Mobile IPv6에서 공개키와 비밀키를 이용한 등록 프로토콜

*허용준 *홍충선 *이대영
*경희대학교 전자정보학부

The Registration Protocol using a Public-Key and Secret-Key in Moile IPv6

*Yong Joon Heo *Choong Seon Hong *Dae Young Lee
*School of Electronics & Information, Kyung Hee University.

요약

Mobile IPv6는 호스트에 이동성을 제공하여주는 Mobile IPv4의 부족한 주소문제를 해결하고자 제안된 차세대 프로토콜이다. 본 논문에서는 Mobile IPv6의 이동노드와 메시지 인증을 위한 단방향 공개키 암호화 기법과 비밀키 기법을 제안한다. 제안된 프로토콜은 이동노드의 인증과 메시지 인증을 위하여 공개키 암호화 기법을 최소화하였으며, 또한 전송 메시지를 최소화함으로해서 이동노드의 부담을 줄이도록 설계하였다.

Ⅰ.서론

인터넷 사용자들의 폭발적인 증가와 이에 따른 부족한 IP주소를 해결하고자 IETF워킹그룹에서 IPv6프로토콜을 제안하게 되었다. 기존의 32비트 주소체계에서 128비트의 주소체계로 증가하게 되었는데, Mobile IPv6는 이러한 IPv6에 이동성을 제공하여주기 위해 제안된 프로토콜이다. Mobile IP프로토콜은[1] 전송 계층의 연결 유지와 IP 계층의 라우팅 문제 해결을 위하여 2개의 IP 주소를 사용한다. 이 2개의 주소 중 하나인 홈주소(Home Address)는 고정된 값으로, TCP연결의 구별등을 위하여 사용되고, 다른 하나의 주소인 COA(care-of-Address)는 새로운 연결 지점마다 값이 바뀌어 이동노드(Mobile node, MN)의 현재의 위치를 반영하는 주소로 이용된다. MN는 홈 네트워크(Home Network)로부터 홈 주소를 부여 받는다. 홈 네트워크는 보통 MN가 등록된 사설 네트워크 또는 사업자 네트워크로서 HA(Home Agent)노드를 포함하는 네트워크이다. 노드가 이동해 홈 네트워크에 연결되어 있지 않고 외부 네트워크(Subnetwork)에 연결되어 있을 때. HA는 초기 MN를 목적지로 한 패킷을 전달받아 MN가 현재 연결된 곳으로 전달하게 되는데 이를 위해 MN는 연결 지점을 바꿀 때마다 새로운 CoA를 HA와 CN에게 등록한다.

본 논문에서는 이러한 Mobile IPv6의 등록 프로토콜에 대해서 알아보고, 공개키와 비밀키를 이용한 안전한 Mobile IPv6 등록 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 MobileIPv6의 등록 프로토콜에 관한 관련 연구에 대해 알아보고 각각의 프로토콜에서의 문제점을 분석한다. 3장에서 본 논문이 제안한 프로토콜을 설명한후, 마지막으로 4장에서 결론 및 향후 연구 방향을 제시한다.

Ⅱ,관련 연구

2.1 Sufatrio, K.Lam의 기법

Sufatrio, K. Lam[5]은 Jacobs[4]의 인증 프로토콜에

본 논문은 2001년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2001-003-E00210)

서 Mobile IP 등록 프로토콜에 공개키와 비밀키를 병행하여 사용함으로써 공개키 기반 암호화의 사용을 줄이는 연구를 하였다.

비밀키를 기반으로 하는 현재의 Mobile IP 인증은 확장이 힘들다는 단점이 있고 상거래에서 중요한 부인봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 공개키 기반의 인증방법을 제안하게 되었는데, 그러나 공개키 암호방식을 사용하면서 제안된 프로토콜은 여러 가지 문제점들이 도출되었다. 그 중 가장 큰 문제점은 MN에서의 공개키 암호화기법이 무선 환경에 맞지 않는다는 것이다. 이동 단말기의 특성상 MN에서의 연산 능력은 제한이 있다.

또 다른 문제점은 MN의 시스템이 복잡해 진다는 것이다. 공개키와 인증서를 생성하기 위해서는 MN에서의 하드웨어나 소프트웨어의 추가가 불가피해지고, 이러한 점들은 MN의 성능을 저하시키는 요인이 된다.

2.2 Return Routability의 기법을 사용한 BAKE

Mobile IPv6에서 새롭게 제안된 인증 프로토콜인 BAKE (Binding Authentication Key Establishment) [6]는 MN와 CN사이의 Binding 메시지 인증을 위해 제안된 프로토콜로서 인터넷의 임의의 위치에 존재하는 공격자에 대한 보호를 목표로 하고 있다.

BAKE에서 사용하는 기본용어는 다음과 같다.

- K_(MN, HA) : MN와 HA사이에 공유되어지는 키값
- K_CN : CN에 의해 생성되어지는 random number
- N1 : MN에 의해 생성되어지는 random number.
- T0=HASH_T0 (K_(MN, HA);N1'||CoA||CNA||HoA)
- T1=HASH_T1 (T0)
- N2:=HASH_N2 (K_CN;0||T1)
- T2:=HASH_T2(K_CN;T1||CoA||CNA||HoA)
- N_BK : MN에 의해 생성되어지는 random number.
- BK:=HASH_BK(N_BK||N2)

그리고 BAKE의 메시지 인증과정은 다음과 같다.

(1) Binding Warning

MN : {CoA, HoA, K_(MN,HA), N1}→초기값

HA : {CoA, HoA, K_(MN,HA)}→초기값

CN : {CNA, K_CN}→초기값

MN→CN : <CoA, CNA, HoA, N1, T1>

MN : {CoA, HoA, K_(MN, HA), N1}

HA : {CoA, HoA, K_(MN, HA)}

CN : {CNA, K_CN } + {CoA, HoA, N1, T1}

(2) Binding Key Request

CN→HA : <CNA, HoA, N1, T1, N2, T2>

HA: {CoA, HoA, K_(MN, HA), CNA, N1, T1, N2, T2}

HA→MN:TUNNEL<CNA, HoA, N1, T1, N2, T2>

HA : {CoA, HoA, K_(MN, HA)}

MN : {CoA, HoA, CNA, K_(MN, HA), N1, T0}

(3) Binding Key Establishment

MN→CN : <CoA, CNA, HoA, T0, T2, N_BK>

Binding Key Establishment 메시지를 통해서 T2를 검증하고 CN와 MN간의 인증을 위한 BK를 생성, 이를 통해 MN와 CN간의 패킷전송이 이루어지게 된다.

하지만 제안된 BAKE메시지 인증과정에서 보여지듯 인증과정에 쓰여지는 메시지가 많아 MN에 부담이 될 수 있고, CN의 신뢰성이 보장되지 못한다는 단점이 있다.

Ⅲ. 공개키 기법과 비밀키를 이용한 MobileIPv6 등록프로토콜

본 논문에서는 기존의 공개키 암호화기법을 사용한 인증과 BAKE protocol의 단점을 해결하기 위한 새로운 Mobile IPv6 등록 프로토콜을 제안한다. 제안된 등록 프로토콜은 공개키 암호화 방식을 최소한으로 사용하여 MN의 부담을 줄이고, 공개키와 비밀키를 사용하여 등록 프로토콜에서 요구되어지는 메시지 수를 최소한으로 줄이도록 하였다.

본 논문에서 사용한 기본 용어는 다음과 같다.

- PK_CN : CN의 공개키
- PK_CN{ } : CN의 공개키로 암호화된 메시지
- K_HA : HA의 비밀키
- K_HA{ } : HA의 비밀키로 암호화된 메시지

· K_(MN, CN) : MN와 CN간에 인증을 위해 사용되어지는 비밀키
· T : 재전송공격 방지를 위한 time stamp
· $Cert_{CN}$: CN의 인증서

제안하는 프로토콜의 수행과정은 다음과 같다.

· Registration :

(R1) MN□HA : K_HA{ K_(MN, CN), T, CoA}, HoA, CNA

(R2) MN□CN : K_HA{ K_(MN, CN), T, CoA}, HoA, CNA

MN은 Binding Cache에 저장하고 있던 K_HA로 MN와 CN사이의 인증을 위해 쓰일 K_(MN, CN)와. T를 암호화하여 HA와 CN에게 보낸다.

(R3) CN□HA : PK_CN{ K_CN, }, HoA, $Cert_{CA}$

CN이 MN로부터 받은 HA의 비밀키를 알아내기 위하여 HA에게 자신의 인증서와 비밀키를 CN의 공개키로 암호화하여 보내게 된다.

(R4) HA

CA(인증기관)을 통하여 CN의 공개키를 얻고, CN으로부터 받은 메시지를 복호화하여 CN의 비밀키를 얻는다.

(R5) HA□CN : K_CN{ K_(MN, CN), T, CoA, K_HA }, HoA

CN의 비밀키로 MN에게서 받았던 K_(MN, CN)와 T, CoA 그리고 자신의(HA) 비밀키를 암호화하여 CN에게 보내게 되다.

(R6) CN

HA에게서 받았던 메시지를 복호화하고 HA를 통한 K_(MN, CN)과 MN에게서 받았던 K_(MN, CN)값을 비교 인증과정을 마치게 된다.

Ⅳ. 결론 및 향후 연구과제

본 논문에서는 Mobile IPv6에서의 등록 프로토콜에 대해 분석하고, 등록 프로토콜에서 요구되어지는 보안사항을 통해 연구되고 있는 프로토콜들의 특성을 살펴 봄으로써 각각의 프로토콜이 가지고 있는 문제점을 해결하고자 공개키와 비밀키를 이용하는 새로운 프로토콜을 제시하였다. 공개키 암호 알고리즘을 최소한으로 사용함으로써, 무선 환경에서도 적합한 공개키 기반 구조가 되도록 하였고, 메시지의 수를 줄임으로 해서 MN의 부담을 줄일 수 있었다.

향후 연구과제로는 제안된 프로토콜의 시뮬레이션 결과를 토대로한 검증이 요구되고, 무선 환경에 적합한 무선 공개키 기반구조(M-PKI)를 통해 프로토콜의 오버헤드를 줄일 수 있는 연구가 기대된다.

참 고 문 헌

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

[2] C. Perkins. ed., "IP Mobility Support version2" Internet Draft, <draft-ietf-mobileip-v2-00.txt>, November 1997.

[3] T. Aura , Micsrosoft, J. Arkko, Ericsson "MIPv6 BU Attacks and Defenses", Internet Draft, <draft-aura-mipv6-bu-attacks-01.txt>, August 2002.

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

[5] Sufatrio, K. Laml, "Mobile IP Registration Protocol : A Security Attack and New Secure Minimal Public- Key Based Authentication", I-SPAN;9, June 1999.

[6] C. Perkins, "Binding Authentication Establishment Protocol for Mobile Ipv6" Internet-draft <draft-perkins-bake-01.txt> 2 july 2001.

[7] Sang-jun Park. "The Authentication Mecahnism using Public-Key Infrastructure in Mobile IP Registration Protocol", 한국통신학회, 2001.

[8] K.J. Lee, S.Y. Lee, Y.J. Kim "Mobile IPv6개발 동향", http://www.ipv6.or.kr/TM/TM2001-005.pdf , 2001.

[9] K.J. Lee ETRI "Binding Authentication Key Establishment-Mobile IPv6", http://www.ipv6.or.kr/wg/security/Interim/01-006.pdf , Nov 2001