

마이크로 및 피코 셀 환경을 위한 인증된 바인딩 갱신 프로토콜

구중숙*, 구중두**, 이기성**
*경기대학교 정보보호학과
**호원대학교 컴퓨터게임학부
e-mail:ygslee@howon.ac.kr

Authenticated Binding Update Protocol for Micro and Pico Cell Environments

Jung-Sook Koo*, Jung-Doo Koo**, Gi-Sung Lee**
*Dept. of Information Security, Kyonggi University
**School of Computer Game, Howon University.

요 약

본 논문에서 마이크로 및 피코 셀 환경에 적합한 인증된 바인딩 업데이트 프로토콜을 제안한다. 제안하는 프로토콜은 CGA (Cryptographically Generated Address) 기반의 티켓 방식을 이용한다. 이 방식은 호스트의 공개키와 서브넷 프리픽스를 이용하여 생성한다. 또한 초기통신 시에 대응노드는 이동노드에게 홈 에이전트를 통한 티켓을 발행한다. 이는 이동노드와 대응노드 간에 직접 바인딩 갱신을 할 수 있도록 도와준다. 또한 대응노드는 티켓 확인을 통한 이동노드를 인증하고 바인딩 업데이트를 안전하게 수행한다. 몇 가지 공격 시나리오를 통한 프로토콜의 안전성을 분석한다. 마지막으로 결론 및 향후 연구 방향에 대해서 제시한다.

1. 서론

모바일 IPv6[1]에서 이동노드가 홈 링크 또는 홈 네트워크에서 외부 링크에 존재하는 다른 노드와 통신도중 통신노드와 다른 외부링크로 이동했을 경우 이동노드는 홈 에이전트 및 기존에 통신하고 있는 대응노드와 바인딩 갱신 과정을 반드시 수행해야 한다. 그렇지 않을 경우 기존에 통신하고 있는 노드와의 연결이 끊어진다. 특히, 공항이나 터미널과 같은 곳에서는 핸드오프가 빈번하게 발생한다. 이런 빈번한 핸드오프는 통신 노드 사이에서 전송되는 패킷 손실 및 공격자로부터 많은 공격 위협에 노출될 수 있다. 따라서 본 논문에서는 마이크로 또는 피코 셀 환경과 같이 핸드오프가 빈번하게 일어나는 환경에 적합한 바인딩 갱신 프로토콜을 제안한다.

이 프로토콜은 기존의 주소 생성 방식과 달리 CGA (Cryptographically Generated Address)[2] 기법을 이용하여 주소를 생성한다. 이는 여러 공격자로부터

각 노드를 인증하기 위함이다. CGA는 통신 노드의 IPv6주소와 공개키를 이용해서 64비트의 인터페이스 식별자를 이용하여 생성되는데 최종적으로 해쉬 함수를 통해 계산된다. 또한 제안하는 프로토콜에서는 CN에 의해 생성되는 티켓을 이용하는데 이는 MN에서 핸드오프가 일어났을 경우 대응노드가 HA와 다시 키 교환 프로토콜을 수행하지 않고 MN을 인증하기 위함이다. 인증방법은 MN이 보낸 티켓을 자신의 개인키로 복호화하여 티켓 안의 세션키를 통해 MN이 전송한 MAC값을 확인하여 메시지의 오류나 사용자를 확인한다. 더욱이 티켓은 초기 통신 시에 수행한 절차를 모두 수행하지 않고도 각 노드를 인증할 수 있어 기존의 방식[1,3,4]과 달리 상호인증을 위한 최소한의 메시지 수인 두 번으로 처리가 가능하다. 또한 티켓은 HA가 동작할 수 없는 환경에서도 바인딩 갱신을 수행할 수 있다는 장점을 가진다. 본 논문의 나머지 구성은 아래와 같다. 2장에서는

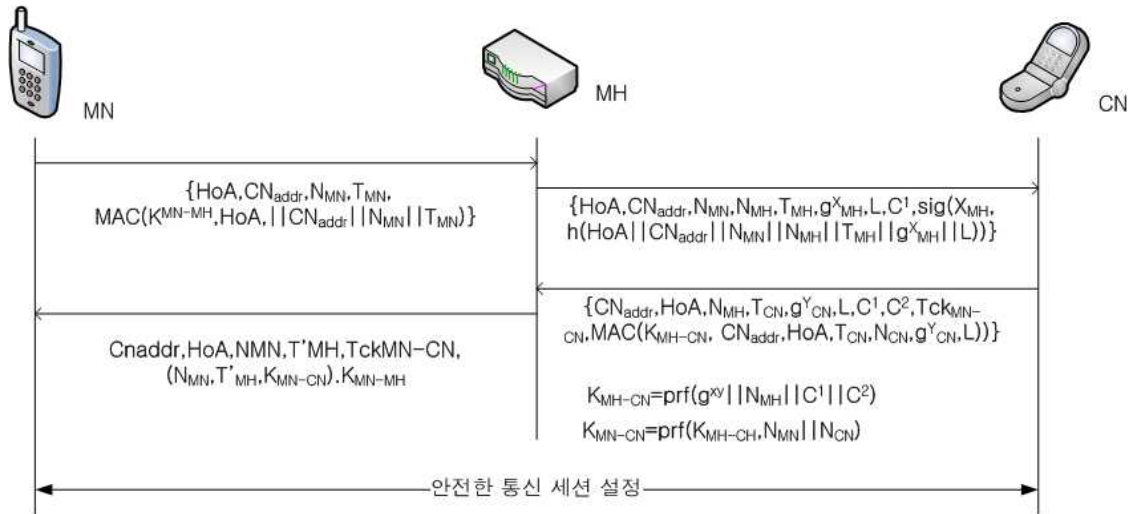


그림 1. MN과 CN사이의 세션키 설정 및 초기 바인딩 갱신 프로토콜

기존에 제안된 논문들에 대해서 살펴보고 3장에서는 이 논문에서 제안하고 있는 바인딩 갱신 프로토콜의 구체적인 방법에 대해 살펴본다. 4장에서는 제안한 프로토콜의 안전성 및 효율성에 대해서 분석할 것이며 마지막으로 결론 및 향후 연구 방향에 대해서 제시한다.

2. 프로토콜

본제안하는 프로토콜은 CGA 기반의 티켓 방식을 사용하는 프로토콜이다. 이번 절에서는 제안하는 프로토콜의 가정과 표기법 및 프로토콜에 대해서 구체적으로 서술한다.

2.1. 프로토콜의 가정 및 표기법

- 이동노드와 대응노드는 서로의 CGA에 대해 확신한다.
- 이동노드와 홈 에이전트는 미리 공유한 비밀키를 가진다.
- 대응노드는 이동노드가 아닌 고정노드로써 광 대역폭 및 풍부한 계산 능력 능력을 갖는다.

표 1. 표기법

표기	의미
MN/MH/CN	이동노드/이동노드의 홈 에이전트/대응노드
HoA/CoA	MN의 홈 주소/의탁주소
CN _{addr}	CN의 홈주소
T _X /N _X /L	노드 X의 타임스탬프/난스/타임스탬프
sig(-K _X ,M)	X노드의 개인키로 생성한 서명
MAC(K,M)	비밀키 K를 이용한 메시지 M의 MAC 값
X/g ^X	MH의 개인키/공개키 쌍
Y/g ^Y	CN의 개인키/공개키 쌍
Tck _{MN-CN}	MN을 위해 CN이 발행한 티켓
m1 m2	메시지 m1과 m2의 비트 결합
C ⁱ	i번째 cookie

2.2. 제안하는 프로토콜

MN과 CN사이의 초기 통신은 그림 1과 같이 수행된다. 초기 통신에서 MN은 HA를 통해서 CN과 통신 세션을 갖는다. 이 단계에서 HA와 CN은 두 노드 사이에 안전하게 데이터를 주고 받기 위해서 비밀키를 생성하고 CN은 MN을 위한 티켓을 발행한다. 일반적으로 초기 통신은 안전하다고 가정하지만 도청과 같은 수동적인 공격은 존재할 수 있기에 제안한 프로토콜은 키 생성에 안전성을 가미했다.

2.2.1. 최초 바인딩 갱신 프로토콜

MN이 CN에게 보내는 통신 연결 요청 메시지는 Neighbor Discovery[6]를 사용하는 HA에 의해서 인터셉트된다.

$$\{HoA, CN_{addr}, N_{MN}, T_{MN}, MAC(K^{MN-MH}, HoA, ||CN_{addr}||N_{MN}||T_{MN})\} \text{ ----- } M_1$$

MN은 M₁메시지를 MH에게 전송하여 CN과의 통신을 요청한다. MH는 MN과 미리 공유된 비밀키를 통해 MN으로부터 전송된 MAC 값을 확인하여 메시지의 무결성을 확인한다. MN이 보내는 N_{MN}는 MH가 응답 메시지를 전송할 경우 MH를 인증하기 위해 사용되면 MN과 CN사이에 사용할 세션키 생성에도 이용된다.

$$\{HoA, CN_{addr}, N_{MN}, N_{MH}, T_{MH}, g^X_{MH}, L, C^1, sig(X_{MH}, h(HoA||CN_{addr}||N_{MN}||N_{MH}||T_{MH}||g^X_{MH}||L))\} \text{ ----- } M_2$$

M₂ 메시지는 MN이 전송한 메시지를 MH가 인터셉트한 후에 메시지를 수정하여 CN에게 보내진다. T_{MH}는 MH의 타임스탬프로써 공격자의 재생공격을 방지하기 위해 추가된 파라미터이다. C¹은 두 노드 사이에 존재할 수 있는 도스 공격이나 Redirect 공격에 완화하기 위한 파라미터이다. 또한 MH는 메시지에 전자서명을 해서 보냄으로써 CN에서 MH를 인증할 수 있다. 마지막으로 g^x는 세션키를 생성하기 위해 MH가 생성한 공개키이다.

$$\{CN_{addr}, HoA, N_{MH}, T_{CN}, g^Y_{CN}, L, C^1, C^2, T_{ck_{MN-CN}}, MAC(K_{MH-CN}, CN_{addr}, HoA, T_{CN}, N_{CN}, g^Y_{CN}, L)\} \text{ ----- } M_3$$

$$K_{MH-CN} = \text{prf}(g^{xy} || N_{MH} || C^1 || C^2)$$

$$K_{MN-CN} = \text{prf}(K_{MH-CN}, N_{MN} || N_{CN})$$

M₂ 메시지를 수신한 CN은 일차적으로 MH에서 수신한 T_{MH}와 C¹을 확인한다. 먼저 g^x를 통해서 MH의 인터페이스 식별자를 생성할 수 있는지 확인한다. 마지막으로, MH의 공개키를 이용해서 전자서명을 확인한다. CN은 C¹에 대한 응답으로 C²를 생성하고 MH와 CN사이에 사용할 비밀키 K_{MH-CN}를 먼저 생성한다. 그런 후에 티켓 안에 들어갈 MN과 CN이 사용할 세션키 K_{MN-CN}을 생성한다. 마지막으로 MN에게 발행해 줄 티켓 T_{ck_{MN-CN}}을 생성한다. 이 티켓은 MN이 외부 링크로 핸드오프가 일어났을 경우 CN과의 바인딩 갱신에서 MN을 인증하고 MN과 CN사이에서 사용할 세션키를 확인하기 위함이다.

$$CN_{addr}, HoA, N_{MN}, T'_{MH}, T_{ck_{MN-CN}}, (N_{MN}, T'_{MH}, K_{MN-CN}).K_{MN-MH} \text{ ----- } M_4$$

MH는 MN의 HoA를 목적지로 전송되는 모든 메시지를 중간에서 가로챌 수 있기 때문에 M₃ 메시지를 수신한 MH는 C¹, C², T_{CN}을 일차적으로 확인한다. 올바른 사용자로부터 온 메시지라는 것을 확인되면 수신한 파라미터들을 이용해서 CN과 HA사이에 사용할 비밀키 및 MN과 CN사이에 사용할 세션키를 생성한다. 또한, MN에게 CN으로부터 수신한 티켓을 전송한다. 마지막으로 MN은 M₄ 메시지를 수신한 후에 N_{MN}과 T'_{MH}를 확인하여 MH를 인증하고

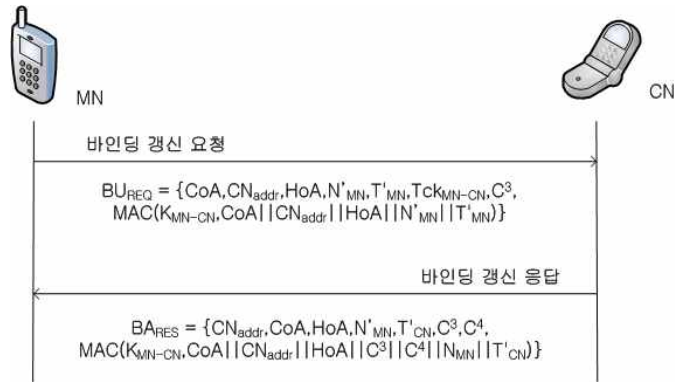


그림 2. MN과 CN사이의 차후 바인딩 갱신 프로토콜

티켓을 얻는다.

2.2.2. 차후 바인딩 갱신 프로토콜

그림 2는 MN이 외부링크로 핸드오프가 일어났을 경우에 수행되는 프로토콜이다. 먼저 MN은 BU 메시지에 CN으로부터 받은 티켓 T_{ck_{MN-CN}}과 쿠키 C³를 추가한다. 또한 메시지 인증을 위해 MAC 값을 같이 전송한다. BU 메시지를 수신한 CN은 먼저 타임스탬프와 쿠키를 통해 정당한 사용자로부터 전송된 메시지인지 확인 후에 티켓을 복호화 하고 두 노드 사이에 사용할 세션키를 얻는다. CN은 MN에게 MN의 쿠키와 자신이 생성한 쿠키 및 메시지 인증을 위해 MAC 값을 같이 전송한다. 이 메시지를 수신한 MN은 두 노드가 생성한 쿠키 값과 타임스탬프 값을 확인한 후에야 비로소 MAC값을 확인하고 CN을 인증한다.

3. 성능분석

이번 절에서는 앞서 제안한 바인딩 갱신 프로토콜의 안전성을 기존 네트워크 환경에 존재할 수 있는 여러 공격에 안전한지 분석한다.

안전성 분석

프로토콜의 안전성은 DoS (Denial of Service)공격과 Redirect 공격, MITM (Man-in-the-middle-attack), Replay 공격에 안전하다는 것을 증명할 것이다.

- **DoS 공격:** 공격자는 불필요한 메시지나 위조된 바인딩 갱신 메시지를 CN에게 플러딩(flooding)할 수 있다고 가정하자. 그럴 경우에 공격은 성공

적으로 이루어진다. 그러나 본 프로토콜에서 CN은 먼저 MN으로부터 온 쿠키와 타임스탬프를 확인한 후에 올바르게 않은 메시지일 경우에는 바로 메시지를 드롭한다. 또한 쿠키정보 역시 캐시에 저장하는 것이 아니기 때문에 메모리 overflow 공격에도 안전할 수 있다.

- **Redirect 공격:** MN과 CN사이의 통신에서, 공격자가 Redirect 공격의 일종인 Session Hijacking 공격을 할 수 있다고 가정하자. 그러나 우리의 프로토콜은 CGA 기반의 티켓 방식을 사용하기 때문에 공격자는 MN의 HoA 인터페이스 식별자를 생성하지 못한다. HoA 식별자와 CoA를 공격자가 얻었다고 해도 공격자는 CN의 비밀키로 암호화된 티켓을 위조할 수 없으므로 Redirect 공격의 일종인 Session Hijacking 공격을 성공시킬 수 없다.
- **중간자 공격 및 재생 공격:** 공격자는 MN과 CN 사이에서 중간자 공격 및 재생 공격을 할 수 있다고 가정하자. 그러나 앞서 살펴 본 공격들과 같이 공격자는 티켓을 위조할 수 없기 때문에 중간자 공격역시 어렵다. 또한 재생 공격 역시 메시지에 포함된 타임스탬프로 인해 어렵다.

4. 결 론

본 논문은 마이크로나 피코 셀 환경과 같이 핸드오프가 빈번하게 일어나는 환경에 적합한 안전하고 효율적인 바인딩 갱신 프로토콜을 제안했다. CGA 기반의 티켓 방식을 사용하기 때문에 여러 공격으로부터 안전할 뿐만 아니라 바인딩 갱신 시에 단 두 개의 메시지만으로 바인딩 갱신을 처리 할 수 있으므로 신속한 핸드오프 처리를 할 수 있다. 향후 연구 과제로는 PDA나 핸드폰 사용자의 증가 및 서비스의 다양한 변화와 진보로 인해서 대응노드가 고정노드가 아닌 이동노드인 상황에서 안전하게 바인딩 갱신을 처리할 수 있는 프로토콜에 대해 연구할 것이다.

참고문헌

- [1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2004.
- [2] T. Aura, "Cryptographically Generated Addresses (CGA)", IETF RFC 3972, March 2005.
- [3] Y. Qiu, J. Zhou, F. Bao, "Protecting All Traffic Channels in Mobile IPv6 Network", 2004 Wireless Communication and Networking Conference (WCNC), Vol. 1, Pages 160-165, March 2004.
- [4] G. Montenegro, C. Castelluccia, "Crypto-Based Identifiers (CBID): Concepts and Application", ACM Transactions on Information and System Security (TISSEC), Vol. 7, No. 1, Pages 97-127, February 2004.
- [5] G. O'Shea, M. Roe, "Child-proof Authentication for MIPv6 (CAM)", ACM Computer Communication Review, Vol 31 Issue 2, Pages 4-8, April 2001.
- [6] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, December 1998.