Secure-FMIPv6: ID 기반 암호시스템에 기반한 안전한 Fast 핸드오버 연구*

이우찬*, 정수진*, 이종혁*, 한영주*, 정태명**
*성균관대학교 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail : {wclee,sjjung,jhlee,yjhan}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Secure-FMIPv6: A Study on Secure Fast Handover based on ID-based Cryptosystem*

Woo-Chan Lee*, Soo-Jin Jung*, Jong-Hyouk Lee*, Young-Ju Han*,
Tai-Myoung Chung**
*Dept. of Computer Engineering, Sungkyunkwan University
**School of Information and Communication Engineering, Sungkyunkwan University

요 약

MIPv6 는 MN(Mobile Node)가 자신의 홈 네트워크를 벗어나 외부 네트워크로 이동하여도 다른 노드들과 끊김 없이 지속적인 통신을 할 수 있게 해주는 인터넷 프로토콜이다. MN 은 외부네트워크로 이동 후 HA(Home Agent) 및 CN(Correspondent Node)로 핸드오버(Handover) 동작의 수행하며 이로 인한 지연이 발생하게 된다. 이러한 지연을 줄이기 위한 대책으로 Fast 핸드오버가 등장하였다. Fast 핸드오버 과정에서 MN 은 이동하려는 서브넷의 라우터(New Access Router: NAR)로의 전환을 위하여 현재 연결된 AR 과 미리 정보를 주고 받게 되고, 이동이 발생한 후에 NAR 과의 핸드오버 지연시간이 감소하게 된다. 반면 공격자가 flooding 을 통해 MN 에게 DoS(Denial of Service) 공격을 가하여 MN 을 다운시킨 후, MN 으로 위장하여 데이터를 가로채는 취약점이 존재한다. 본 논문에서는 위의 취약점을 보완하기 위하여 핸드오버 과정에서 주고받는 메세지에 대한 기밀성 및 노드 인증을 제공하는 ID 기반 암호시스템에 기반한 안전한 Fast 핸드오버 방식을 제안한다. 제안하는 모델은 메시지의 암호화와 노드 인증을 통해 무결성 및 기밀성을 보장하고 Traditional PKI 시스템에 비해 공개키 인증시간을 단축하는 이점을 가질 것으로 기대된다.

1 서론

MIPv6(Mobile IPv6)[1]는 MN(Mobile Node)가 자신의 홈 네트워크를 벗어나 외부 네트워크로 이동하여도 다른 노드들과 끊김 없이 지속적인 통신을 할 수 있게 해주는 인터넷 프로토콜이다. MN 은 새로운 서브넷에서 통신이 가능하게 하기 위해 NewCoA(Care-of-Address)를 생성하고, BU(Binding Updat)를 통해 HA(Home Agent) 및 CN(Correspondent Node)에 등록한다. 그러나 이러한 핸드오버 과정에서 통신 지연이 발생하며, 이러한 지연을 감소시키기 위한 방법으로 Fast 핸드오버 방식이 표준화 되었다[2].

Fast 핸드오버 방식은 MN 이 새로운 서브넷으로 이동을 한 뒤 BU 과정을 수행함에 따라 생기는 지연을 줄이기 위해, MN 이 이동하기 전에 미리 이동하려는 새로운 서브넷의 CoA 를 생성한 후에 이동을 하는 것이다.

이때 MN 이 이동하려는 서브넷의 라우터 정보가 공격자에게 노출되어 공격자가 MN 으로 위장할 수

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성・지원사업의 연구결과로 수행되었음.

있는 보안상 취약점이 존재한다. 따라서 본 논문에서는 위장 공격을 막기 위하여 메시지에 대한 암호화와 메시지를 주고받는 노드들에 대한 인증을 제공하는 ID 기반 암호시스템에 기반한 안전한 Fast 핸드오버 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 Fast 핸드오버의 동작 및 보안상 취약점을 설명한다. 3 장에서 ID 기반 암호시스템의 특징 및 동작과정을 설명하며, Secure-FMIPv6 프로토콜을 제안한다. 4 장에서 제안된 기법에 대한 분석을 하며, 끝으로 5 장에서 결론을 맺는다.

2 관련 연구

2.1 FMIPv6

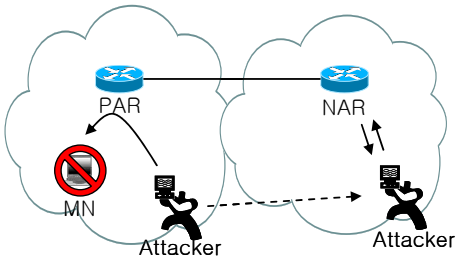
FMIPv6(Fast Mobile IPv6)의 동작은 predictive 모드와 reactive 모드로 구분할 수 있다. 두 모드의 차이는 PAR 이 MN 이 이동하려는 NAR 에 대한 정보를 얻을 수 있는 시점으로, 전자는 NAR 의 정보를 2 계층 핸드오버가 수행되기 이전에 알 수 있고, 후자는 2 계층 핸드오버가 일어난 후에 NAR 를 알 수 있다[7].

FMIPv6 의 predictive 모드의 각 메시지들에 대한 설명은 다음과 같다.

1) RtSolPr/PrRtAdv: MN 이 주변의 라우터 정보를 알아내기 위해 RtSolPr(Router Solicitation for Proxy)를 PAR 에 보내고, PAR 은 MN 에게 하나 이상의 라우터 정보를 담은 PrRtAdv(Proxy Router Advertisement)를 보낸다.
2) FBU: 핸드오버를 요청하는 메시지로 MN 이 PAR 에게 FBU(Fast Binding Update)를 보낸다.
3) HI/HAck: 두 라우터간의 정보 교환용 메시지로 PAR 이 NAR 에게 HI(Handover Initiate)를 보내고 HAck(Handover Acknowledgement)를 받는다.
4) FBack: FBU 메세지에 대한 확인 메시지로 PAR 이 MN 과 NAR 에게 FBack(Fast Binding Acknowledgement)를 보낸다.
5) FNA: 핸드오버 완료에 대한 메시지로 MN 이 NAR 에게 FNA(Fast Neighbor Advertisement)를 보낸다.

2.2 보안 위협

MN 이 CN 과 통신을 하고 있고, 공격자가 통신 채널을 도청하고 있다고 가정하자. 이때 MN 이 PAR 과의 Fast 핸드오버 과정을 수행하게 되면, 공격자는 BU 메세지로부터 MN, CN, PAR, 그리고 NAR 의 주소 등 공격에 유용한 정보를 얻을 수 있다. 공격자는 (그림 2)과 같이 flooding 을 통해 MN 에게 DoS(Denial of Service) 공격을 가하여 MN 의 동작을 일시적으로 다운시키고, MN 과 CN 의 통신은 지연되거나 중단되게 된다. PAR 은 MN 의 다운 상태를 통신이 끊긴 것으로 판단하고 CN 으로부터 전송되는 데이터를 MN 이 Fast



(그림 1) Attacking and Masquerading MN by Attacker

핸드오버를 통해 선택한 NAR 에게 보내고, NAR 은 PAR 로부터 받은 데이터를 보관한다. 이때 공격자는 자신을 MN 으로 위장하여 NAR 에게 FNA 를 전송하여 연결을 맺으며, NAR 이 보관하고 있던 데이터를 전송 받는다. 이와 같은 과정을 통해 공격자는 MN 의 데이터를 얻을 수 있게 된다.

2.3 보안 요구 사항

BU 메시지에는 MN, PAR, NAR 의 IP 주소가 포함되어 있다. 따라서 BU 메시지에 기밀성을 제공하며 메시지를 전송하는 각 노드에 대해 인증을 수행하기 위한 암호시스템이 요구된다.

관용키 방식은 암호화와 복호화에 동일한 키를 사용하며, 키의 길이가 64bits~256bits 로 속도가 빠르다. 반면, 안전한 키 분배와 n 통신노드와 통신시 n(n-1)개의 키를 관리해야 하는 문제가 있다[5].

Traditional PKI(Public Key Infrastructure)는 공개키를 관리하는 계층적인 CA(Certificate Authority)를 도입하여 공개키를 분배하고 인증하는 관리상의 오버헤드가 증가하였다[5][6]. 따라서 키 인증시간을 줄이기 위한 암호시스템의 적용이 필요하다.

3 Secure-FMIPv6 프로토콜

본 논문에서는 앞 절에서 기술한 FMIPv6 의 보안 요구 사항을 수용하기 위해서 키 분배 및 관리의 측면에서 뛰어난 효율성을 보이는 ID 기반 암호시스템을 적용한 Secure-FMIPv6 프로토콜을 제안한다.

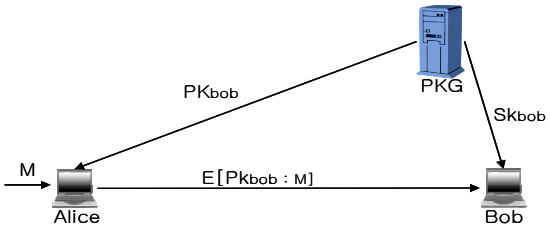
A. ID 기반 암호시스템(ID-based Cryptosystem)

ID 기반 암호시스템은 1984 년 Shamir 에 의해 처음 제안되었다[3]. 이 암호에서 ID 는 객체를 인증할 수 있는 유일한 식별자를 의미한다. 이러한 객체의 ID 를 기반으로 생성한 공개키로 사용하여 암호화 및 서명 작업을 수행하게 된다.

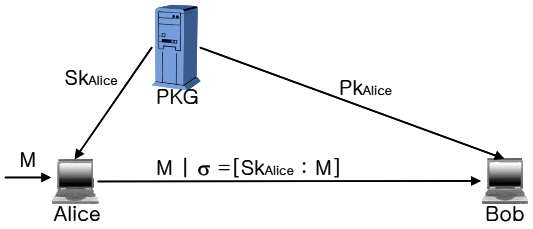
(그림 2)과 (그림 3)는 ID 기반 암호화와 서명의 기본적인 구조로써, 통신을 하는 두 사용자와 각 사용자의 ID 를 사용해서 키를 생성해주는 신뢰할만한 제삼자인 PKG(Private Key Generator)가 존재한다. 암호화와 서명은 각각 다음의 과정을 수행한다[3][4].

1) ID-based Encryption

- Setup: PKG 는 사용자에 대해 사용자의 ID 로부터 공개키(Pk)와 개인키(Sk)를 생성한다.



(그림 2) ID-based Encryption Overview



(그림 3) ID-based Signature Overview

- Private Key Extraction: 사용자는 자신의 ID 를 통해 PKG 에 인증을 한 뒤 개인키를 얻는다.
- Encryption: 상대방의 ID 와 공개키를 사용하여 원문 메시지를 암호화한다.
- Decryption: 받은 암호문을 개인키로 복호화하여 원문 메시지를 얻는다.

2) ID-based Signature

- Setup: PKG 는 사용자에 대해 사용자의 ID 로부터 공개키와 개인키를 생성한다.
- Private Key Extraction: 사용자는 자신의 ID 를 통해 PKG 에 인증을 한 뒤 개인키를 얻는다.
- Signature Generation: 자신의 개인키를 사용하여 메시지에 대한 서명 σ 을 생성한다.
- Signature Verification: 메시지와 서명 σ 을 받은 후, 상대방의 공개키를 사용하여 σ 을 복호화하고 메시지와 비교한다.

B. Secure-FMIPv6 프로토콜의 개요

Secure-FMIPv6 프로토콜은 ID 선정과 Secure Fast Handover 메커니즘으로 구성된다.

1) ID 선정

네트워크 환경에서 노드의 ID 로는 IP 주소나 MAC 주소 등을 생각해 볼 수 있다. 제안하는 Secure-FMIPv6 프로토콜에서 각 노드의 ID 는 다음과 같다.

- MN 의 ID

  MN 은 영구적으로 변하지 않는 주소인 HoA(Home Address)와 이동에 따라 변하는 CoA(Care of Address)를 가진다. 여기서 MN 의 ID 는 HoA 로 정한다. 만약 CoA 를 ID 로 정하면 MN 이 이동할 때마다 PKG 는 새로운 CoA 에 대해 새로운 공개키와 개인키를 생성해야 하는 부담을 가지게 되므로 고정 주소인 HoA 를 선택하였다.

- AR 의 ID

  AR 은 자신이 연결된 네트워크의 수에 따라 여러 IP 주소를 가지게 된다. 따라서 MN 에 의해 인식되는 ID 는 MN 의 CoA 의 prefix 에 해당하는 AR 의 IP 주소로 정한다.

Secure-FMIPv6 는 기존의 FMIPv6 에 키 생성을 담당하는 신뢰할만한 제 삼자인 PKG 를 추가한 구조이다. PKG 는 MN, PAR, 그리고 NAR 의 ID 를 기반으로 키를 생성하고 각 인터페이스에 개인키를 분배하며, 노드의 요청에 따른 공개키를 분배하는 역할을 한다.

2) Secure Fast Handover 구조 및 메커니즘

Secure Fast Handover 메커니즘은 인증을 위한 정보를 생성하는 과정과 메시지와 인증 정보를 암호화하는 과정으로 나눌 수 있다.

- 인증 정보 생성

  제안하는 Secure-FMIPv6 에서의 인증은 노드 인증으로써 메시지를 보내온 상대방이 정당한 사용자임을 인증한다. 따라서 노드의 ID 를 자신의 개인키로 암호화 하여 인증 정보를 생성한다.

$$\sigma = E[H(Sk_X : X_{ID})]$$

  위의 식은 제안하는 인증 정보 생성 알고리즘이며, X 의 ID 를 X 의 개인키로 암호화하여 인증 정보를 생성한다.

  (그림 4)에서 각 노드의 인증 정보는 다음과 같다.

  $\sigma 1 = E[H(Sk_{MN} : MN_{ID})]$: MN 의 인증 정보
  $\sigma 2 = E[H(Sk_{PAR} : PAR_{ID})]$: PAR 의 인증 정보
  $\sigma 3 = E[H(Sk_{NAR} : NAR_{ID})]$: NAR 의 인증 정보

- 메시지 및 인증 정보 암호화

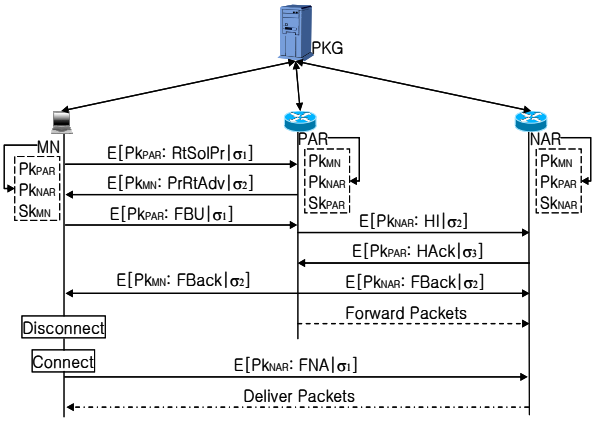
  Secure-FMIPv6 동작은 기본적인 FMIPv6 동작에 해당하는 메시지들을 인증 정보와 함께 암호화하는 과정을 추가하였다. 송신자는 앞 절에서 생성한 인증 정보와 메시지를 수신자의 공개키로 암호화한 후 메시지를 전송하게 된다.

$$E[Pk_X : M|\sigma]$$

  위의 식은 제안하는 암호화 알고리즘이며, X 의 공개키 Pk_X 로 메시지 M 과 인증정보 σ 를 암호화하는 것을 의미한다.

Secure-FMIPv6 의 일반적인 메시지 처리 절차는 다음과 같다.

① 송신자는 자신의 ID 로 PKG 에 인증하고 개인키를 획득한다.



(그림 4) Secure-FMIPv6 Process

② 획득한 개인키로 자신의 ID 를 암호화하여 인증 정보를 생성한다.
③ 송신자는 수신자의 ID 에 해당하는 공개키를 PKG 로부터 얻는다.
④ 수신자의 공개키로 보내고자 하는 메시지와 위에서 생성한 인증 정보를 암호화 한 후, 수신자에게 전송한다.
⑤ 수신자는 자신의 ID 에 해당하는 개인키를 PKG 로부터 획득한다.
⑥ 획득한 개인키로 수신한 메시지를 복호화하여 원문 메시지와 인증 정보를 획득한다.
⑦ 송신자의 ID 에 해당하는 공개키를 PKG 로부터 얻는다.
⑧ 송신자의 공개키로 인증 정보를 복호화하고 얻은 정보를 송신자의 ID 와 비교하여 사용자 인증을 수행한다.

4 성능평가

Traditional PKI 시스템이 CA 를 통한 3 단계 공개키 인증을 하며, 공개키 인증서 생성에 사용하는 알고리즘으로 RSA-SHA1 를 사용한다고 할 때, 제안한 Secure-FMIPv6 프로토콜에 적용한 ID 기반 암호시스템의 키 인증시간 및 CA 및 PKG 와의 통신횟수는 (표 1)과 같다.

(표 1) Comparison between Tradition PKI and ID-based PKI

	Traditional PKI	ID-based PKI
Key verification	4.784ms	0ms
Numbers of communication with CA or PKG	6 회	2 회

Traditional PKI 시스템의 경우 상대 노드의 공개키에 대한 인증을 위해서는 상위 CA 에 대한 인증이 전제되어야 하므로, 매 핸드오버 시 총 3 번의 인증서에 대한 인증이 필요하다. 하나의 인증서에 대한 인증시간은 4.784ms 이며, 3 단계의 인증에 걸리는 시간은 14.352ms 이다[8].

반면 제안한 Secure-FMIPv6 프로토콜은 ID 정보를 사용하여 PKG 로부터 상대 노드의 공개키를 분배받기 때문에, 공개키에 대한 인증과정을 거치지 않는다. 따라서 공개키의 인증시간을 단축하였으며, PKG 와 두 번의 통신으로 상대 노드의 공개키를 얻을 수 있게 되었다.

5 결론

본 논문에서는 Mobile IP 환경에서 핸드오버시의 지연을 감소시키기 위해 표준인 Fast 핸드오버 동작이 가지고 있는 보안 취약점에 대해 살펴보고, 취약점을 보완하기 위해서 ID 기반 암호시스템을 적용한 Secure-FMIPv6 프로토콜을 제안하였다.

이 프로토콜은 Fast 핸드오버시 주고 받는 메시지에 대해 암호화를 수행하여 메시지의 기밀성을 유지하고, 각 노드의 ID 를 인증정보로 사용하여 노드 인증을 수행함으로써 보안 요구사항을 만족시켰다.

그러나 메시지의 암호화와 인증 정보 생성으로 FMIPv6 의 오버헤드 증가가 발생한다.

따라서, 향후에는 본 프로토콜의 보안 강도는 유지하면서 오버헤드를 감소시킬 수 있도록 메커니즘 개선에 대하여 연구할 것이다.

참고문헌

[1] D. Johnson, C. Perkins and J. Arkko, “Mobility Support in IPv6”, RFC3775, June 2004.
[2] R. Koodi, “Fast Handovers for Mobile IPv6”, RFC 4068, July 2005.
[3] A. Shamir, “Identity-based Cryptosystems and Signature Schemes”, Proceedings of CRYPTO’84, LNCS 196, pp.27-53, Springer-Verlag, 1984.
[4] Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo, “A Survey of Identity-Based Cryptography”, AUUG 2004.
[5] A. Menezes, P. van Oorschot and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1997.
[6] Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, John Wiley & Sons, Inc., 1996.
[7] 박재홍, “Mobile IP 적용 기술”, Telecommunication Review, 제 14 권 5 호, October 2004.
[8] Crpyto++, “http://www.eskimo.com/~weidai/benchmarks.html”