무선 오버레이 네트워크에서 Mobile IPv6를 위한 커버로스 기반의 안전한 바인딩 업데이트[1)]

정회윤○ 송세화 최형기
성균관대학교 정보통신공학부
{fatric, dreaminsh, hkchoi}@skku.edu

Kerberos based Secure Binding Update for Mobile IPv6 in Wireless Overlay Networks

Hoeyun Jeong○ Sehwa Song Hyoung-Kee Choi
School of Information and Communication Engineering, Sungkyunkwan University

요 약

Mobile IPv6에서 단말이 이동을 하게 되면 경로 최적화를 위한 바인딩 업데이트를 하게 된다. 안전한 바인딩 업데이트를 위해 RFC 3775에서 Return Routability가 제안 되었다. 그러나 Return Routability는 MN과 HA 사이에는 IPSec으로 Secure Path를 보장 받지만, MN과 CN 사이에는 바인딩 업데이트 과정에 공격자가 개입할 경우 다양한 공격에 노출될 수 있다. 이에 본 논문에서는 CN도 MN과 같이 HA와 Secure Channel을 보유한 이동 단말일 경우, 각 HA 사이에 커버로스 서버를 이용한 키 분배를 통해 바인딩 업데이트 메시지가 전달되는 전 구간에 걸쳐 안전한 경로를 확보하는 아키텍쳐를 제안한다.

1. 서 론

급속하게 발전한 인터넷 환경과 더불어 무선통신 기술의 발전과 다양한 단말기의 보급으로 인해 무선 인터넷 환경도 급진적으로 발전하고 있다. 이렇게 기하급수적으로 늘어나는 사용자 수로 인해 32비트 Internet Protocol version 4(IPv4)의 주소 사용률은 포화상태에 왔고 머지않아 고갈될 것으로 예상되고 있다[1]. 이에 Internet Engineering Task Force(IETF) 주도로 표준화가 진행되는 Internet Protocol version 6(IPv6)는 크게 늘어난 주소공간과 향상된 보안기능을 제공할 뿐 아니라 자동구성(auto configuration)과 이동성(mobility)을 제공함으로써 효율적인 네트워킹 환경을 구성할 수 있다[2].

인터넷 환경에서 단말은 접속된 네트워크로부터 유일한 주소를 부여 받는다. 이 고정된 주소를 패킷의 목적지 주소로 지정하여 통신을 한다. 그러나 이동 인터넷 환경에서 단말이 하나의 네트워크에서 다른 네트워크로 이동하는 경우 주소가 변경되어 서비스가 중단되므로 다시 연결을 시도해야 한다. 이와 같이 네트워크를 이동하면서 서비스를 사용할 때의 문제점을 해결하기 위해 이동 단말이 사용 중인 서비스를 계속 이용할 수 있도록 하기 위한 Mobile IPv6(MIPv6) 기술이 제안 되었다[3]. MIPv6는 HoA(Home Address)와 CoA(Care of Address)를 사용하여, 이동 단말이 다른 네트워크로 이동하여도 지속된 통신을 제공한다.

MIPv6에서 이동 단말을 Mobile Node(MN)이라 하고, MN과 통신하는 대상 단말을 Correspondent Node(CN)라 하며, MN이 이동전에 있던 네트워크의 라우터는 HA(Home Agent)라 한다. MIPv6에서는 MN이 새로운 네트워크로 이동하여도 HA를 거치지 않고 CN이 MN으로 직접 통신할 수 있는 경로 최적화(Route Optimization)를 지원하는데, MN은 자신의 이동을 CN에게 바인딩 업데이트를 통해 알려줘야 한다. 이 바인딩 업데이트 과정이 안전하지 못하면 악의적인 공격자에 의해 다양한 공격을 받을 수 있다. 따라서 안전한 바인딩 업데이트는 보안을 위해 꼭 필요하다.

본 논문에서는 MN 뿐만 아니라, CN도 고정된 서버가 아니라 HA를 통해 이동 중에도 통신을 지속하는 단말인 환경을 가정한다. 이 때, MN과 HA간에는 기존 MIPv6에서 지원하는 IPSec을 통하여 확보된 Secure Path를 사용하고, MN의 HA와 CN의 HA간에는 커버로스(Kerberos)[4]를 통해 신뢰관계를 확보하는 아키텍쳐를 제안한다. 이를 통해 MN과 CN간에 Secure Path Relay를 통해 안전하게 바인딩 업데이트를 진행할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 배경이 되는 Mobile IPv6, 커버로스를 설명한다, 그리고 관련 연구와 미흡한 점에 대해 3장에서 언급한다. 4장에서는 기존 MIPv6의 바인딩 업데이트의 보안 문제를 정리한다. 5장에서는 제안하는 아키텍쳐 및 바인딩 업데이트 절차를 설명한다. 6장에서 Security Analysis를 통해 기존의 제안에 비해 보안에 있어서 우수함을 제시한다. 7장의 결론으로 끝맺음한다.

1) 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
(IITA-2008-C1090-0801-0028)

2. 배 경

2.1 Mobile IPv6

MIPv6에서 MN은 위치와 상관없이 변하지 않는 Home-of Address(HoA)와 다른 네트워크로 이동했을 때 해당 네트워크에서 임시로 부여 받은 Care-of Address(CoA)를 갖는다[3]. MN이 새로은 네트워크로 이동해서 CoA를 부여 받게 되면, Home Agent(HA)에 이 주소를 등록해야 MN의 위치와 관계없이 HoA를 이용해 통신하던 다른 단말들의 계속된 통신이 가능하다. 홈 네트워크에 MN이 없을 때 도착된 메시지는 등록된 주소를 통해 HA가 전달하게 된다. 이 방식의 통신은 모든 메시지가 항상 HA를 거쳐야만 하므로 비효율적이다. MIPv6에서는 이 문제의 해결을 위해 HA와 더불어 통신 중이던 CN에게도 CoA를 알려서 HA를 거치지 않고 직접 통신할 수 있는 방법을 제공한다. 이렇게 HA와 CN에게 CoA를 알리는 과정을 바인딩 업데이트(BU)라고 한다. 안전한 BU인증을 위해 여러 제안이 있었으나 현재 RFC 3775에서는 MN과 CN사이의 두 가지 경로에 대한 인증을 바탕으로 하는 Return Routability(RR)을 채택하고 있다[3].

바인딩 업데이트과정에서 MN과 HA 사이의 경로는 IPSec ESP에 의해 인증(Authentication), 무결성(Integrity), 기밀성(Confidentiality) 서비스가 적용되어 안전하게 보호된다[3, 5]. 그러나 MN과 CN사이와 HA와 CN사이의 RR메시지는 평문으로 전달되어 완벽하게 보호되지 못한다[6]. 악의적인 공격자가 두 경로 모두 접속이 가능하므로 다양한 공격에 쉽게 노출될 수 있다.

2.2 커버로스

커버로스(Kerveros)는 MIT의 아테나 프로젝트의 일환으로 개발된 분산 환경에서 개체 인증 서비스를 제공하는 네트워크 인증 시스템이다[4]. 신뢰하는 제3의 서버가 서비스를 이용하려는 클라이언트의 사용자를 인증함으로 서버와 클라이언트의 신뢰관계가 형성 된다.

사용자가 처음 로그인할 때 클라이언트는 Key Distribution Center(KDC)에 Ticket Granting Ticket(TGT)요청 메시지를 암호화해서 보낸다. KDC는 정상적인 사용자로 인증되면, Ticket Granting Server(TGS)에 접근하여 TGT발급하고, 클라이언트와 TGS의 세션 키를 생성하여 전송한다. 이 메시지 또한 암호화되어 전송된다. 클라이언트는 TGS에 서비스 티켓의 발급 요청 메시지를 보낸다. 요청을 받은 TGS는 TGT를 인증하고 성공하면 클라이언트가 서버와 통신할 때 사용할 세션 키를 생성하고, 서비스 티켓과 함께 전송한다. 이렇게 하여 클라이언트는 세션 키와 서비스 티켓을 이용하여 서비스를 요청할 수 있다.

클라이언트가 TGS로 부터 서비스 티켓을 받을 때 서버와의 세션 키를 얻게 되므로, 신뢰하는 커버로스 서버로부터 두 단말(서버, 클라이언트)은 이 세션 키를 이용해 비밀 통신이 가능해지고 안전한 경로(Secure Path)를 확보할 수 있게 된다.

3. 관련연구

H.Fathi 등은 Wirelss Overay Network에서 PKI와 LR-AKE based RSA 등의 프로토콜을 사용한 보안 아키텍쳐를 제안하였다[7]. 제안된 방법은 기존의 MIPv6의 방법을 상당부분 변경하기 때문에 적용시키기 어렵다. MN과 CN의 HA간 PKI를 사용하여 보안 채널을 확보한다. 또한 MN과 HA간에는 LR-AKE based RSA라는 저자들이 만든 프로토콜을 통해 보안 채널을 확보한다. HA들간에 PKI를 해야 하기 때문에, 새로운 HA가 생기면, 이전 HA은 새로운 HA의 Public key를 미리 확보해야 한다. 그리고, MN은 향후 바인딩 업데이트에 사용될 키를 새롭게 갱신하는 장점이 있지만, 이미 MN과 HA사이에는 IPSec으로 보호되기 때문에 불필요한 갱신 프로토콜이 필요하다. J.M.Park 등은 MN과 HA간의 인증에 Ticket 기반의 AAA인증 방법을 제안하였다[8]. AAA 서버와 Ticket개념을 사용하여 HA와 MN의 바인딩 업데이트 및 인증에 대해 정의하고 있으나, MIPv6에 적용되지 않아, CN과의 통신에 대해서는 고려되지 않았다.

4. 바인딩 업데이트의 Security Problem

RFC 3775에서 MN과 CN간의 안전한 바인딩 업데이트를 Return Routability를 통해 지원하고 있다[3]. Return Routability는 CN이 MN이 가진 두 개의 IP주소(HoA, CoA)가 모두 도달 가능한지 확인해보는 것을 목적으로 한다. 그래서 CN은 HoA, CoA로 키 생성을 위한 두 개의 token을 전송하고, MN은 두 개의 token을 모아서 한 개의 키로 만든 후, 이 키로 메시지 인증코드(MAC)을 붙여 바인딩 업데이트를 하게 된다. 이 과정에서 공격자가 개입할 경우, 표 1과 같은 공격에 노출될 수 있다.

표 1. 바인딩 업데이트시 공격유형

공격이름	내 용
Session Hijacking	CN에서 MN으로 전송되어야 할 데이터를 공격자가 가로챌 수 있다.
Flooding Attack	불특정 IP주소로 다수의 데이터를 redirect시킨다.
Movement Halting Attack	MN이 새로운 CoA를 획득하여 바인딩 업데이트를 하더라도, 다시 이전 CoA로 거짓 Binding을 시킨다.
Denial of Service Attack	CN에게 많은 HoTI, CoTI 전송을 통해 process / memory를 소모시킨다.

이러한 공격은 이동 중에 지속적인 통신에 큰 위협이

될 수 있으며, 상위 Layer에서 암호화통신이 되지 않으면 중요한 정보가 공격자에게 전송될 소지가 있다. 이러한 문제점은 MN과 CN간에 아무런 Secure Channel이 존재하지 않기 때문에 발생한다. 특히, MN과 CN간에 Pre-Share Key가 존재하지 않기 때문에, MN-HA처럼 IPSec으로 보호하기에 무리가 따른다. 본 논문에서는 CN이 MN처럼 HA와 Secure Channel을 보유한 이동단말일 경우에, 위에서 제시한 문제점을 해결할 수 있는 아키텍쳐와, Secure Channel을 확보하는 Scheme을 제시하고자 한다.

5. 제안하는 아키텍쳐 및 바인딩 업데이트

다양한 무선 단말기 보급과 무선 인터넷 서비스로 인해 통신 대상마저 고정된 서버가 아닌 무선 단말인 경우도 발생하게 되었다. 이러한 환경에서의 바인딩 업데이트 과정은 MN의 HA(HA_{MN})와 CN의 HA(HA_{CN})사이의 경로가 추가 되었다. 보안정책은 이러한 모든 경로에 적용할 수 있는 안전하고 효율적인 방법 이어야 한다. 본 장에서는 무선 단말끼리의 통신에서 바인딩 업데이트시 안전한 키를 확립하기 위한 secure path를 정의한다. 그림 1에서 MN과 CN은 IPSec Tunnel을 이용해 각 HA와 신뢰할 수 있는 구간을 확보하고, 신뢰관계가 없는 각 HA 끼리는 신뢰할 수 있는 제 3의 서버인 커버로스 서버를 통해 신뢰구간을 확보한다. 이로써, 최종 단말에서 최종 단말까지 전 구간의 Secure Channel을 확보할 수 있게 된다.

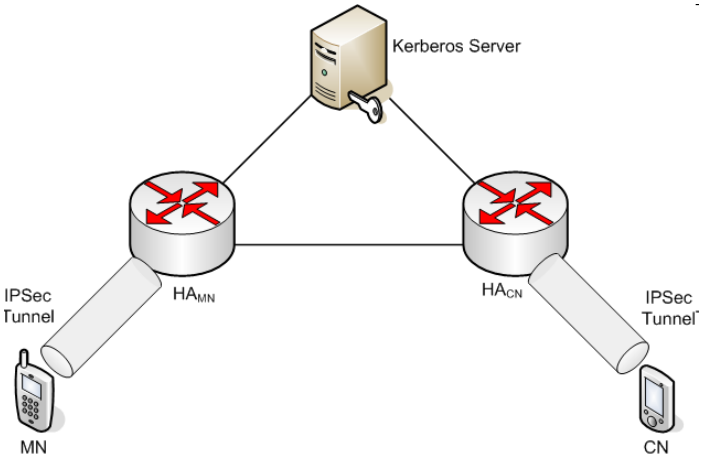

그림 1. Kerberos 기반의 아키텍쳐

각 단의 HA는 커버로스 서버와 이미 신뢰관계를 갖고 있다고 가정한다. HA를 지원하는 Service Provider간의 협약을 통해 여러 방법을 통해 신뢰관계를 확립할 수 있지만, 커버로스를 통하게 되면, 전체적인 HA들의 수가 변하게 되어도, HA에 추가적인 역할 없이, 커버로스 서버가 처리를 해주게 되어, 전체적인 확장성(Scalability)이 증대될 수 있다. 그리고 각 MN은 기존 RFC 3775[3]에 의거 HA와 IPSec을 통해 안전하게 데이터를 안전하게 주고받을 수 있다.

핸드오버(Handover) 절차를 포함한 전체적인 흐름은 그림 2와 같고, 절차는 다음과 같다.

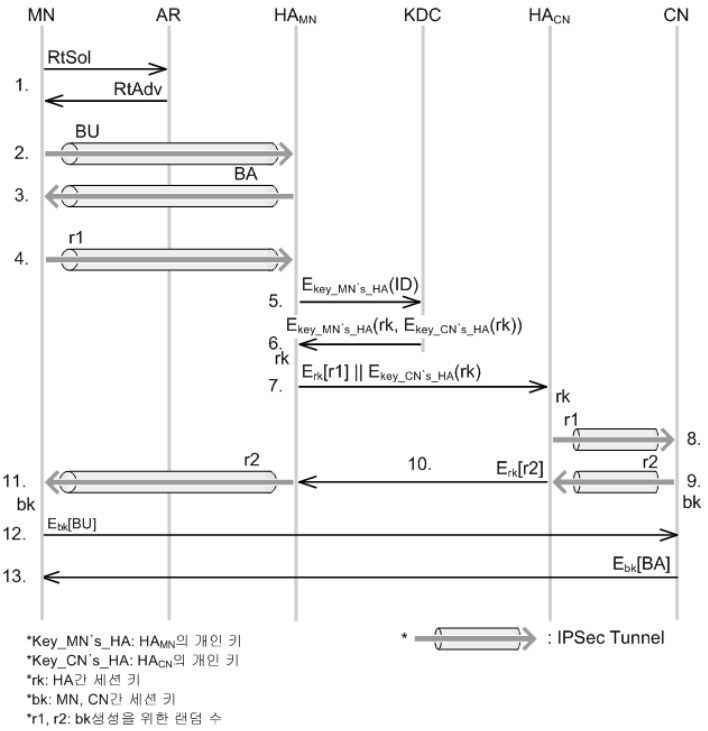

그림 2 제안하는 안전한 Handover Procedure

① MN ↔ AR : MN은 이동을 인식한다.

② MN → HA_{MN} : 이동을 인식한 MN은 새로운 CoA를 알리기 위해 HA_{MN}으로 IPSec Tunnel을 이용해 BU메시지를 안전하게 보낸다.

③ HA_{MN} → MN : BU메시지의 인증이 정상적이면 BA메시지 역시 IPSec을 이용해 안전하게 보낸다.

④ MN → HA_{MN}: CN에게 보낼 BU메시지를 보호하기 위해 MN과 CN간의 암호화키가 필요하다. 이 키를 생성하기 위해 $r1$(Random Number)을 생성해서 보낸다.

⑤ HA_{MN} → KDC : HA_{MN}과 HA_{CN}은 아직 신뢰관계가 형성 되지 않아 각 HA와 신뢰관계가 있는 제3의 서버(KDC)로부터 인증을 받고, 서로의 신뢰관계를 형성한다. 여기에 필요한 인증을 받기위해 (식 1)과 같은 메시지를 KDC에 보내 인증을 요구한다. (식 1)은 HA_{MN}의 개인 키 ($Key\_MN's\_HA$)로 자신의 ID를 암호화한다.

$$E_{Key\_MN's\_HA}(ID) \quad \text{(식 1)}$$

⑥ KDC → HA_{MN} : KDC는 미리 등록된 정보로 ID를 인증하고, HA_{MN}과 HA_{CN}간의 비밀통신에 필요한 키인 rk을 생성하고, (식 2)를 통해 세션 키(rk)를 포함하는 Ticket을 생성하여 HA_{MN}에게 보낸다.

$$E_{Key\_MN's\_HA}(rk, E_{Key\_CN's\_HA}(rk)) \quad \text{(식 2)}$$

⑦ HA_{MN} → HA_{CN}: HA_{MN}은 KDC로부터 받은 암호화된 세션 키(rk)와 $r1$을 (식 3)과 같은 메시지로 보낸다.

$$E_{rk}(r1) \| E_{Key\_CN's\_HA}(rk) \quad \text{(식 3)}$$

⑧ HA_{CN} → CN: HA_{CN}은 자신의 개인 키($Key\_CN's\_HA$)로 해독해서 세션 키(rk)를 알아내고, 이것으로 HA_{MN}과 키를 공유하게 된다. 이 세션 키를 이용해서 $r1$을 알아낸다. 이렇게 확보한 $r1$은 IPSec으로 CN에게 전달한다.

⑨ CN → HA_{CN} : CN은 $r2$(Random number)를 생성하고 IPSec을 이용해 HA_{CN}에게 보낸다. 이때 받은 $r1$과의 조합으로 (식 4)와 같이 MN이 생성한 $r1$과 CN이 생성한 $r2$를 해쉬함수를 통해 BU를 암호화 할 암호화 키(bk)를 생성한다.

$$bk = H(r1 \| r2) \quad \text{(식 4)}$$

⑩ HA_{CN} → HA_{MN} : HA_{CN}은 ⑥에서 확보한 세션 키(rk)를 이용해 $r2$를 (식 5)와 같이 암호화해서 전송한다.

$$E_{rk}(r2) \quad \text{(식 5)}$$

⑪ HA_{MN} → MN : 암호화된 $r2$를 rk로 풀고 IPSec으로 MN에게 전송한다.

⑫ MN → CN : $r2$를 받은 MN은 자신이 보냈던 $r1$과의 조합으로 ⑨와 같은 방법으로 bk를 생성한다. 생성된 bk를 이용해 BU메시지를 (식 6)과 같이 암호화해서 CN에게 전송한다.

$$E_{bk}(BU) \quad \text{(식 6)}$$

⑬ CN → MN : BU메시지를 인증하고 BA메시지를 bk를 이용해 (식 7)과 같이 암호화해서 전송한다.

$$E_{bk}(BA) \quad \text{(식 7)}$$

이동된 MN은 IPSec을 이용해 자신의 HA와 안전하게 바인딩 업데이트를 하고, CN과의 바인딩 업데이트를 위해서 Secure Path를 확보하기 위한 키 bk를 확보한다. 이를 위해 랜덤 수 $r1$과 $r2$를 주고받는데 이 과정에서의 보안은 커버로스 서버를 통해 얻은 rk을 이용해 보장 받는다. 이로써 전체 과정의 전 구간에 Secure Path를 확보할 수 있고 외부 공격으로부터 안전하게 바인딩 업데이트를 실시할 수 있다.

6. Security Analysis

제안된 아키텍쳐 및 핸드오버시 바인딩 업데이트방법을 통해 기존의 MIPv6에서의 보안상 문제점을 해소할 수 있다. 우선 CN역시 MN과 동일한 형태의 무선단말일 때, Secure Path를 확장하였다. 즉 MN-HA구간만 보호되고 있었지만, 바인딩 업데이트 메시지가 전달되는 전 구간에 걸쳐 암호화하여 안전하게 전달된다. 특히 유사한 HA와 HA간 커버로스 서버를 통한 키 분배는 HA간 PKI를 할 경우보다 연산 량을 줄여줄 수 있다. 다음으로 CN은 바인딩 업데이트시 유지해야할 정보량을 줄이게 된다. 이를 통해 기존 방법에서 발생할 수 있는 Denial of Service(DoS)공격에 저항성을 가진다.

7. 결론

이동성 있는 단말이 증가함에 따라 Mobile IPv6의 중요성도 증대하고 있다. 본 논문에서는 통신하는 양 단이 Mobile IPv6를 사용하는 Wireless Overlay Network에서의 안전한 바인딩 업데이트를 위한 커버로스를 사용하는 아키텍쳐를 제안하였다. 통신하는 양 단이 HA를 보유하는 상황에서 HA들과 Secure Path가 있는 서버를 통해 HA들은 티켓을 통해 Secure Path를 획득한다. 이를 통해 네트워크에 HA가 증가 하더라도 각 HA는 KDC를 이용해 간단하게 키를 공유할 수 있다. 또한 이를 통해 MN과 CN이 서로 키를 안전하게 공유하는 Flow를 제시하였다. 기존에 제안된 방법에 비해 기존 Mobile IPv6의 변화가 적으면서, MN과 CN간에 안전한 경로를 확장한다. MN과 CN간에는 처음 한번 키를 확립하게 되면, 그 이후에는 해당 키를 이용한 암호화를 통해 HA들을 거치지 않고, 빠른 바인딩 업데이트를 지원할 수 있다.

참고문헌

[1] G. Huston, "IPv4 Exhaustion Nears “, Internet Society, The ISP Column, July [2007]

[2] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December [1998]

[3] D. Johnson, C. Perkinsm, J. Arkko, "Mobility Support in IPv6", RFC 3775, June [2004]

[4] J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September [1993]

[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November [1998]

[6] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December [2005]

[7] H. Fathi, S. H. Shin, K. Kobara, S. S. Chakraborty, H. Imai, R. Prasad, "Leakage-Resilient Security Architecture for Mobile IPv6 in Wiress Overlay Networks", IEEE journal on selected areas in communications, Vol.23 November [2005]

[8] J. M. Park, E. H. Bae, H. J. Pyeon, K. J. Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network", LECTURE NOTES IN COMPUTER SCIENCE, Vol.- No.2668, [2003]