Mobile-IP 등록 프로토콜에서 공개키를 이용한 인증 방안

학생회원 박상준*, 정회원 홍충선* 이대영*

The Authentication Mechanism Using Public-Key Infrastructure in Mobile IP Registration Protocol

Sang Jun Park* *Student Member*, Choong Seon Hong*, Dae Young Lee* *Regular Members*

요 약

Mobile IP(RFC2002)는 호스트에 이동성을 제공하여주는 대표적인 프로토콜이다. 본 논문에서는 공개키 기반의 인증서와 인증기관을 이용한 Mobile IP 등록 프로토콜을 제안한다. 제안된 프로토콜은 이동 노드의 등록 메시지를 인증하고 재전송 공격을 방지하며 공개키 암호화 사용을 최소로 하였다. 또한, 제안 프로토콜은 인증서를 사용하여 에이전트들과 이동 노드들 사이에 직접적인 인증을 할 수 있도록 설계하였다. 컴퓨터 모의 실험을 통하여 제안 프로토콜은 기존에 연구되어진 공개키를 기반으로 하는 Mobile IP 등록 프로토콜보다 통신 성능이 우수함을 알 수 있다.

ABSTRACT

Mobile IP(RFC2002) is representative protocols that support mobility to host. In this paper, we propose a mobile IP registration protocol using public-key based certificates and CA(certification authority). Our proposed protocol authenticates the registration message of mobile node and prevents replay attack and minimal use of public key cryptography. Also, Our proposed protocol directly authenticates between agents and mobile nodes using certificates. Through the computer simulation, we prove that our proposal has better performance than the previous public-key based Mobile IP registration protocol.

Ⅰ. 서 론

Mobile IP 프로토콜[1,2]은 IETF 워킹그룹에서 제안한 표준으로, 호스트의 이동성을 지원하여주는 프로토콜이다. Mobile IP는 전송 계층의 연결 유지와 IP 계층의 라우팅 문제를 해결하기 위해 2개의 IP 주소를 사용한다. 이 2개의 주소 중 하나인 홈 주소(Home Address)는 고정된 값으로, TCP 연결을 구별하는 등의 목적으로 사용된다. 다른 하나의 주소인 COA(Care-Of-Address)는 새로운 연결 지점마다 값이 바뀌며, 이동 노드(mobile node, MN)의 실제적인 위치를 반영하는 주소로 이용된다. MN는 홈 네트워크(home network)로부터 홈 주소를 부여받는다. 홈 네트워크는 HA(home agent) 노드를 포함하는 네트워크로, 보통 MN가 등록된 사설 네트워크 또는 사업자 네트워크이다. 노드가 이동해 홈 네트워크에 연결되어 있지 않고 다른 네트워크, 즉 외부 네트워크(foreign network)에 연결되어 있을 때, HA는 MN를 목적지로 한 모든 패킷을 받아 MN가 현재 연결된 외부 네트워크로 패킷을 전달한다.

MN는 연결 지점을 바꿀 때마다 새로운 COA를 HA에게 등록한다. HA는 홈 네트워크로 들어온 패킷을 MN에게 전달하기 위해, 패킷을 COA로 전송

* 경희대학교 전자정보학부 (sjpark@digital.kyunghee.ac.kr)
논문번호 : 010343-1116, 접수일자 : 2001년 11월 16일
이 논문은 2001년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2001-003-E00210)

한다. 이때 패킷의 새로운 목적지는 COA로 바뀌게 되는데 흔히 이 작업을 redirection 이라고 한다. 패킷이 COA로 도착되면 원래의 형태대로 목적지가 홈 주소인 패킷으로 바꾸는 작업이 이루어진다. 최종적으로 패킷이 MN에게 전달되면 이 패킷은 마치 고정된 주소로 전달된 패킷과 동일하게 취급되어, TCP 또는 그 이상의 상위 계층에게 전달된다.

Mobile IP에서 HA는 redirection을 위해 MN의 COA를 목적지로 하는 IP 패킷 헤더를 생성한다. 생성된 헤더는 원래의 패킷을 감싸는 새로운 IP 패킷의 헤더로 사용된다. 즉, 원래 패킷의 헤더에 들어있던 목적지 주소인 MN의 홈 주소는 새로운 패킷의 페이로드(payload)에 포함되어, COA까지 라우팅 되는 동안 이 패킷을 처리하는 라우터들에게 아무런 영향을 주지 못하게 된다. 이와 같이 원래의 패킷을 새로운 패킷 속에 감싸 전송하는 것을 터널링(tunneling)이라고 한다.

현재의 Mobile IP 프로토콜에서는 라우트 최적화(route optimization), Ingress 필터링, 이동노드의 이동 관리와 데이터 전송 기법등과 같은 기술적인 문제와 구현상의 문제들이 여전히 남아 있다. 그러나 Mobile IP의 가장 큰 당면 과제는 보안 문제이다. 모든 통신에서 보안 문제는 필수적으로 해결해야 할 부분이다. Mobile IP에서도 전자상거래, 데이터 통신, 전자메일 등 다양한 서비스가 원활하게 제공되기 위해서는 보안 문제가 선결되어야 한다. 특히 인터넷에서 사용 중인 다양한 보안 구조들과 Mobile IP가 공존할 수 있도록 하기 위한 연구가 수행되고 있다[3][4]. 그 예로 방화벽을 이용한 Mobile IP 보안 유지 방법 등이 연구되어 지고 있다[5]. Mobile IP의 보안성을 증대시키기 위해서는 강력한 인증 절차와 데이터의 보호를 위한 암호화 기능이 필요하다. 유선네트워크의 보안문제와는 별개로 Mobile IP에서는 호스트들의 이동성 지원을 위해 무선환경을 사용하게 되므로 무선환경에 적합한 보안 및 인증 프로토콜이 구축되어져야 한다. 그러나, 무선환경 자체의 단점인 낮은 대역폭(low bandwidth), 이동 단말기의 연산 능력(computing power), 그리고 이동 단말기의 짧은 전지 수명 등이 Mobile IP의 보안 문제를 해결하는데 많은 어려움으로 작용하고 있다.

비밀키를 기반으로 하는 현재의 Mobile IP 인증은 확장이 힘들다는 단점이 있다. 이는 인터넷과 같은 방대한 규모의 네트워크에서 효과적으로 키를 관리하지 못하기 때문이다. 또한, 전자상거래와 보안 서비스에서 중요한 부인봉쇄 서비스를 제공할 수 없으며, 메시지 재사용 공격(replay attack)이나 MN에 대한 서비스 거부(denial of service) 공격에 노출되기 쉽다. 이를 보안하기 위한 공개키 기반의 Mobile IP가 연구중이나 무선 환경에서의 공개키 암호화기법 사용에 대한 적합성 여부가 새로운 문제점으로 제시되었다[3].

본 논문에서는 위와 같은 인증과정에서의 문제점을 해결하고자 비밀키과 공개키를 이용한 안전한 Mobile IP 등록 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Mobile IP 및 Mobile IP 등록 프로토콜에 대해 알아본다. 3장에서는 Mobile IP 등록 프로토콜에 관한 관련 연구에 대해 알아보고 기존 프로토콜에서의 문제점을 분석한다. 4장에서 본 논문이 제안한 프로토콜을 설명하고 5장에서 시뮬레이션 결과를 분석한 후, 마지막으로 6장에서 결론 및 향후 연구 방향을 제시한다.

Ⅱ. Mobile IP 등록 프로토콜

2.1 Mobile IP 등록 과정에서의 보안

Mobile IP 등록 프로토콜에서는 메시지 인증 코드(Message Authentication Code, MAC)[6]값을 이용하여 MN와 HA간의 인증과 메시지의 무결성을 검사한다. 이 경우 MN와 HA는 서로 공유하는 비밀키를 갖게된다.

메시지 재사용 공격(replay attack)을 방지하기 위해 Mobile IP에서는 두 가지 방법을 선택하여 사용한다. 하나는 타임 스탬프(time stamp)를 사용할 수 있고, 다른 하나는 랜덤한 숫자인 nonce를 사용할 수 있다[7].

타임 스탬프를 이용한 등록 프로토콜은 MN가 메시지를 전송할 때, 현재 시각을 첨부하여 전송한다. 메시지를 받은 HA는 자신의 시간과 타임 스탬프를 비교하여 그 차이가 일정한 범위 안에 포함되면 타임 스탬프를 정당한 것으로 처리하며, 범위를 벗어날 경우 무효로 처리한다.

Nonce를 이용한 기법은 메시지를 전송할 때마다 랜덤함 수인 nonce를 첨부하는 방법이다. MN은 HA로 메시지를 보낼 때 이전에 HA로부터 받은 nonce(N_{HA})와 함께 새로운 nonce(N_{MN})를 생성하여 보낸다. FA는 이 메시지를 HA로 중계해 주고 HA는 MN이 보낸 N_{HA}와 자신이 예전에 MN으로 보낸 nonce를 비교하여 MN을 인증한다. 또한, HA는

MN이 보낸 N_{MN}를 등록결과 메시지에 포함시켜 MN에게 보내면 MN는 HA에게 받은 N_{MN}와 자신이 예전에 HA에게 보낸 nonce를 비교하여 HA을 인증한다.

2.2 Mobile IP 등록 프로토콜

MN이 새로운 FA로 이동하면 MN은 FA로부터 얻은 자신의 COA를 HA에게 등록하게 된다. MN는 등록 메시지를 FA에게 보내주면, FA는 이 등록 메시지를 HA에게 전달하여 준다. 이러한 등록 과정은 재사용 공격을 방지하기 위하여 타임 스탬프와 nonce를 선택하여 이루어지게 된다.

메시지의 등록과정에서 사용되는 기본 용어는 다음과 같이 정의된다.

- M, N : 메시지 M과 N의 연결
- MN_{HM} : MN의 홈 주소
- MN_{COA} : MN의 care-of-address
- HA_{id} : HA의 IP 주소(HA의 ID)
- FA_{id} : FA의 IP 주소(FA의 ID)
- N_{MN}, N_{HA} : 각각의 MN와 HA의 nonce
- T_{MN}, T_{HA} : 각각의 MN와 HA의 타임 스탬프
- {M}K : 키 K로 암호화한 메시지 M
- <M>K : 키 K에 의한 메시지 M의 MAC 값
- S_{MN-HA}: MN과 HA의 비밀키
- *Request* : 등록 요청을 나타내는 비트 패턴
- *Reply* : 응답을 나타내는 비트 패턴
- *Result* : 등록 요청에 대한 결과값
- *advertisement* : 광고 메시지를 나타내는 비트 패턴

nonce를 이용하는 등록 프로토콜 과정은 다음과 같다.

(0) HA→MN : N_{HA} (전 과정에서 HA에게 받은 nonce)
(1) MN→FA : M_1, $<M_1>$SMN-HA
M_1 = *Request*, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}
(2) FA→HA : M_1, $<M_1>S_{MN-HA}$
(3) HA→FA : M_2, $<M_2>S_{MN-HA}$
M_2 = *Reply*, *Result*, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}
(4) FA→HA : M_2, $<M_2>S_{MN-HA}$

타임 스탬프를 이용하는 등록 프로토콜 과정은 다음과 같다.

(0) HA→MN : T_{HA} (전 과정에서 HA에게 받은 타임 스탬프)
(1) MN→FA : M_1, $<M_1>S_{MN-HA}$
M_1 = *Request*, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, T_{MN}
(2) FA→HA : M_1, $<M_1>S_{MN-HA}$
(3) HA→FA : M_2, $<M_2>S_{MN-HA}$
M2 = *Reply*, *Result*, FA_{id}, HA_{id}, MN_{HM}, T;
if $T=T_{MN}$, T_{MN} is *OK*
if $T\neq T_{MN}$, T_{MN} is *not OK*

Ⅲ. 관련 연구

3.1 Jacobs의 공개키 기반 인증

비밀키를 기반으로 하는 현재의 Mobile IP 인증은 확장이 힘들다는 단점이 있다. 또한, 상거래에서 중요한 부인봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Jacobs는 공개키 기반의 인증방법을 제안하였다[8].

제안에서 Mobile IP 제어 메시지(control message)의 인증을 위하여 MN와 에이전트(홈 네트워크와 외부 네트워크)간에 X.509 디지털 서명(digital certificates), 공개키, 그리고 디지털 서명을 사용하였다. 또한, 모든 제어 메시지에 추가되어야 하는 인증정보를 전달할 새로운 Certificate Extension 메시지 형식을 정의하였다.

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

그러나, 공개키 암호방식을 사용하면서 제안된 프로토콜은 여러 가지 문제점들이 도출되었다. 그중 가장 큰 문제점은 MN에서의 공개키 암호화기법이 무선 환경에 맞지 않는다는 것이다.

이동 단말기의 특성상 MN에서의 연산 능력(computing power)은 제한이 있다. 공개키 기반의 암호화기법을 사용하였을 경우 비밀키 기반의 암호화기법을 사용하였을 때보다 약 1000배의 비용이 증가하므로[9], MN의 성능을 저하시키는 요인이 된다. 그리고, 무선 환경에서의 낮은 대역폭은 MN가 인증기관(Certification Authority, CA)으로부터 인증서 취소 목록(Certificate Revocation List, CRL)를 전송 받을 수 있을 만큼 충분하지 못하다. 따라서 MN는 주기적으로 CRL을 업데이트 할 경우, 네트워크의 성능이 떨어지게 된다. 공개키를 사용함으로

써 발생되는 또 다른 문제점은 MN의 시스템이 복잡해 진다는 것이다. 공개키와 인증서를 생성하기 위해서는 MN에서의 하드웨어나 소프트웨어의 추가가 불가피해진다.

3.2 Sufatrio, K. Lam의 기법

Sufatrio, K. Lam은 Jacobs의 인증 프로토콜에서 공개키 기반 암호화의 사용을 줄이는 연구를 하였다[10].

Mobile IP 등록 프로토콜에서 공개키와 비밀키를 병행하여 사용함으로써 Jacobs의 제안에서 생기는 오버헤드를 줄이는 방법을 제시하였다.

제안된 프로토콜은 아래와 같다.

· Agent Advertisement :

(AA1) FA→MN : M_1, <<M_1>> K_{FA}^{-1}, $Cert_{FA}$

M_1 = *Advertisement*, FA_{id}, MN_{COA}

· Registration :

(R1) MN→FA : M_2, <M_2>S_{MN-HA}

M_2 = *Request*, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}, [message in AA1]

(R2) FA→HA : [message in R1], N_{FA}

(R3) HA : (upon receipt of R2)

- validate <M_2>S_{MN-HA} using S_{MN-HA}
- check whether FA_{id} in AA1 = FA_{id} in M_2
- validate $Cert_{FA}$ based on existing PKI at HA
- validate <<M_1>> K_{FA}^{-1} using authenticated K_{FA}

(R4) HA→FA : M_3, <<M_3>> K_{HA}^{-1}, $Cert_{HA}$

M_3 = M_4, N_{FA}

M_4 = *Reply*, *Result*, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}, <M4>S_{MN-HA}

(R5) FA

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

(R6) HA→MN : M_4

(R8) MN : (upon receipt of R6)

- Validate <M_4>S_{MN-HA} using S_{MN-HA}

제안된 프로토콜에서는 FA가 보내는 광고 메시지에 자신의 인증서와 함께 자신의 개인키로 서명한 메시지를 MN에게 전달한다. 그러나 이 광고 메시지는 무선환경을 통하여 전달되기 때문에, FA가 이 메시지를 받을 경우 많은 오버헤드가 발생되게 된다. 또한, FA가 직접 MN을 인증할 수 없도록 설계되어있다.

Ⅳ. 공개키 기반의 안전한 Mobile IP 등록 프로토콜

본 논문에서는 Jacobs 제안의 단점을 해결하는 새로운 Mobile IP 등록 프로토콜을 제안한다. 제안된 등록 프로토콜은 공개키 암호화 방식을 최소한으로 사용하여 MN의 부담을 줄였으며, 인증서를 이용한 인증방식으로 에이전트(agent)들과 이동 노드(mobile node)간의 직접적인 인증이 이루어지도록 하였다. 또한 제안하는 프로토콜은 nonce를 이용한 등록 프로토콜을 기반으로 한다. 타임 스탬프를 이용한 등록 프로토콜의 경우 MN와 HA 사이의 시간 동기화 등의 문제가 있으므로, 보다 간결한 nonce를 이용한다.

4.1 기본 용어

본 논문에서 사용한 기본 용어는 다음과 같다.

- CA : 인증기관(Certification Authority)
- K_{HA}, K_{FA} : HA, FA의 공개키
- K_{HA}^{-1}, K_{FA}^{-1} : HA, FA의 개인키
- $Cert_{HA}$, $Cert_{FA}$, $Cert_{MN}$: HA, FA, MN의 인증서
- <<M>> K_A^{-1} : A의 개인키를 이용한 메시지 M의 디지털 서명
- N_{HA}, N_{FA}, N_{MN} : 각각의 HA, FA, 그리고 MN의 nonce
- *advertisement* : 광고 메시지를 나타내는 비트 패턴

4.2 제안 프로토콜

MN가 FA로 이동하여 FA의 COA를 획득하는 과정은 다음과 같다.

· Agent Advertisement :

(AA1) FA→MN : M_1

M_1 = *advertisement*, FA_{id}, MN_{COA}

MN는 FA가 보내는 광고 메시지를 받아서 FA의 ID(주소)와 COA를 획득한다. FA의 광고 메시지요소는 기본적인 요소만을 포함하여 무선환경에서의 오버헤드를 줄일 수 있게 하였다. 다음 과정으로 FA는 자신이 획득한 COA를 HA에게 등록하게 된다.

· Registration :

(R1) MN→FA : M_2, $<M_2>_{S_{MN\text{-}HA}}$, $Cert_{MN}$
M_2 = *Request*, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}

(R2) FA
· validate $Cert_{MN}$

(R3) FA→HA : M_3, $<<M_3>>_{K_{FA}^{-1}}$, $Cert_{FA}$
M_3 = M_2, N_{FA}

(R4) HA
· validate $Cert_{FA}$
· validate $<<M_3>>_{K_{FA}^{-1}}$ using K_{FA}
· decryption $<M_2>_{S_{MN\text{-}HA}}$, using Secret key, $S_{MN\text{-}HA}$
· validate N_{HA}

(R5) HA→FA : M_4, $<<M_4>>_{K_{HA}^{-1}}$, $Cert_{HA}$
M_4=M_5, N_{FA}
M_5=*Reply*, *Result*, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}, $<M_5>_{S_{MN\text{-}HA}}$

(R6) FA
· validate N_{FA}
· validate $Cert_{HA}$
· validate $<<M_4>>_{K_{HA}^{-1}}$

(R7) FA→MN : M_5

(R8) MN
· validate $<M_5>_{S_{MN\text{-}HA}}$
· validate N_{MN}

등록을 위해서 MN는 기존의 Mobile IP와 같은 방식의 작업을 수행한다. MN는 자신이 획득한 COA와 등록요청 메시지를 MN와 HA의 비밀키를 통해 MAC 값을 얻어, 등록 요청 메시지와 함께 전송한다(R1). 이 메시지에는 MN의 인증서인 $Cert_{MN}$가 포함되어있다. MN는 $Cert_{MN}$를 생성하기 위하여 스마트 카드를 이용하거나, 자신의 인정서가 보관되어있는 CA의 URL을 FA에게 보내주게 함으로써, $Cert_{MN}$생성에 대한 부담을 줄일 수 있게 한다. 이러한 메시지를 받은 FA는 MN을 인증한 CA에 접속하여 MN의 인증서인 $Cert_{MN}$를 확인한다(R2). FA는 MN에게서 받은 요청 메시지에 자신의 nonce를 포함하여 FA의 개인키, K_{FA}^{-1}을 이용하여 암호화한 후 FA의 인증서인 $Cert_{FA}$와 함께 HA에게 보낸다(R3). HA에서는FA의 CA에 접속하여 $Cert_{FA}$를 확인한 후 FA의 공개키, K_{FA}를 획득하여 $<<M3>>_{K_{FA}^{-1}}$를 복호화하여 FA를 인증한다. 또한, HA와 MN의 비밀키인 $S_{MN\text{-}HA}$를 이용하여 $<M_2>_{S_{MN\text{-}HA}}$를 확인하고 N_{HA}를 확인하여 MN을 인증한다(R4). FA와 MN의 인증과정이 끝난 후 HA는 MN의 등록요청에 대한 응답 메시지를 FA에게 전달한다(R5). 이 응답 메시지에는 FA가 HA를 인증할 수 있는 인증서인 $Cert_{HA}$가 포함되어 있고, HA의 새로운 nonce인 N'_{HA}를 다시 생성하여 메시지에 첨가시킨다. FA는 HA의 메시지를 받은 후, N_{FA}와 $Cert_{HA}$를 검사하여 HA를 인증하는 과정을 거친다(R6). FA는 HA의 인증기관에 접속하여 $Cert_{HA}$를 확인한 후 HA의 공개키, K_{HA}^{-1}를 획득한 후 $<<M_4>>_{K_{HA}^{-1}}$를 확인한다. HA에 대한 FA의 인증과정이 끝나면 FA는 MN에게 등록에 대한 응답 메시지를 전달한다(R7). 응답 메시지를 받은 MN는 N_{MN}를 확인하고, MN와 HA의 비밀키($S_{MN\text{-}HA}$)를 이용하여 메시지를 인증한다(R8).

그림 1은 제안 프로토콜의 시퀀스 다이어그램을 보여준다.

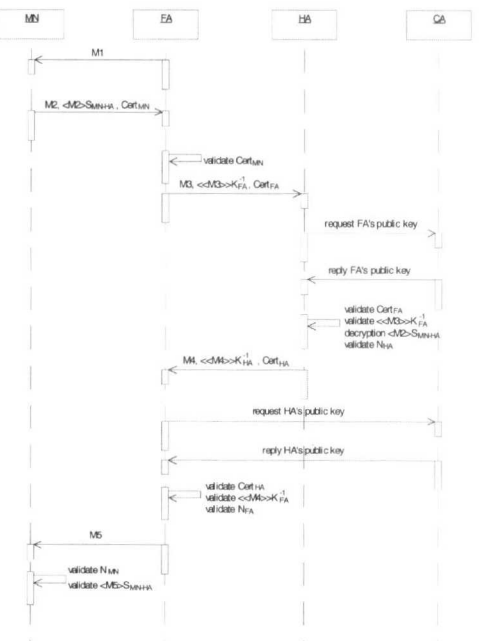


그림 1. 제안 프로토콜의 시퀀스 다이어그램

4.3 분석 및 평가

제안한 프로토콜은 기본적으로 Mobile IP 등록 프로토콜의 기본적인 절차를 유지하여 기존의 프로토콜 및 다른 확장 프로토콜들과의 호환성을 가질 수 있도록 하였다.

MN가 COA를 획득하는 과정에서 무선환경의 특성을 고려하여 광고 메시지(advertisement message)의 요소를 최소화하여 오버헤드를 줄일 수 있도록 하였다.

MN에서는 공개키 암호화의 사용을 최소화하기 위해 자신의 인증서인 $Cert_{MN}$를 발행할 때 스마트 카드를 이용하거나, 인증서가 보관되어있는 CA (Certificate Authority)의 URL을 전송하여 FA가 인증서를 확인할 수 있도록 설계하였다.

기존의 프로토콜에서는 FA가 단순히 MN과 HA의 메시지를 전송하는 수동적인 기능만을 수행하였으나, 제안 프로토콜에서는 FA가 MN과 HA를 직접 인증할 수 있도록 하였기 때문에, 위장된 HA와 MN의 재사용 공격(replay attack)으로부터 보호될 수 있다. 또한, FA에 대한 인증이 없던 기존의 방식과는 달리 FA를 인증할 수 있도록 설계되었기 때문에, FA로 위장한 공격자가 MN에 대한 서비스 거부 공격(denial service attack)을 하기 힘들도록 하였다.

그러나 공개키 기반 구조를 이용함으로써 프로토콜 전반에 오버헤드가 발생되었다. 인증기관과의 경로 구축에 대한 오버헤드 및 인증서 취소 목록(Certificate Revocation List, CRL)의 업데이트, 전자 서명 생성 및 확인 등으로 인하여 FA와 HA의 부담이 증가하였다. 그러나 FA와 HA가 유선환경이고 이러한 절차들을 수행하기 위한 충분한 연산능력(computing power)을 갖출 수 있다고 판단된다.

V. 시뮬레이션 결과

제안된 프로토콜의 성능을 평가하기 위하여 비밀키만을 이용한 기존의 등록 프로토콜과 공개키를 이용하는 Sufatrio, K. Lam의 등록 프로토콜, 그리고 본 논문에서 제안하는 등록 프로토콜에 대한 각각의 Request, Reply 등록 메시지 패킷을 만들어 MN와 FA사이의 유선과 무선 통신 성능을 평가하였다. 유선과 무선의 통신속도는 각각 9600bps로 설정하였다. 제안한 프로토콜은 기본적으로 Mobile IP 등록 프로토콜의 기본적인 절차를 유지하여 기존의 프로토콜 및 다른 확장 프로토콜들과의 호환성을 가질 수 있도록 하였다. 또한, MN가 COA를 획득하는 과정에서 무선환경의 특성을 고려하여 광고 메시지(advertisement message)의 요소를 최소화하여 오버헤드를 줄일 수 있도록 하였다.

MN에서는 공개키 암호화의 사용을 최소화하기 위해 자신의 인증서인 CertMN를 발행할 때 스마트 카드를 이용하거나, 인증서가 보관되어있는 CA의 URL을 전송하여 FA가 인증서를 확인할 수 있도록 설계하였다.

시뮬레이션 환경으로 OS는 Windows 2000 Server, PC는 Pentium Ⅲ 제온 800Mhz dual, Tool은 OPNET 8.0을 사용하였다.

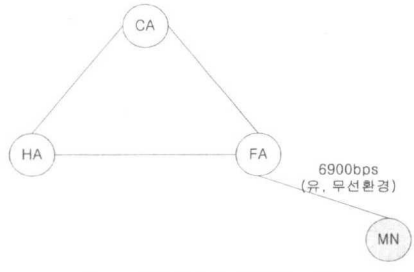


그림 2. 시뮬레이션 네트워크 환경

시뮬레이션의 네트워크 환경은 그림 2와 같다.

그림 3, 4, 5, 6는 등록 request, replay 패킷에 대한 유선환경에서의 통신성능을 평가한 것이고, 그림 7, 8, 9, 10은 등록 request, reply 패킷에 대한 무선환경에서의 통신성능을 평가한 것이다. 본 논문에서 제안한 등록 프로토콜과 기존의 비밀키 등록 프로토콜을 비교하여 보면 제안 프로토콜은 공개키를 사용하기 때문에 비밀키를 사용할 때보다는 통신성능평가는 낮게 나왔으나 이는 공개키를 이용함으로써 생기는 오버헤드 때문이며 상대적으로 replay attack이나 다른 보안공격으로부터 안전할 수 있다. 또한, 같은 공개키와 비밀키를 이용하는 Sufatrio, K. Lam 등록 프로토콜보다 등록 프로토콜 메시지의 요소를 줄임으로써 통신성능을 향상시킬 수 있었다.

그림 3, 4는 등록요청패킷(Registration request packet)에 대한 유선 환경에서의 Utilization과 End-to-End Delay를 평가한 것이다. 그림에서 Sufatrio의 등록 프로토콜이 성능평가가 가장 낮게 나왔다. 또한, 본 논문에서 제안한 프로토콜과 기존 비밀키만을 사용한 프로토콜의 성능을 비교하여 보면 약간의 차이는 나지만 이는 공개키를 사용하여

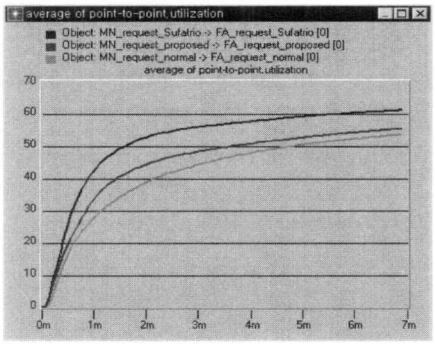


그림 3. 유선환경에서의 Utilization
(Registration request packet)

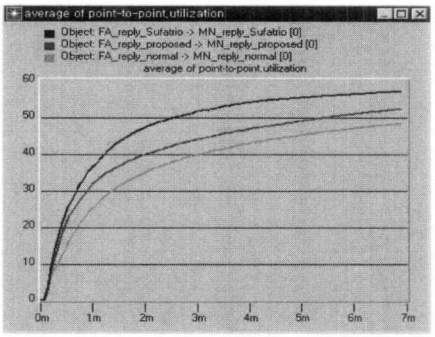


그림 5. 유선환경에서의 Utilization
(Registration reply packet)

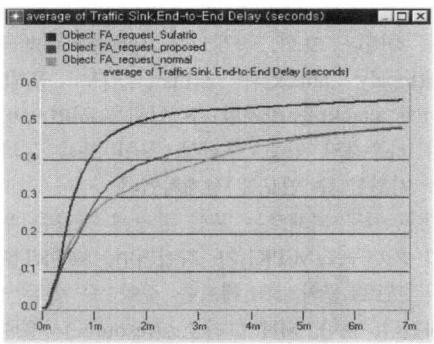


그림 4. 유선환경에서의 ETEdelay
(Registration request packet)

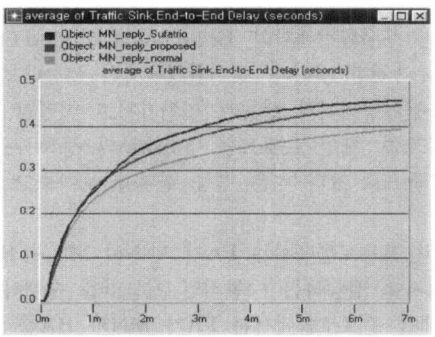


그림 6. 유선환경에서의 ETEdelay
(Registration reply packet)

생기는 오버헤드 때문이며, 인증과정에 있어서는 제안 프로토콜이 보안문제에 있어서 공개키를 사용하여 얻을 수 있는 안전한 인증, 보안공격에의 대응, 부인봉쇄서비스 제공 등과 같은 장점을 획득할 수 있다.

그림 5, 6은 등록응답패킷(Registration reply packet)에 대한 유선 환경에서의 Utilization과 End-to-End Delay를 평가한 것이다. 실험 결과는 등록요청패킷과 마찬가지로 비밀키 등록 프로토콜, 제안 프로토콜, Sufatrio의 순으로 보다 나은 성능 결과를 보여주고 있다. 등록응답패킷은 등록요청패킷보다 메시지 요소가 적기 때문에 등록요청패킷보다 성능이 좋음을 보여주고 있다.

그림 7, 8, 9, 10은 등록요청패킷, 등록응답패킷

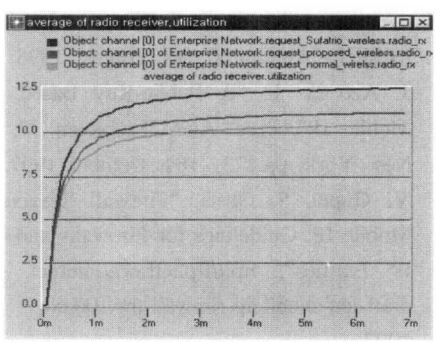


그림 7. 무선 환경에서의 Utilization
(Registration request packet)

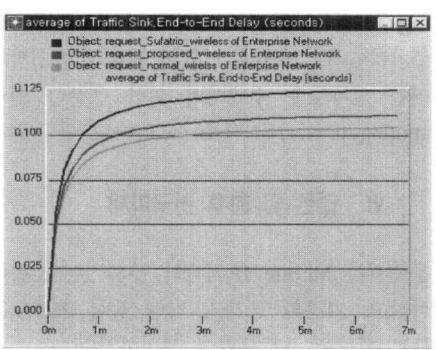


그림 8. 무선 환경에서의 ETEdelay
(Registration request packet)

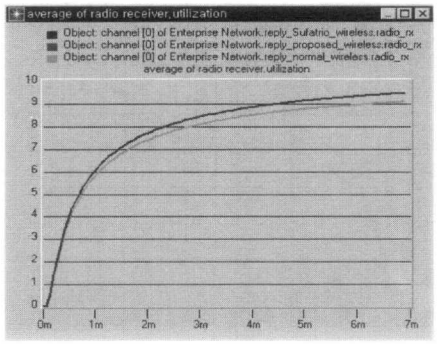


그림 9. 무선 환경에서의 Utilization
(Registration reply packet)

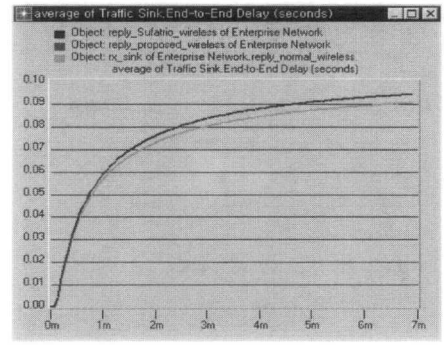


그림 10. 무선 환경에서의 ETEdelay
(Registration reply packet)

에 대한 무선환경에서의 Utilization과 End-to-End Delay를 측정한 것이다. 무선환경에서의 성능비교는 앞선 유선환경에서의 성능과 마찬가지고 비밀키 등록 프로토콜, 제안 프로토콜, Sufatrio의 등록 프로토콜의 순으로 보다 나은 성능 결과를 보여주고 있다.

기존의 프로토콜에서는 FA가 단순히 MN과 HA의 메시지를 전송하는 수동적인 기능만을 수행하였으나, 제안 프로토콜에서는 FA가 MN과 HA를 직접 인증할 수 있도록 하였기 때문에, 위장된 HA와 MN의 재사용 공격(replay attack)으로부터 보호될 수 있다. 또한, FA에 대한 인증이 없던 기존의 방식과는 달리 FA를 인증할 수 있도록 설계되었기 때문에, FA로 위장한 공격자가 MN에 대한 서비스 거부 공격(denial service attack)을 하기 힘들도록 하였다.

그러나 공개키 기반 구조를 이용함으로써 프로토콜 전반에 오버헤드가 발생되었다. 인증기관과의 경로 구축에 대한 오버헤드 및 인증서 취소 목록(Certificate Revocation List, CRL)의 업데이트, 전자 서명 생성 및 확인 등으로 인하여 FA와 HA의 부담이 증가하였다. 그러나 FA와 HA가 유선환경이고 이러한 절차들을 수행하기 위한 충분한 연산능력(computing power)을 갖출 수 있다고 판단된다.

Ⅵ. 결론 및 향후 연구과제

본 논문에서는 Mobile IP에서의 등록 프로토콜에 대해 분석하고, 기존의 공개키 기반 등록 프로토콜을 보완하는 새로운 프로토콜을 제시하였다.

공개키 암호 알고리즘을 최소한으로 사용함으로써, 무선환경에서도 적합한 공개키 기반 구조가 되도록 하였다. 또한, 공개키를 사용함으로써 재사용 공격(repaly attack)과 서비스 거부 공격(denial service attack)을 방지할 수 있도록 하였으며, 메시지와 사용자의 인증, 무결성, 부인 봉쇄 등의 서비스를 지원할 수 있도록 설계하였다.

향후 연구 과제로는 무선 환경에 적합한 무선 공개키 기반구조(M-PKI)가 확정되면, M-PKI를 이용하여 프로토콜의 오버헤드를 줄일 수 있는 연구가 기대된다. 또한, MN의 리소스(resource)사용에 대한 과금(accounting)과 관련된 보안문제도 좋은 연구가 될 것이다.

참 고 문 헌

[1] C. Perkins. ed., "IP Mobility Support," IETF RFC2002, October 1996.

[2] C. Perkins. ed., "IP Mobility Support version 2," Internet Draft, <draft-ietf-mobileip-v2-00.txt >, November 1997.

[3] S. Jacob, "Mobile IP Public Key Based Authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-00.txt>, August 1998.

[4] J. Azo et al., "A Public-Key Based Secure Mobile IP", Proc. ACM Mobicom 97, ACM, New York, pp.173~184, October 1997.

[5] V. Gupta, S. Glass, "Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP Entities", ftp://ftp.ietf.org/internet -drafts/dratf-ietf-mobileip-firewall-trav-00.txt, March 1997.

[6] A.J. Menezes, P.C. Oorschot, S.A. Vanstone, "Handbooks of Cryptography", CRC Press,

Boca Raton, 1997

[7] C. Perkins, "IP Mobility Support for IPv4, revised", Internet Draft, <draft-ietf-mobileip-rfc2002-bis-02.txt> , July 2000

[8] S. Jacobs, "Mobile IP Public Key Based Authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-00.txt>, August 1998.

[9] R.L. Schneier., "Applied Cryptography, 2nd edition: Protocol, Algorithms, and Source Code in C," Wiley, New York, 1996.

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

박 상 준(Sang Jun Park) 학생회원

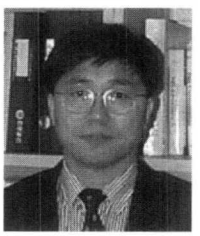
2000년 : 경희대학교 전자공학과 졸업 (학사)

2000.3 ~ 2002.2 : 경희대학교 전자공학과 (공학석사과정)

2002.3 ~ 현재 : 신도리코 중앙연구소

<주관심 분야> 네트워크 보안, 무선인터넷 보안

홍 충 선(Choong Seon Hong) 정회원



1983년 : 경희대학교 전자공학과 졸업 (학사)

1985년: 경희대학교 전자공학과 (공학석사)

1997년 : Keio University, Department of Information and Computer Science (공학박사)

1988년 ~ 1999년: 한국통신 통신망 연구소 선임 연구원/ 네트워킹연구실장

1999년 ~ 현재: 경희대학교 전자정보학부 조교수

<주관심 분야> 인터넷 서비스 및 망 관리 구조, 분산 컴포넌트관리, IP 프로토콜, 멀티미디어 스트리밍 등

이 대 영(Dae Young Lee) 정회원

1964년: 서울대 물리학과 졸업 (학사)

1971년: 캘리포니아 주립대학원 컴퓨터학과 (공학석사)

1979년: 연세대학교 전자공학과 (공학박사)

1971년 ~ 현재: 경희대학교 전자정보학부 교수

1990년 ~ 1993년 : 경희대학교 산업정보대학원 대학원장

1999년 ~ 2000년 : 한국통신학회 회장

<주관심 분야> 영상처리, 컴퓨터 네트워크, 컴퓨터 시스템