Mobile IPv6 BU(Binding Updates)인증 방안에 관한 연구

임강규, 남길현

국방대학교, 전산정보학과

A Study on the BU(Binding Updates) Authentication Methods In Mobile IPv6

Kang-Kyu Lim, Kil-Hyun Nam

Department of Computer & Information Science, National Defense Univ.

요 약

본 논문에서는 Mobile IPv6 환경에서 보안성이 있는 인증 메커니즘을 제안한다. Internet draft에서 제안하고 있는 RR 방식의 BU 인증 메커니즘은 MN-CN, HA-CN간 두 경로 모두에 공격자가 접근하지 못한다는 전제로 인해 BU 인증을 위한 공유키 생성 시 취약성을 내포하여 만약 공격자가 두 경로 모두에 접근 가능할 경우 노드간 통신하는 전 단계에 걸쳐 수동적, 능동적 공격에 노출되게 된다. 제안한 BU 인증 메커니즘은 최초 안전한 BU 인증을 위한 공유키를 생성 후 차후 이어지는 BU 인증은 이러한 안전성을 바탕으로 신속한 인증이 이루어지는 2단계의 인증 메커니즘을 제안함으로써 공유키의 노출을 최소화하여 보다 높은 수준의 보안을 제공하였다.

I. 서 론

현재 이동 노드를 사용하여 인터넷을 접속하는 사용자를 위해 이동성(Mobility)을 제공하는 방법인 Mobile IP는 IETF(Internet Engineering Task Force)의 mobileip(IP Routing for Wireless / Mobile Hosts) W/G에 의해 개발된 프로토콜로써 위치를 이동하여 인터넷 접속점 변경을 가능하게 하는 이동성 지원을 IP 계층에서 지원하여 전송계층 이상에서의 연결을 투명하게 유지한 상태에서 물리적 접속을 변경할 수 있도록 허용한다.

Mobile IP에서 새로운 위치 정보를 등록하는 과정을 바인딩 갱신(BU : Binding Update)이라고 하며, BU 인증을 위한 여러 가지 제안들이 있었지만, 현재 Internet draft[1]에서는 RR(Return Routability) 방식을 제안하고 있다. 그러나 이 RR 방식은 전체적인 인증 시간은 짧은 반면, MN (Mobile Node)과 CN(Correspondent Node)에 이르는 두 가지 경로에 대한 인증을 바탕으로 하고 공유키를 생성하기 위하여 전송되는 메시지들이 평문이므로 두 경로 모두에 접근 가능한 공격자에게 쉽게 노출이 되는 취약성을 가지고 있다.

본 논문에서는 Mobile IP를 이용할 때 안전하고 효율적인 BU 인증 메커니즘을 제안한다. 그리고 제안하는 메커니즘의 고려요소 중 가장 중요한 것은 경로 접근이 가능한 공격자라 하더라도 쉽게 공유키를 생성하지 못하게 하는 안전성과, 이동 노드의 특성인 제한된 자원과 프로세싱 능력을 고려하여 신속성을 확보하는 것이다.

제안한 BU 인증 메커니즘은 최초 안전한 BU 인증을 위한 공유키를 생성 후 차후 이어지는 BU 인증은 이러한 안전성을 바탕으로 신속한 인증이 이루어지는 2단계의 인증 메커니즘을 제안함으로써 공유키의 노출을 최소화하여 보다 높은 수준의 보안을 제공할 수 있다.

II. MIPv6 draft 상의 RR방식의 BU 인증 분석

1. BU 인증 절차

RR절차는 MN이 CN에게 보내는 CoA(Care-of Address)와 HoA(Home Address)가 사실상 도달

가능한 주소인지 어느 정도 합리적인 보장을 해준다. 오직 이 보장만으로 CN은 MN으로부터 오는 BU를 받아들일 수 있고, MN으로 보내는 데이터 트래픽을 MN이 요구한 CoA로 전송한다. 이것은 MN이 요구한 2개의 주소(CoA, HoA)로 명기된 패킷들이 MN으로 전송되는지를 테스트하여 이루어지고, MN은 CN이 CoA, HoA로 보내는 특정 데이터(keygen tokens)를 수신했다고 증명할 수 있으면 그 테스트를 통과시킨다. MN은 이러한 데이터를 결합해서 Kbm으로 표기되는 바인딩 관리키(binding management key)를 만든다. 그림 1과 그림 2는 RR 절차의 전체적인 과정을 보여준다.

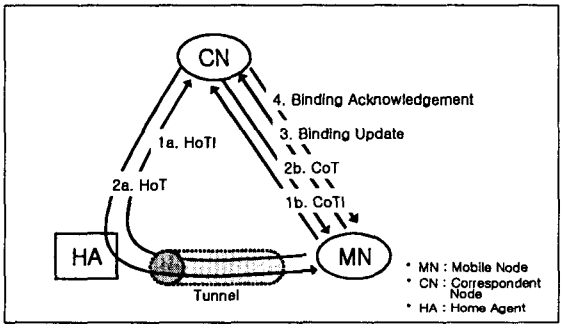

그림 1: BU 키 확립을 위한 RR 절차 동작 과정

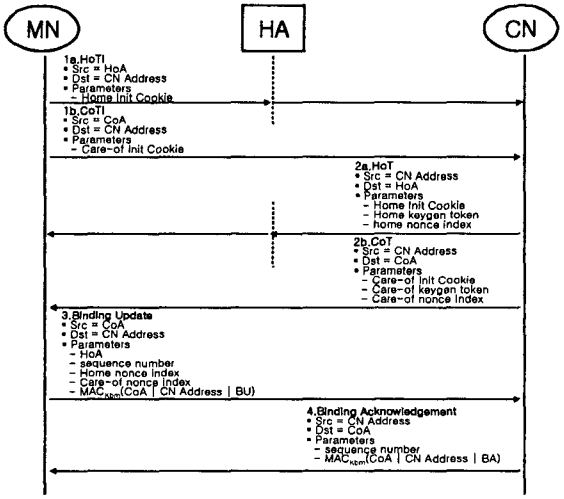

그림 2: RR 절차에 의한 BU 메시지 전달 과정

HoTI(Home Test Init message)와 CoTI(Care-of Test Init message)들은 동시에 CN에게 보내지며, HoT(Home Test message)와 CoT (Care-of Test message)들은 거의 동시에 MN에게 되돌려지고, 이 네 개의 메시지들이 RR 절차를 구성한다. 이 절차에서 CN은 아주 적은 프로세스를 필요로 하게 된다.

MN이 HoT, CoT 메시지를 둘 다 받으면 RR 절차는 완료된다. RR 절차의 결과로 MN은 BU를 CN에게 보내는데 필요한 데이터를 확보하게 된다. MN은 바인딩 관리키인 Kbm을 만들기 위해 token들을 아래와 같이 해쉬함수 SHA1로 계산한다.

$$Kbm = SHA1\,(homekeygentoken \mid careofkeygentoken) \quad (1)$$

MN이 Kbm을 만들고 난 후, CN에게 검증 가능한 BU를 제공할 수 있다. 그림 3은 BU등록 절차와 이를 인증하기 위한 BA메시지 흐름을 보여준다.

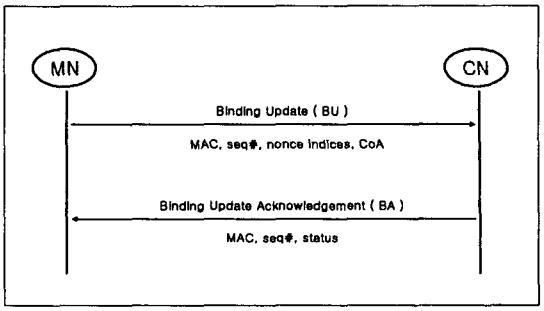

그림 3: BU, BA 메시지 전송 과정

2. RR 인증방식의 취약점 분석

RR(Return Routability)는 BU 보호를 위해 CN에서 HA를 경유하여 MN에게 보낸 패킷의 수신 여부를 확인하는 방식으로 이것은 HA는 홈 등록을 통해 MN의 정확한 위치를 알고 있을 것으로 가정하여 MN에게 터널링[4]을 통하여 정확히 전달할 수 있을 것으로 기대하고 암호키 구성에 사용되는 값, 메시지의 인증 및 재전송 방지를 위한 비표(nonce)나 토큰 등을 보내며, MN으로부터의 응답을 통해 전송된 값이 제대로 전달되었는지 확인한다. RR 인증방식의 중요한 보안 특성들은 다음과 같다.

첫째, HA와 MN 사이의 중요 정보는 IPsec ESP[2]에 의해 보호된다. 이것은 공격자가 MN 주위의 네트워크에 위치하더라도 ESP가 보호하는 정보를 볼 수 없으므로 공격을 불가능하게 만든다. 그러나 ESP의 보호를 받지 못하는 HA-CN 구간에 위치하는 공격자에 대한 방어는 제공하지 못한다.

둘째, 대칭적 메시지 교환을 사용하여 CN이 서비스 거부 공격의 경유지로 사용되는 반사 공격(reflection attack)을 방지한다.

셋째, CN은 BU가 이루어질 때까지 각 요청에 따른 어떠한 상태정보도 기억할 필요가 없는 방식으로 작동함으로써 상태 저장 공간의 소모를 이용하는 서비스 거부 공격을 방지한다.

넷째, 복잡한 연산을 요하는 공개키 암호를 사용하지 않으므로 해서 CPU 소모를 통한 서비스 거부 공격도 방지하고 있다.

그러나 전달되는 메시지는 암호화되지 않기 때문에 완벽한 보안을 제공하지는 못한다. 즉, CN과 HA 사이의 전송경로 상의 임의의 노드 또는 HA와 MN 사이의 전송이 암호화되지 않을 경우 해당 경로상의 임의의 노드가 CN이 MN에게 보낸 메시지들을 볼 수 있고, 따라서 이들 노드들은 MN을 위장하는 것이 가능해진다.

또한 MN이 링크 상에 있는 동안 BU가 보내지면 메스커레이드(Masquerade)와 중간자(MITM) 공격은 바인딩 유효기간을 설정함으로써 그러한 공격에 대한 노출을 제한할 수 있지만, 현재와 미래의 통신과 노드들에 대해서도 실시될 수 있다. 이러한 공격의 예는 네트워크에 한 번 방문한 노드가 더 이상 그 링크에 존재하지 않더라도 그 링크의 트래픽을 훔치는 경우이다. 즉, MIPv6에서의 공격은 공격자가 공격가능 위치를 떠난 후에도 지속된다는 것이다. 이러한 공격은 잘 알려진 주소를 가진 노드들에게만 적용할 수 있는 공격이다.

III. Mobile IPv6 BU 인증방식 제안 및 분석

1. BU 인증방식 제안

안전한 Kbm을 생성하기 위해 여러 가지 방법들이 있지만 제안하는 메커니즘은 두 가지이며, 첫째, 최초 BU 전송시 사용하는 인증방식은 Okamoto-Shirasi의 스타형 네트워크 구성을 바탕으로 한 방식[3]을 응용하여 안전한 Kbm을 생성하여 이를 장기간(long term key) 사용하고, 두 번째는 최초 BU 인증시 사용된 안전한 Kbm을 가지고 이후 이어지는 BU 시 이를 활용하는데 기존의 인터넷 드래프트[1]에서 제안하는 RR 방식의 인증방식을 응용하여 제안한다.

1) 1단계(최초 BU 전송시의 인증방식)

가) 스타형 네트워크 구성을 응용한 제안

최초 BU 전송시 사용하는 인증방식은 Okamoto-Shirasi의 스타형 네트워크 구성을 바탕으로 한 방식[3]을 응용하여 Kbm을 생성한다. 그림 4는 Kbm 생성절차를 나타낸다.

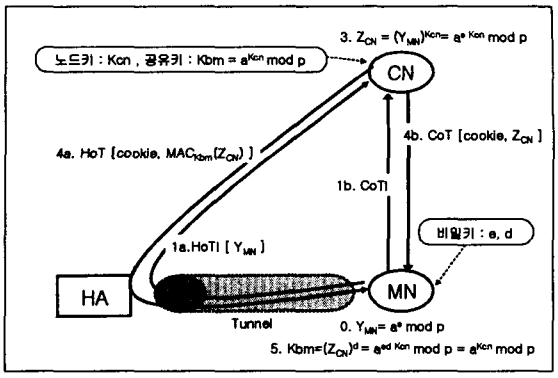

그림 4: 최초 BU 인증을 위한 제안 인증방식

Step 0. 인증과 키 교환 프로토콜이 시작되기 전에 MN과 CN은 키 교환 사전 준비작업으로 MN은 공개키 YMN을 미리 계산하고, CN은 공유키 즉 Kbm을 CN의 비밀키인 노드키 Kcn을 이용하여 미리 계산해 놓는다. 여기서 a, p는 공개된 것이다.

$$Y_{MN} = a^{e} \bmod p \qquad (2)$$

$$Kbm = a^{Kcn} \bmod p \qquad (3)$$

Step1. MN은 HoTI와 YMN을 HA를 경유하여 CN으로 전송하고, CoTI는 CN으로 직접 전송한다.

M1 : MN ⇒ HA ⇒ CN : HoTI [YMN]

M2 : MN ⇒ CN : CoTI

여기서 HoTI와 CoTI는 기존의 RR절차상의 것과 동일하나 HoTI의 매개변수에 YMN을 추가하였다.

Step2. CN은 수신한 YMN을 노드 키 Kcn으로 분배정보 ZCN을 계산한다.

$$Z_{CN} = (Y_{MN})^{Kcn} = a^{eKcn} \bmod p \qquad (4)$$

Step 3. CN은 분배정보 ZCN을 BU 관리키로 해쉬한 결과를 HA를 경유하여 MN에게 전송하고 분배정보 ZCN을 직접 MN에게 전송한다.

M3: MN⇒HA⇒CN: HoT[home init cookie, MACKbm(ZCN)]

M4: MN ⇒ CN : CoT[care-of cookie, ZCN]

Step 4. MN은 CN에서 직접 수신한 분배정보

ZCN에 비밀키 d로 바인딩 키인 Kbm을 계산하고 이 Kbm으로 CN에서 HA를 경유하여 전송한 BU 관리키로 해쉬한 결과인 MACKbm(ZCN)을 검증한다.

$$Kbm = (Z_{CN})^d = (Y_{MN})^{dKcn} = a^{edKcn} \bmod p = a^{Kcn} \bmod p \quad (5)$$

이 과정에서 생성된 Kbm은 Internet draft[1] 상의 BU 인증 방식에 비해 다소 계산량은 많지만 보안성이 있으므로 이후 이어지는 BU 인증을 위한 공유키로 장기간 사용할 수 있다.

나)공개키 시스템을 응용한 제안

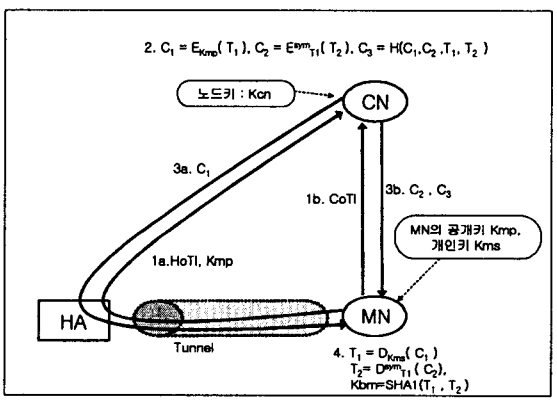

그림 5 공개키 시스템을 응용한 제안 방식

Step 1. MN은 BU 인증 시작을 위한 메시지 HoTI와 CoTI를 각각 HA와 CN에게 전송한다. 여기서의 HoTI는 MN의 공개키 Kmp를 포함하고 CoTI는 RR 방식과 동일하다.

Step 2. CN은 넌스를 생성하여 아래의 식으로 T1, T2를 만들고 이를 비밀키로 한다.

T1= First64(HMAC_SHA1(Kcn, (home address | nonce | 0)))
T2= First64(HMAC_SHA1(Kcn, (care-of address | nonce | 1)))

계산된 T1과 T2를 이용하여 MN에게 전송할 C1, C2, C3를 아래와 같이 계산한다.

$$C1 = E_{Kmp}(T1)$$
$$C2 = E^{sym}_{T1}(T2)$$
$$C3 = H(C1, C2, T1, T2)$$

Step 3. CN은 C1과 CKY_h를 MN에게 HA를 경유하여 전송하고 C2, C3, CKY_c는 MN에게 직접 전송한다. 이 쿠키들은 경로검증을 위해 사용된다.

Step 4. MN은 HA를 경유하여 수신한 C1을 자신의 개인키로 T1을 복호화하여, CN으로부터 직접 수신한 C2를 T1을 대칭키로 T2를 복호화한다. 그리고 C2, T1, T2를 H함수처리하여, 수신한 C3와 비교하여 HA를 경유해 온 메시지와 CN으로부터 온 메시지를 인증한다. 또한 T1과 T2를 가지고 Kbm을 계산한다.

$$T1 = D_{Kms}(C1)$$
$$T2 = D^{sym}_{T1}(C2)$$
$$C3 = H(C1, C2, T1, T2)$$
$$Kbm = SHA1(T1 \mid T2)$$

2) 2단계(최초 이후의 BU 전송시의 인증방식)

기존의 RR방식에서 바인딩 관리키는 식 (1)과 같이 CN이 생성하는 토큰들로만 만들어진다. 그러나 제안하는 방식은 최초 BU 전송시의 인증방식에서 안전한 바인딩 관리키인 Kbm을 이용하여, 이후 이어지는 BU 관리키 생성은 기존의 Internet draft[1]의 RR방식에서 안전한 Kbm을 이용하여 새로운 안전한 바인딩 관리키 K'bm을 생성해 낸다.

$$K0bm = SHA1(Kbm \mid homekeygentoken \mid careofkeygentoken) \quad (6)$$

Internet Draft[1] 상의 RR 인증 방식에서 키생성 토큰(keygen token)들이 평문으로 전송되어 토큰들만 알면 바인딩 관리키를 생성할 수 있지만 이 과정에서는 키생성 토큰들을 알고 있어도 Kbm이 노출되지 않는 한 K'bm을 생성해 낼 수 없게 된다. 따라서 최초 BU 인증 이후 이어지는 BU는 신속하면서도 안전한 인증을 할 수 있다.

2. 안전성 분석

암호화 프로토콜의 안전성은 그 암호학적 기반들의 안전성과 함께, 그 프로토콜에 대한 공격들을 통해 분석할 수 있다. 어떤 형태의 공격이 오랜 기간동안 성공하지 못한 프로토콜들은 그 공격에 대하여 잠정적으로 안전한 것으로 인정되며, 일부분이 공격당하면 그 공격의 방어를 위한 개선된 프로토콜이 제안되는 형식으로 순환된다. 따라서 새로운 프로토콜을 제안할 때에는 유사한 성격

을 가진 이전 프로토콜에 대한 공격방법을 기초로 하여, 가능한 공격들에 대한 분석으로 안전성에 대한 검증을 수행한다. 이 절에서는 제안한 BU 인증 메커니즘들을 이전의 프로토콜에 대한 공격 방법을 기초로 하여, 가능한 공격들에 대한 안전성을 분석하였다.

1) MITM(Man-In-The-Middle) 공격에 대한 안전성

경로변경(Redirect Attack)과 같이 패킷의 흐름을 변경할 수 있는 능력을 가진 공격자는 아주 쉽게 통신 세션(session) 중간에 자신을 끼워 넣는 MITM 공격을 할 수 있다. 이와 같은 공격이 가능하기 위해서 공격자는 MN과 CN 사이의 경로상에서 전송되는 패킷을 관찰하고 그 안에 담긴 데이터를 수정할 수 있어야만 한다.

IETF W/G에서 제안하는 RR방식에서는 만약 공격자가 MN-CN, HA-CN의 두 경로 모두 접근 가능할 경우 바인딩 관리키 Kbm을 생성할 수 있어 전송되는 패킷의 내용을 변경하여 MITM 공격을 수행할 수 있다.

그러나 제안하는 BU 인증 방식에서 공격자가 노드들의 경로 사이에서 패킷의 데이터 내용을 변경하여 자신을 다음과 같은 이유로 MITM 공격자로 위장하지 못한다.

첫째, 스타형 네트워크 구성 방식을 응용한 제안 방식에서는 MN이 HA를 경유하여 CN에게 전송하는 Y_{MN} 과 CN이 MN에게 전송하는 분배정보 Z_{CN} 을 이용하여 Kbm을 계산해야만 한다. 그러나 이러한 유한체상에서의 이산대수 문제는 RSA 알고리즘을 풀기위해 요구되는 인수분해의 어려움과 동치이다. 따라서 공격자가 자신을 노드의 경로사이에 MITM 공격자로 위장하는 것은 이산대수 문제를 해결하는 것만큼 어려운 일이다.

둘째, 공개키 시스템을 응용한 제안 방식에서는 BU 메시지 암호화에 사용하는 Kbm을 생성하기 위해 암호문 C2를 전송하는 송신자의 비밀키를 이용한다. 즉 송신자만이 해당 암호문을 생성할 수 있다는 묵시적인 인증을 제공한다. 따라서 사용자 A의 비밀키 T2를 알지 못하는 공격자는 위장하여 정당한 형태의 메시지를 전송할 수 없어 MITM 공격은 불가능하게 된다.

2) DoS(Denial Of Service) 공격에 대한 안전성

DoS(Denial of Service) 공격을 방어하기 위해서는 양 상대 노드가 각 상대 노드에 대한 확실한 인증을 확보하기 전에는 그 노드에 대한 어떠한 정보라도 생성(저장)하지 않음으로써 달성할 수 있다.

제안한 BU 인증 방식 모두다 IETF W/G에서 제안하는 RR 방식과 동일하게 경로상에서 두 상대 노드를 인증하여 바인딩 관리키인 Kmb을 생성하고, BU와 관련된 메시지를 전송하여 확실한 인증을 확보한 후에 CN의 캐쉬에 MN에 관한 바인딩을 생성하거나 수정함으로써 DoS 공격에 대한 위협을 최소화하였다. 또한 최초의 BU메시지 인증 후 MN의 이동이나 BU의 유효기간의 도래로 새로이 BU를 인증해야할 경우 바인딩 관리키인 Kbm을 양 상대노드가 가지고 있으므로 이것으로 MN이 새로이 BU 메시지를 전송하면서 통신하려는 CN이 이전에 MN과 통신한 CN이라는 것을 확신할 수 있기 때문에 CN이 새로운 바인딩 데이터를 캐쉬에 갱신하기 전에 확실히 상대노드에 대한 인증을 확보할 수 있다.

3) 이전의 세션키가 노출되는 경우의 안전성

암호 시스템에서 매 세션마다 동일한 키를 이용하여 암호문을 생성하는 경우에 한 세션의 키만 노출되면 이전의 모든 암호문이 공개되므로 매 세션마다 서로 다른 키를 사용하여 메시지를 암호화하는 것이 바람직하다.

제안하는 최초 BU 인증방식에서 생성된 바인딩 관리키인 Kbm은 안전하지만 이동 노드들의 자원을 많이 소모하므로 최초 생성된 키는 장기간(long term key)사용하고 제안한 2번째 단계의 인증방식에서 생성된 키는 기존에 확립한 Kbm을 이용하여 메시지의 노출 없이 바인딩을 위한 세션키(short term key)를 확립한다. 그리고 제안한 모든 메커니즘에서 비밀키를 생성하기 위하여 매 세션마다 서로 다른 랜덤수를 선택하여 암호화하여 전송하므로 이전의 세션키가 노출되더라도 현재의 키생성에 대한 안전성에는 영향이 없다. 또한 세션키 생성에 사용된 랜덤수가 노출되더라도 해당 세션 이외 다른 세션의 키생성에는 영향을 끼치지 못하고 안전하게 된다.

IV. 결론

본 논문에서는 Mobile IPv6 상에서 제공하는 BU 인증 방식을 분석하였고, 이 분석을 토대로 보다 강한 인증을 제공하는 메커니즘을 제안하였다.

기존의 인증 메커니즘들은 노드간 통신의 전 단계에 있어서 동일한 BU 인증 메커니즘을 사용함으로써 Internet draft 상의 인증 메커니즘의 경우 바인딩 관리 키(binding management key)를 생성하기 위해 메시지들이 평문으로 전송되기 때문에 MN-CN, HA-CN 두 경로 모두에 접근가능한 공격자라면 쉽게 바인딩 관리키를 생성하여 수동적, 능동적 공격을 할 수 있는 보안 특성과 취약성을 가지게 되어 악의를 가진 공격자에 의한 위협이 항상 존재하게 되었다.

제안한 BU 인증 메커니즘에서는 전체적으로 2단계의 BU 인증 과정을 거치도록 하여 바인딩 관리키의 노출을 최소화 하였다. 1단계는 상대노드에게 최초로 BU 인증 요구를 할 때 다소 계산량은 많지만 MN-CN, HA-CN 두 경로 모두에 접근가능한 공격자라 할지라도 RR 방식처럼 바인딩 관리키를 생성할 수 없는 보안성을 가지도록 하였고, 2단계는 이후 이어지는 BU 인증 요구에서는 1단계에서 협상된 공유키를 사용하여 보다 신속한 인증을 할 수 있도록 하였다. 제안한 BU 인증 메커니즘은 계산량이 Internet draft 상의 RR 방식의 인증 메커니즘 보다는 최초 BU 인증시에만 약간 더 복잡할 수 있으나, 그 이후는 안전한 보안성을 확보한 가운데 신속한 BU 인증을 유지한다.

본 논문에서는 모바일 노드들이 현재 제한된 자원을 가지고 있음을 전제하였다. 따라서 향후 이러한 문제들이 해결될 경우 보다 강력한 인증을 할 수 있는 프로토콜의 연구가 필요할 것이다.

참고문헌

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6.", draft-ietf-mobileip-ipv6-24 .txt, June 2003.

[2] Stephen Kent and Randall Atkinson, "IP Encapsulating Security Payload(ESP)." IETF RFC 2406, November 1998.

[3] 권용진, 박종서, 조성준, 현대 암호 이론, 인터비젼, pp 229-241, September 2001.

[4] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.