한국산학기술학회논문지
Vol. 8, No. 6, pp. 1519-1523, 2007

마이크로 및 피코 셀 환경에 적합한 인증된 모바일 IPv6 바인딩 갱신 프로토콜

이기성[1*]

Authenticated Mobile IPv6 Binding Update Protocol for Micro/Pico Cell Environments

Gi-Sung Lee[1*]

요 약 본 논문은 모바일 IPv6를 기반으로 하는 마이크로 및 피코 셀 환경에서 핸드오프 또는 핸드오버 시에 빠르고 안전한 바인딩 갱신을 해결하기 위한 제안이다. 기존의 주소 생성 방식과 달리 본 프로토콜에 참여하고 있는 노드나 라우터는 CGA(Cryptographically Generated Address) 방식을 통해 주소를 생성한다. 이동노드는 한정된 전력과 계산능력을 가지고 있기 때문에 키 생성 시에는 홈 에이전트가 이동노드를 대신하여 대응노드와 키 동의 프로토콜을 수행한다. 대응노드는 키를 생성한 후 티켓 안에 키를 포함시켜 자신의 개인키로 암호화하여 이동노드에게 전송한다. 이는 홈 에이전트나 동작하지 않는 환경에서도 두 노드 간에 직접 통신을 하기 위함이다. 성능 분석에서는 몇 가지 공격 시나리오를 통한 프로토콜의 안전성을 분석하고 기존 프로토콜과 비교함으로써 효율성을 분석한다. 마지막으로 결론 및 향후 연구 방향에 대해서 제시한다.

Abstract In this paper, we propose the fast and secure binding update protocol as handoff or handover in the micro and pico environment based on mobile IPv6. The nodes or routers on participating in this protocol generate their addresses from cryptographically generated addresses (CGAs) method unlike previous address generation method. The mobile node (MN) includes in home network or home link has limited power and computational abilities. So the home agent (HA) of the MN executes key agreement protocol with the correspondent node (CN) on behalf of the MN. The CN then creates a ticket on including session key, lifetime of ticket, and so on. It then transmits it to the MN via the HA of the MN. The ticket is used to communicate directly between the MN and its CN. In performance analysis, we analyze security of proposed binding update protocol under various attack scenarios and efficiency by comparing proposed protocol with prior binding update protocols. Finally we make a conclusion of this paper and present future works.

Key Words : 모바일 IPv6, 바인딩 갱신, 경로 최적화, CGA

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 위험에 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 공

이 논문은 2007년 호원대학교 교내연구비의 지원에 의하여 연구되었음
[1]호원대학교 컴퓨터게임학부
*교신저자: 이기성(ygslee@howon.ac.kr)

개키를 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 기존에 제안된 논문들에 대해서 살펴보고 3장에서는 이 논문에서 제안하고 있는 바인딩 갱신 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 살펴본다. 첫 번째 프로토콜은 CAM[5] 프로토콜이다. MN에서 핸드오프가 발생했을 경우 한 번의 메시지만으로 CN과 바인딩 갱신을 수행할 수 있다는 장점을 가진다. 그러나 MN이 PDA나 핸드폰과 같이 계산 능력과 배터리의 수명에 제한을 갖는 노드일 경우에는 CAM 프로토콜은 적합하지 않을 수 있다. 왜냐하면 MN에서 전자서명과 같이 계산량이 많은 연산을 수행해야 하기 때문이다. 또한 CN에서 서명 확인을 통한 노드를 인증하기 때문에 도스(DoS, Denial of Service) 공격 또는 리소스 고갈 공격의 위험에 노출될 수 있다. 두 번째 프로토콜은 CN에 대한 도스 공격을 완화하기 위해 클라이언트 퍼즐 개념을 이용한 (Crypto-Based Identifiers)[4] 프로토콜이다. 이 프로토콜은 앞서 살펴 본 CAM과는 다르게 MN에서 전자서명을 하는 대신에 계산능력이나 배터리의 수명에 제한이 없는 HA에서 처리함으로써 MN에 대한 부담을 줄였다. 또한 CAM에서는 식별자 생성에 기본적으로 누구나 쉽게 획득할 수 있는 서브넷 프리픽스 정보가 들어가지만 CBID의 경우에는 MN의 위치정보 및 임의로 생성한 값이 들어간다. 그러므로 주소 생성에 좀 더 나은 안전성을 제공할 수 있다. 그러나 바인딩 갱신은 신속하고 빠르게 처리되어야 하는 작업이다. CBID는 퍼즐을 해결하기 위해 필요한 시간이 바인딩 갱신을 지연시킬 수도 있다는 단점을 가진다. 세 번째 프로토콜은 ECBU (Extended Certificate-Based Binding Update)[3]이다. 이 프로토콜은 인증센터에서 발행한 인증서를 가지고 바인딩 갱신을 수행한다. 이 프로토콜의 단점이라고 하면 바인딩 갱신을 수행하기 위해서 필요한 메시지 수이다. 우리가 제안한 프로토콜의 경우에는 티켓을 이용한 두 번의 메시지로 바인딩 갱신을 수행되는데 반해서 ECBU는 8번의 메시지가 전송된다. 따라서 이는 효율성 측면에서 볼 때 약간의 단점을 가질 수도 있다.

3. 프로토콜

이번 절에서는 제안하는 프로토콜의 가정과 표기법 및 프로토콜에 대해서 구체적으로 서술한다.

3.1 프로토콜의 가정

- MN과 CN은 서로의 CGA에 대해 신뢰한다.
- MN과 MN의 HA는 미리 공유된 비밀키를 가진다.
- CN과 HA는 MN과 달리 고정노드로써 광 대역폭 및 풍부한 계산 능력 능력을 갖는다.

3.2 표기법

- MN/MH/CN : 이동노드/이동노드의 홈 에이전트/대응노드.
- HoA/CoA: MN의 홈 주소/의탁주소.
- CN_{addr}: CN의 홈 주소.
- BU/BA: 바인딩 갱신/바인딩 갱신에 대한 응답.
- $T_X/N_X/L$: 노드 e의 타임스탬프/난수/라이프 타임.
- MAC(K,M) : 메시지를 인증하기 위해 사용되는 해시 함수 (K:키, M: 메시지).
- K_{MH-CN}/K_{MN-CN}: MH와 CN사이의 비밀키/MN과 CN 사이의 세션키.
- C^i: i번째 쿠키(cookie) 값.
- X/g^X: MH의 개인키/공개키 쌍.
- Y/g^Y: CN의 개인키/공개키 쌍.
- sig(PK,M): 개인키 PK를 이용한 메시지 M의 전자서명
- Tck_{MN-CN}: MN을 위해 CN이 발행한 티켓.
- m1||m2: 메시지 m1과 m2의 비트 결합.

3.3 제안하는 프로토콜

MN과 CN사이의 초기 통신은 그림 1과 같이 수행된다. MN은 MH(Mobile's HA)를 통해서 CN과 통신한다. 이 때 MH와 CN은 전력과 계산능력에 제한을 받지 않는 노드이기 때문에 다소 계산량이 많지만 안전한 메시지 전송을 위해 전자서명을 이용한다. 두 노드 사이에 MN을 위한 키 동의 과정이 끝나면 CN은 MN과 자신이 사용할 세션키와 세션키의 수명, 기타 사용자의 홈 주소, 기타 등등을 포함하고 있는 티켓을 생성한다. 초기 프로토콜은 MN과 CN 사이에 세션키가 없는 경우로 기존의 프로토콜들과 같이 MH를 이용하여 바인딩 갱신을 수행한다. 티켓이 발행된 이후에는 MN은 MH의 도움 없이 CN과 직접 바인딩 갱신을 수행할 수 있다. 특히, 기존의 방식과 달리 MH가 동작하지 않는 환경에서 유용할 수 있다.

3.3.1 초기 통신 프로토콜

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

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

MN은 M_1메시지를 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.

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

M_2 메시지는 MN이 전송한 메시지를 MH가 인터셉트한 후에 메시지를 수정하여 CN에게 보내진다. T_{MH}는 MH의 타임스탬프로써 공격자의 재생공격을 방지하기 위해 추가된 파라미터이다. C^1은 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.

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

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

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

M_2메시지를 수신한 CN은 일차적으로 MH에서 수신한 T_{MH}와 C^1을 확인한다. 먼저 g^x를 통해서 MH의 인터페이스 식별자를 생성할 수 있는지 확인한다. 마지막으로, MH의 공개키를 이용해서 전자서명을 확인한다. CN은 C^1에 대한 응답으로 C^2를 생성하고 MH와 CN사이에 사용할 비밀키 $K_{MH\text{-}CH}$를 먼저 생성한다. 그런 후에 티켓 안에 들어갈 MN과 CN이 사용할 세션키 $K_{MN\text{-}CN}$을 생성한다. 마지막으로 MN에게 발행해 줄 티켓 $Tck_{MN\text{-}CN}$을 생성한다. 이 티켓은 MN이 외부 링크로 핸드오프가 일어났을 경우 CN과의 바인딩 갱신에서 MN을 인증하고 MN과 CN사이에서 사용할 세션키를 확인하기 위함이다.

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

MH는 MN의 HoA를 목적지로 전송되는 모든 메시지를 중간에서 가로챌 수 있기 때문에 M_3 메시지를 수신한 MH는 C^1, C^2, 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 M_4 메시지를 수신한 후에 N_{MN}과 T'_{MH}를 확인하여 MH를 인증하고 티켓을 얻는다.

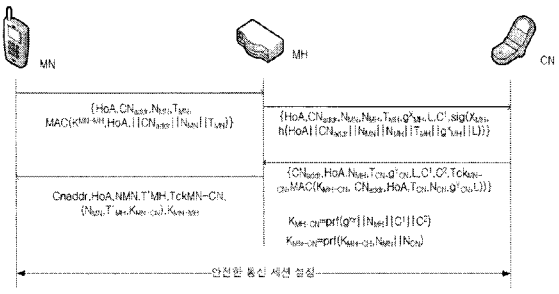

그림 1. MN과 CN사이의 세션키 설정 및 초기 바인딩 갱신 프로토콜

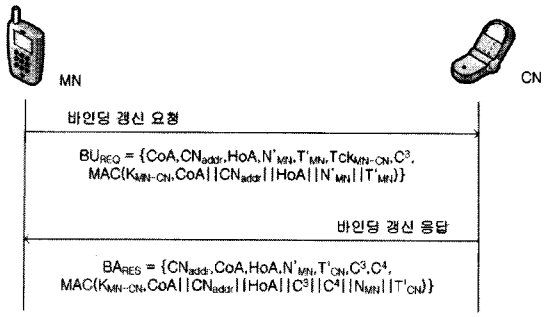

그림 2. MN과 CN사이의 차후 바인딩 갱신 프로토콜

3.3.2 차후 바인딩 갱신 프로토콜

그림 2는 MN이 외부링크로 핸드오프가 일어났을 경우에 수행되는 프로토콜이다. 먼저 MN은 BU 메시지에 CN으로부터 받은 티켓 Tck_{MN-CN}과 쿠키 C^3를 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.

4. 성능분석

본 절에서는 제안한 바인딩 갱신 프로토콜이 DoS (Denial of Service) 공격과 Redirect 공격, MITM (Man-in-the-middle-attack), replay 공격 및 기타 공격 시나리오에 안전하다는 것을 증명한다.

4.1 안전성 분석

- **DoS 공격**: 공격자는 불필요한 메시지나 위조된 바인딩 갱신 메시지를 CN에게 플러딩(flooding) 할 수 있다고 가정하자. 그럴 경우에 공격은 성공적으로 이루어진다. 그러나 본 프로토콜에서 CN은 먼저 MN으로부터 온 쿠키와 타임스탬프를 확인한 후에 올바르지 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 CN사이에서 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.
- **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 CN사이의 세션키는 $K_{MH-CN}=H(g^{XY}||N_{MH}||N_{CN})$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.

4.2 효율성 분석

MN에서 핸드오프가 일어난 후에 BU 프로토콜의 메시지 수와 각 노드에서 처리해야 할 계산량을 비교하여 프로토콜의 효율성을 분석한다.

표 1. 프로토콜의 효율성 분석

	RR[1]	ECBU[3]	CBID[4]		제안하는 프로토콜	
			BCBID	ECBID	초기 BU	차후 BU
메시지 수	8	8	4	7	**4**	**2**
MN의 계산	None	None	DH(1)/DS(2)	None	**DH(2)**	**None**
CN의 계산	None	DH(1)/DS(2)	DH(1)/DS(2)	DH(1)/DS(2)	**DH(4)/DS(2)**	**None**
HA의 계산	None	DH(1)/DS(2)	None	DH(1)/DS(2)	**DH(4)/DS(2)**	**None**

- DH/DS: Diffie-Hellman 계산/전자서명 - None: DH 및 DS를 계산하지 않음
- BCBID/ECBID: 기본 CBID/확장 CBID

표 1에서 메시지의 수는 RR이 가장 많지만 각 노드에서 처리해야 하는 계산량이 비교적 적다. 하지만 ECBU는 메시지의 수는 RR과 같지만 계산량이 많은 전자서명은 전력과 계산능력에 제한이 없는 HA에서 MN을 대신하여 처리하기 때문에 MN에 대한 계산적 부담은 적다. CBID의 경우에는 BCBID는 메시지의 수는 적지만 MN에서 처리해야할 계산량이 많기 때문에 부담이 있지만 확장 CBID인 ECBID에서는 그에 대한 부담을 MN의 HA가 처리하기 때문에 MN의 부담을 덜어준다. 하지만 이런 과정을 마이크로 및 피코 셀 환경과 같이 빈번하게 핸드오프가 발생하는 환경에서 매번 반복해야 하기 때문에 효율성이 떨어질 수 있다. 하지만 제안하는 바인딩 갱신 프로토콜은 초기에는 MN의 계산 부담을 줄이게 위해 MH에서 처리하고 티켓이 발행된 차후 바인딩 갱신 후부터는 두 노드 사이에 두 번의 메시지 교환으로 바인딩 갱신을 수행할 수 있기 때문에 더욱 효율적이다. 또한, 제안하는 프로토콜은 차후 바인딩 갱신 후부터는 MH가 동작하지 않아도 바인딩 갱신을 수행할 수 있지만 기존의 몇몇 프로토콜은 동작하지 못할 수 있다. MH없이 바인딩 갱신을 처리할 수 있다고 해도 MN에게 계산적 부담을 많이 주는 방식이다.

5. 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.

이 기 성(Gi-Sung Lee) **[종신회원]**

- 1993년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

<관심분야>
이동통신, 멀티미디어 통신, 네트워크 보안