마이크로 및 피코 셀 환경에 적합한 MIPv6 바인딩 갱신 프로토콜

구중두*, 이기성*
*호원대학교 컴퓨터・게임학부
e-mail:jdkooinfo@gmail.com

Mobile IPv6 (MIPv6) Binding Update Protocol for Micro and Pico Cell Environments

Jung-Doo Koo*, Gi-Sung Lee*
*School of Computer Game, Howon University

요 약

본 논문에서는 핸드오프가 빈번하게 발생할 수 있는 마이크로 및 피코 셀 환경에 적합한 MIPv6 바인딩 갱신 프로토콜을 제안한다. 이는 안전성과 효율성을 고려하기 위해 CGA (Cryptographically Generated Addresses) 기반의 티켓 방식을 이용한다. 프로토콜의 분석 결과 기존의 다른 프로토콜에 비해 적은 계산량을 필요로 한다.

1. 서론

모바일 IPv6[1]에서 이동노드가 홈 링크 또는 홈 네트워크에서 통신하고 있는 중에 외부링크로 이동했을 경우에 이동노드는 홈 에이전트 및 기존에 통신하고 있는 대응노드와 바인딩 업데이트 과정을 수행해야 한다. 그렇지 않을 경우 통신하고 있는 노드와의 통신은 두절된다. 특히, 공항이나 터미널과 같은 곳에서는 핸드오프가 빈번하게 발생한다. 이런 빈번한 핸드오프는 통신 노드 사이에서 전송되는 패킷 손실 및 공격자로부터 많은 공격 위험에 노출될 수 있다. 따라서 우리는 마이크로 또는 피코 셀 환경과 같이 핸드오프가 빈번하게 일어나는 환경에 적합한 바인딩 업데이트 프로토콜을 제안한다.

제안하는 프로토콜은 CGA (Cryptographically Generated Address)[2] 기반의 티켓 방식을 사용한다. CGA는 통신 노드의 IPv6주소와 공개키를 이용해서 64비트의 인터페이스 식별자를 생성하는데 이용된다. 예를 들어, 이동노드의 홈 주소의 인터페이스 식별자는 홈 주소의 서브넷 프리픽스 정보와 공개키가 해쉬 함수를 통해서 계산된다. 이런 주소를 이용한 각 노드의 인증 및 공격으로부터 안전성을 제공한다. 또한 티켓은 이동노드에서 핸드오프가 일어났을 경우에 티켓을 발행한 대응노드에게 전송함으로써 이동노드를 인증할 수 있고 티켓 안의 세션키를 이용해서 두 노드 사이에 안전하게 통신을 할 수 있다.

초기 통신 시에 안전하게 교환된 티켓을 이용함으로써 기존의 바인딩 업데이트 프로토콜[1,3,4]보다 적은 메시지만으로 안전하게 바인딩 업데이트를 수행한다.

본 논문의 나머지 구성은 아래와 같다. 2장에서는 기존에 제안된 논문들에 대해서 살펴보고 3장에서는 이 논문에서 제안하고 있는 바인딩 업데이트 프로토콜의 구체적인 방법에 대해 살펴본다. 4장에서는 제안한 프로토콜의 안전성 및 효율성에대해서 분석할 것이며 마지막으로 결론 및 향후 연구 방향에 대해서 제시한다.

2. 관련연구

기존에 제안된 프로토콜은 크게 CGA에 기반한 프로토콜과 그렇지 않은 프로토콜로 나누어서 살펴보도록 한다.

첫 번째 프로토콜은 CGA에 기반 하는 CAM[5] 프로토콜이다. 이동노드에서 핸드오프가 발생했을 경우에 한 번의 메시지만으로 바인딩 갱신을 수행한다는 장점을 가진다. 그러나 이동노드가 PDA나 핸드폰과 같이 계산 능력과 베터리의 수명에 제한을 갖는 노드일 경우에는 CAM 프로토콜은 적합하지 않을 수 있다. 왜냐하면 이동노드에

서 계산량이 많은 전자서명에 대한 부담감을 가지기 때문이다. 또한 대응노드에서 서명 확인을 통한 노드를 인증하기 때문에 도스 공격 또는 리소스 고갈 공격의 위험에 노출될 수 있다.

두 번째 프로토콜은 대응노드에 대한 도스 공격을 막기 위해 클라이언트 퍼즐 개념을 이용한 CGA 기반의 프로토콜인 CBID (Crypto-Based Identifiers)[4]이다. 이 프로토콜은 앞서 살펴 본 CAM과는 다르게 이동노드에서 전자서명을 하는 대신에 연산능력이 뛰어난 홈 에이전트에서 처리함으로써 더욱 효율적이다. 또한 CAM에서는 식별자 생성에 서브넷 프리픽스 정보가 들어가지만 CBID의 경우에는 이동노드의 위치정보 및 임의로 생성한 값이 들어간다. 그러므로 주소 생성에 더욱 안전할 수 있다. 그러나 바인딩 업데이트는 식속하고 빠르게 처리되어야 하는 작업이다. CBID는 퍼즐을 해결하기 위해 필요한 시간이 바인딩 업데이트를 지연시킬 수도 있다는 단점을 가진다.

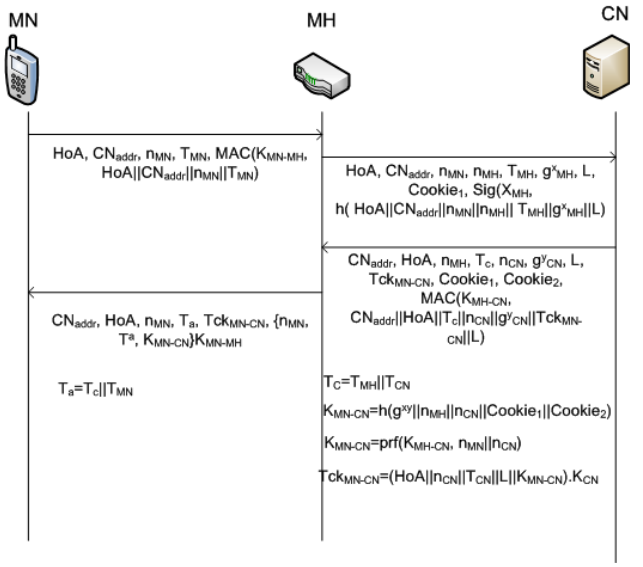
세 번째 프로토콜은 ECBU (Extended Certificate-Based Binding Update)이다. 이 프로토콜은 인증센터에서 발행한 인증서를 가지고 안전하게 바인딩 업데이트를 수행하는 프로토콜이다. 이 프로토콜의 단점이라고 하면 바인딩 업데이트를 수행하기 위해서 필요한 메시지 수이다. 우리가 제안한 프로토콜의 경우에는 티켓을 이용한 두 번의 메시지로 바인딩 업데이트가 수행되는데 반해서 ECBU는 8번의 메시지를 교환한다. 따라서 ECBU는 효율성 측면에서 볼 때 약간의 단점을 가질 수도 있다.

3. 제안하는 프로토콜

제안하는 프로토콜은 표 1과 같은 용어를 사용하고 MN과 CN은 각 노드의 CGA에 대에 확신하며 MN과 MH는 미리 공유한 비밀키를 가진다.

[표 1] 표기법

표기	의미
$MN/MH/CN$	이동노드/홈에이전트/대응노드
HoA/CoA	MN의 홈 주소 / 위탁주소
CN_{addr}	CN의 주소
BU/BA	바인딩 갱신 / 바인딩 갱신에 대한 응답
$T_e/N_e/L$	노드 e의 타임 스탬프/난수/라이프 타임(수명)
$MAC(K,M)$	메시지 인증 코드(K:키, M:메시지
K_{MH-CN} /K_{MN-CN}	MH와 CN사이의 비밀키/ MN과 CN사이의 세션키
x_{MN}/g^{x}_{MN}	MN의 diffie-hellman 개인키/공개키 쌍
y_{CN}/g^{y}_{CN}	CN의 diffie-hellman 개인키/공개키 쌍
Tck_{MN-CN}	MN과 CN사이의 티켓
$sig()$	전자서명
$A\|B$	메시지 A와 B의 비트 결합

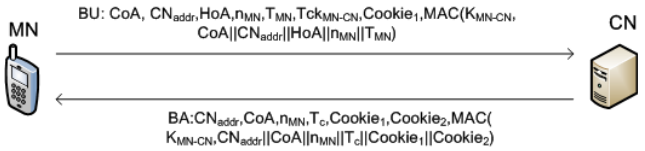


[그림 1] MN과 CN 사이의 초기 프로토콜

또한 CN은 이동가능한 노드가 아닌 고정노드로서 광 대역폭 및 풍부한 계산 능력을 갖는다고 가정한다.

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 추가했다. MN이 CN에게 보내는 통신 연결 요청 메시지는 Neighbor Discovery[6]를 사용하는 HA에 의해서 인터셉트된다. MN은 HA에게 CN과의 통신을 요청한다. MN은 HA와 공유하고 있는 비밀키를 가지고 MAC을 통해서 메시지를 인증한다. MN이 보내는 n_{MN}는 MN과 CN사이에 사용할 세션키 생성에 필요한 파라미터이다.

M_2 메시지는 MN이 전송한 메시지를 인터셉트한 후에 그 메시지를 수정하여 CN에게 보내지는 메시지이다. T_{MH}는 HA의 타임스탬프로써 이 메시지를 수신하는 CN에서 일차적인 필터링 역할을 하기 위해서 사용되는 파라미터이다. $Cookie_1$ 역시 T_{MH}와 같이 두 노드 사이에 존재할 수 있는 도스 공격이나 Redirect 공격에 대응하기 위해서 보내지는 일차적 필터링 역할을 수행하는 파라미터이다. 또한 HA는 메시지에 전자서명을 해서 보냄으로써 CN에서 HA를 인증할 수 있다. M2메시지를 수신한 CN은 일차적으로 HA에서 수신한 타임스탬프 T_{MH}와 $Cookie_1$을 확인한다. 먼저, g^x를 통해서 MN의 HoA의 인터페이스 식별자를 생성할 수 있는지 확인한다. 마지막으로, HA의 공개키를 이용해서 전자서명을 확인한다. CN은 $Cookie_1$에 대한 응답으로 $Cookie_2$를 생성하고 MH와 CN사이에 사용할 비밀키 KMH-CH를 생성한다. 또한 티켓 안에 들어갈 MN과 CN이 사용할 세션키 K_{MN-CN}을 생성한다. 마지막으로 MN에게 발행해 줄 티켓 Tck_{MN-CN}을 생성한다. 이 티켓은



[그림 2] MN과 CN 사이의 direct 바인딩 갱신 프로토콜

MN이 핸드오프가 일어날 경우 CN과의 바인딩 업데이트에서 MN을 인증하고 MN과 CN사이에서 사용할 세션키를 확인하기 위함이다. M3 메시지를 수신한 HA는 Cookie와 CN과 자신의 타임스탬프를 결합한 Tc를 일차적으로 확인한다. 적당한 사용자로부터 온 메시지라는 것이 확인되면 수신한 파라미터들을 이용해서 CN과 HA사이에 사용할 비밀키 및 MN과 CN사이에 사용할 세션키를 생성한다. 또한, MN에게 CN으로부터 수신한 티켓을 전송한다. MN은 자신이 보낸 난스와 각 노들의 타임스탬프를 결합한 T_a를 확인하고 티켓을 얻는다. 수신한 티켓은 CN에서 MN의 핸드오프 발생 시에 MN을 인증할 때 사용한다.

다음은 MN이 핸드오프가 일어났을 경우 그림 2와 같이 프로토콜이 수행된다. 먼저 MN은 BU 메시지에 CN으로부터 받은 티켓과 쿠키를 추가한다. 또한 메시지 인증을 위해 MAC을 계산한다. BU 메시지를 수신한 CN은 먼저 타임스탬프와 쿠키를 통해 정당한 메시지인지를 확인한다. 또한, 티켓을 복호화 한 후에 두 노드 사이에 사용할 세션키를 확인한다. CN은 MN에게 MN의 쿠키와 자신이 생성한 쿠키 및 메시지 인증을 위해 MAC 값을 전송한다. 이 메시지를 수신한 MN은 먼저 두 노드가 생성한 쿠키 값과 타임스탬프의 결합인 T_c를 확인한 후에야 비로소 MAC값을 확인한다.

4. 성능분석

DoS 공격을 포함한 기존 네트워크 환경에 존재할 수 있는 공격 시나리오에 제안하는 프로토콜이 얼마나 강건하지를 보인다.

- **DoS 공격**: 공격자는 불필요한 또는 위조된 바인딩 업데이트 메시지를 CN에게 플러딩 할 수 있다고 가정하자. 그럴 경우에 공격은 성공적으로 이루어진다. 그러나 우리의 프로토콜에 CN은 먼저 MN으로부터 온 쿠키와 타임스탬프를 확인한 후에 올바르지 않은 메시지일 경우에는 바로 메시지를 드롭한다. 또한 쿠키정보 역시 캐쉬에 저장하는 것이 아니기 때문에 메모리 오버플로우 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 티켓을 위조할 수 없으므로 Redirect 공격의 일종인 Session Hijacking 공격을 성공시킬 수 없다.

- **중간자 공격 및 재생 공격**: 공격자는 MN과 CN사이에서 중간자 공격 및 재생 공격을 할 수 있다고 가정하자. 그러나 앞서 살펴 본 공격들과 같이 공격자는 티켓을 위조할 수 없기 때문에 중간자 공격은 어렵다. 또한 재생 공격 역시 메시지에 포함된 타임스탬프로 인해서 어렵다.

- **초기 통신시에 세션키 및 비밀키 도청 공격**: 초기 통신을 할 때 공격자가 도청을 할 수 있다. 그러나 중요한 세션키나 비밀키는 알아 낼 수 없다. 왜냐하면 MH와 CN 사이의 세션키 는 $K_{MH-CN}=H(g^{xy}||n_{MH}||n_{CN})$와 같이 생성한다. 그러나 공격자는 DH 세션키인 g^{xy}를 생성할 수 없다. 또한 MN과 CN사이의 세션키는 MH와 CN사이의 비밀키 K_{MH-CN}을 알아 낼 수 없기 때문에 이 키 또한 알아 낼 수 없다.

5. 결론

본 논문에서는 핸드오프가 빈번하게 발생할 수 있는 마이크로 및 피코 셀 환경에 안전하고 효율적일 수 있는 바인딩 갱신 프로토콜을 제안했다. 이 프로토콜은 CGA 기반의 티켓 방식을 사용하기 때문에 여러 공격으로부터 안전할 뿐만 아니라 바인딩 업데이트 시에 단 두 개의 메시지만으로 바인딩 업데이트를 수행하기 때문에 짧은 시간에 바인딩을 수행할 수 있다는 장점을 가진다.

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.