용하게 되며 이동 노드의 전력 소모를 가속화 시킨다. 키를 사용하여 암복호화 하는 시간은 계산 비용이 높은 작업으로 직접적으로 성능을 좌우하며 많은 작동은 전력 소모를 일으킨다

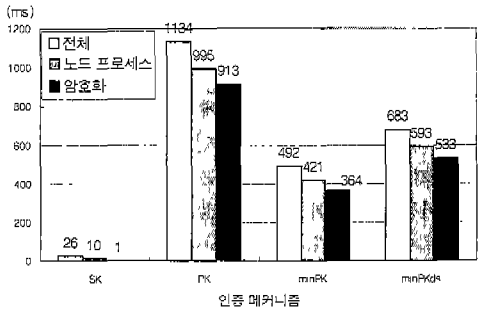


그림 7 전체등록시간, 노드 프로세스 시간, 암호화시간

그림 7은 인증 메커니즘별 전체 인증 시간, 노드 프로세스 시간, 암호화 시간을 보여준다. SK에서는 대부분의 등록시간은 노드와 에이전트 사이의 전달 지연시간으로 기인한다. 비밀키를 이용한 암복호화 시간은 매우 적다. 그러나 PK에 오면 공개키를 이용한 암복호화를 하는 시간이 SK에 비하여 1118배나 늘어나서 공개키 과정의 비용이 높다는 것을 다시 한번 확인할 수 있다. 공개키의 과정이 복잡하다는 것 뿐 아니라 PK에서는 암복호화 과정이 여러 번 일어난다. 공개키 이용이 늘어날수록 전체 등록시간에서 차지하는 암복호화 과정이 차지하는 비중이 증가한다. 전체 등록시간에서 암복호화 시간이 차지하는 부분은 공개키 계산 과정이 많은 경우일수록 높다. PK에서 암복호화 시간이 높은 것은 노드와 에이전트사이에 인증과정에서 공개키를 이용하여 인증을 하고, 공개키 사용을 보장하기 위하여 인증기관에서 인증서를 발급할 때 공개키 계산을 하기 때문이다. 결국 전체 등록시간을 증가시키는 중요 요인으로는 공개키 사용으로 인한 계산 비용의 증가와 공개키 사용에 따른 인증서 발급으로 추가 인증 기관의 공개키 사용이 있으며 전달 받는 메시지 수의 증가로 인한 긴 지연시간에 기인한다.

4.3.4 이동 노드의 위치 변화에 따른 전체 등록시간

Mobile-IP는 매크로 이동성을 지원하는데 적합한데 만약 매우 작은 지역만 처리할 수 있는 무선 트랜스리시버 사이를 움직이는 것과 같은 마이크로 이동성을 가지는 경우에 사용되기에는 오버헤드가 너무 크다. 따라서 Mobile-IP가 매크로 이동성을 기반으로 한다는 것을 가정으로 할 때 이동 노드의 위치 변화에 따른 인증 시간을 계산한다[13].

그림 8은 이동 노드가 홈 네트워크로부터 1 km에서 40 km까지 멀어져 갈 경우 인증을 위하여 필요한 시간을 보여준다.

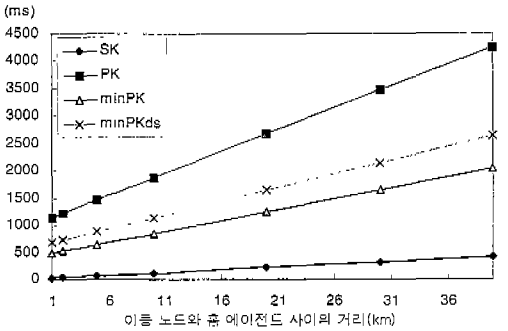


그림 8 이동 노드의 위치 변화에 따른 등록 시간

이동 노드와 홈 에이전트 사이의 거리가 1 km에서 40 km까지 멀어질 때 SK의 등록 시간은 13배나 증가하였으나 실제 시간은 420 ms밖에 걸리지 않는다. 이에 반하여 PK의 경우 4 배로 증가율은 낮았으나 전체 인증시간이 4초가 넘는다. 이에 반하여 minPK에서는 PK의 반도 걸리지 않으며 제안된 minPKds도 비슷한 선을 유지한다. minPKds는 이동 노드가 홈 네트워크로부터 멀어짐에 따라 더 사용하기에 적합함을 알 수 있다.

4.3.5 서브넷 크기와 이동 속도에 따른 실제 적용 가능성

여기서는 앞에서 비교된 네 가지의 인증 메커니즘이 서브넷의 크기와 이동 노드가 이동하는 속도에 따라서 실제 어떤 메커니즘을 알맞게 사용할 수 있는가를 알아보고자 한다.

그림 9는 서브넷의 크기가 0.1 km에서 1 km 사이일 경우 이동 노드가 이동하는 속도에 따라 그 서브넷에서

머무는 시간을 나타낸다. 서브넷의 크기는 마이크로 셀일 때 0.1 km 에서부터 매크로 셀일 때 1 km이상으로 변한다. 이동하는 사용자의 속도는 걸어다닐 때 1~2 km/h를 가정하며 자동차를 타고 움직이는 100 km/h까지 고려한다. 이런 다양한 시뮬레이션 환경을 기반으로 각각 인증 메커니즘의 등록 시간이 전체 서브넷에서 머무는 시간에서 차지하는 비율을 알아보았다.

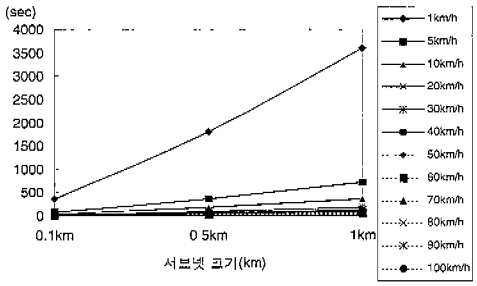


그림 9 이동 속도에 따른 서브넷 머무는 시간

그림 10과 같이 서브넷의 크기가 0.1 km일 경우에는 전체 서브넷에 머무는 시간에 대하여 인증이 차지하는 비율이 크다. 특히 이동 속도가 빨라짐에 따라 그 비율은 급격하게 증가한다. 실제로 Mobile-IP에서 새로운 서브넷에 들어가면 새 위치 정보에 대하여 인증을 받고 데이타그램을 터널링해서 받는데 시간이 오래 걸리므로 인증이 차지하는 비율이 적어야 한다. 그렇지 않을 경우 인증을 받고 터널링 되어 오고 있는 데이타그램을 받기도 전에 또 다른 새로운 서브넷으로 이동하게 되어 인증과 터널링에 드는 오버헤드만 지나치게 높아지고 실제로 데이타그램을 전송 받는 시간이 짧아진다. 이 경우에는 인증 시간이 짧은 것이 중요하므로 성능 저하가 가장 적은 SK를 사용하는 것이 바람직하다.

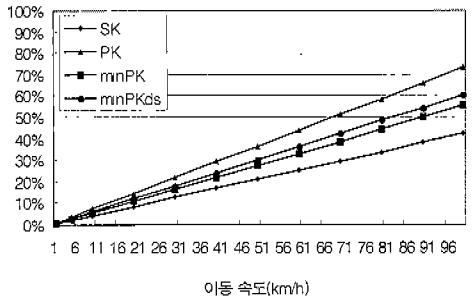


그림 10 서브넷 크기 0.1 km일 때 인증 차지율

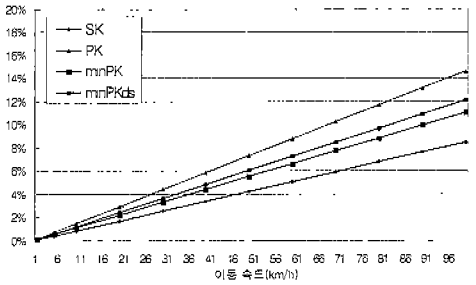


그림 11 서브넷 크기 0.5 km일 때 인증 차지율

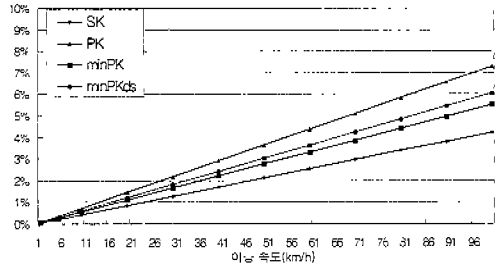


그림 12 서브넷 크기 1km일 때 인증 차지율

그림 11과 같이 서브넷의 크기가 0.5 km일 경우 20~30 km/h일 때에는 PK도 사용할 수 있으나 그 이상의 속도로 움직일 경우에는minPKds를 사용하여 원하는 서비스를 제공받으면서 성능 저하를 줄이는 방법이 좋다. 그러나 그림 12와 같이 서브넷의 크기가 1 km일 경우에는 이동 속도가 100 km/h까지 빨라져도 서브넷에 머무는 시간에 대한 인증 차지 비율이 8% 미만으로 유지된다. 실제로 50 km/h로 이동할 때까지는 PK를 사용해도 좋다.

이와 같이 서브넷과 이동 노드의 상황에 따라서 인증 메커니즘을 보안과 성능에 따라서 바람직한 인증 메커니즘을 골라 사용할 수 있다. Mobile-IP에서는 등록시 인증을 위하여 사용한 메커니즘을 선택할 수 있으므로 등록에 참여하는 노드 사이에 먼저 사용할 인증 메커니즘을 협상하면 된다[14].

5. 결론 및 향후 과제

본 논문에서는 Mobile-IP망에서 제공하는 인증 메커니즘 중 기존에 제안되어 있는 방식에 대하여 비교분석하였고, 보안이 중요한 네트워크에서 필요로 하는 전자서명을 첨가한 최소 공개키 인증 메커니즘을 제시하였다.

시뮬레이션은 네 가지 종류의 메커니즘으로 나누어 구현되었다. 첫번째는 비밀키 기반 인증 메커니즘으로

적은 계산 비용으로 이동 노드에게 적합하고 전체 인증 시간이 짧다는 면에서 효율적이다. 그러나 비밀키의 사용으로 많은 사용자에게 서비스를 제공하기에는 확장성이 떨어지고 외부 에이전트의 보안이 제공되지 않는다는 단점이 있다. 두 번째는 공개키 기반 인증 메커니즘으로 인증 기관을 통한 공개키 사용으로 사용자가 많은 인터넷에서 확장성을 제공하나 이동 사용자가 계산하기에는 부담스러운 공개키 사용으로 현실적으로 구현되기에는 부적합하다. 세 번째는 계산이 복잡한 공개키를 최소로 사용하는 최소 공개키 기반 인증 메커니즘으로 보안을 유지하면서 높은 성능 향상을 보여주었다. 다만 이 방법은 이동 노드가 부인방지 서비스를 제공하지 않기 때문에 보안이 중요한 시스템이 있는 네트워크에 들어가 새로운 위치를 등록시키기에는 그 위치 등록 인증 기능이 부족하다는 단점이 있다.

따라서 본 논문에서는 이동 노드가 전자서명을 함으로써 위치 등록에 대한 부인방지 서비스를 제공하였고 최소로 공개키를 사용함으로써 효율성을 유지하였다. 시뮬레이션 결과를 통해서 본 논문에서 제안한 인증 메커니즘이 안전하고 효율적으로 작동하는 사실을 확인할 수 있었다. 제안한 인증 메커니즘은 보안을 유지하면서도 공개키 사용을 최소로 사용하여 등록 중 필요한 인증 과정을 수행할 수 있었고, 특히 이동 노드에 전자서명을 첨가함으로써 보안이 중요한 시스템에서 위치 등록에 사용될 수 있는 방안으로 기능을 향상시켰다. 또한 이동 노드에서 수행된 계산 시간을 감소시켜 이동 노드의 전력 소모를 줄였고 이동 노드가 가진 자원 제약의 문제를 해결하였다. 이런 방법으로 제안된 인증 메커니즘은 Mobile-IP가 가진 이동성이란 특성에 적합하도록 구성되었으며 이동 노드에서 위치 등록에 대한 부인방지 서비스를 제공함으로써 보안이 중요한 시스템에서 필요한 서비스를 충분히 제공함을 확인했다.

향후 연구 과제로는 많은 사용자가 Mobile-IP를 이동하는 환경에서 성능을 향상시키기 위한 다양한 구현 방법이 연구되어야 할 것이다. 많은 사용자가 인증 기관에 동시에 접근하는 경우에 인증 기관의 성능에 따라서 인증서를 발급받고 확인하는 시간이 달라질 것이다. 그 외에도 이동 노드에서 계산을 최소로 줄이기 위해서는 이동 장치에서 많이 사용되고 있는 불균형 공개키 기반 알고리즘을 적용해보아 성능 향상이 가능한지 연구되어져야 할 것이다[15]. 더 나아가 전체 인증 시간, 핸드오버, 데이타그램의 전송시 보안 부분을 연결하여 연구할 경우 전반적인 Mobile-IP의 구현상 최적화 방향을 찾아볼 수 있을 것이다.

참 고 문 헌

[1] Charles E. Perkins, "Mobile IP," IEEE Communication Magazine, pp. 84-99, May. 1997.

[2] Uyless Black, "Advanced Internet Technologies," Prentice Hall, 1999.

[3] Charles E. Perkins, "Mobile Networking Through Mobile IP," http://church.computer.org/internet/v2n1/ perkins.htm, 1997.

[4] Charles P. Pfleeger, "Security in Computing Second Edition," Prentice Hall, 1997.

[5] William Stallings, "Data and Computer Communications," Fifth Edition, Prentice Hall, 1997.

[6] C. Perkins, "IP Mobility Support," RFC2002, http://www.ietf.org/rfc/rfc2002.txt, 1996.

[7] Mihir Bellare, Phillip Rogaway, "The Exact Security of Digital Signature How to Sign with RSA and Rabin," Proceedings of the Advanceds in Cryptology Eurocrypt 96, pp. 309-416,1996.

[8] ITU Rec. X.509, "The Directory : Authentication Framework, Information Technology Open Systems Interconnection," http://www.itu.int, Nov. 1993.

[9] Radia Perlman, "An Overview of PKI Trust Models," IEEE Network, pp. 38-43, Nov./Dec. 1999.

[10] S Jacobs, "Mobile IP Public Key Based Authentication," http://search.ietf/org/internet-drafts/draft-jacobs-mobileip-pki-auth-01.txt, 1999.

[11] RSA Laboratory, "RSAREF Demonstration Program," http://www.geocities.com/SiliconValley/Network/2811/algo/rsa/rsaref20.zip, 1991.

[12] Vipul Gupta, Abhijit Dixit, "The Design and Development of a Mobility Supporting Network," ISPAN96, 1996.

[13] Maurizio Dell'Abate, Martino De Marco, Vittorio Trecordi, "Performance Evaluation of Mobile IP Protocols in a Wireless Environment," Proceedings of the 1998 IEEE International Conference on Communications, V. 3, pp.1810-1816, 1998.

[14] Sufatrio, Kwok-Yan Lam, "Scalable Authentication Framework for Mobile-IP(SAFe -MIP)," http://search.ietf.org/internet-drafts/draft-rio-mobileip-safe-mip-00.txt, 1999.

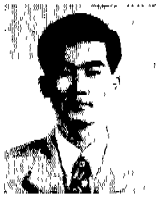
[15] Colin Boyd, Anish Mathuria, "Key Establishmenet Protocols for Secure Mobile Communications : A Selective Survey," Information Security and Privacy(ACISP98), Vol. 1438, pp. 344-355. 1998.

정 선 이

1998년 2월 이화여자대학교 국어국문학과 학사. 2000년 8월 이화여자대학교 대학원 컴퓨터학과 석사. 2000년 7월 ~ 2000년 9월 Tokyo IBM Research Laboratory. 2000년 9월 ~ 현재는 Lucent Technologies 연구원. 관심분야는 이동통신, 보안, Mobile-IP, UMTS, WCDMA, XML.

채 기 준

1982년 연세대학교 수학과 학사. 1984년 미국 Syracuse University 컴퓨터과학과 석사. 1990년 미국 North Carolina State University 컴퓨터공학과 박사. 1990년 ~ 1992년 미국 해군사관학교 컴퓨터학과 조교수. 1992년 ~ 현재 이화여자대학교 컴퓨터학과 교수. 관심분야는 네트워크 보안, 액티브네트워크 보안 및 관리, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능평가.



장 종 수

1984년 경북대학교 공과대학 전자공학과 학사. 1986년 경북대학교 대학원 전자공학과 학사. 2000년 충북대학교 대학원 컴퓨터공학과 박사. 1989년 7월 ~ 현재 한국전자통신연구원 선임연구원 정보보호기술연구본부 네트워크보안구조연구팀 팀장. 관심분야는 Network Security Management, Active Network.

손 승 원

1984년 경북대학교 공과대학 전자공학과 학사. 1994년 연세대학교 대학원 전자공학과 석사. 1999년 충북대학교 대학원 컴퓨터공학과 박사. 1991년 8월 ~ 현재 한국전자통신연구원 책임연구원 정보보호기술연구본부 네트워크보안연구부 부장. 관심분야는 IC Card, Biometry, Active Network.