情報保護學會論文誌
第16卷 第5號, 2006. 10

모바일 IPv6 네트워크를 위한 티켓 기반의 인증된 바인딩 갱신 프로토콜

구 중 두,[1†] 김 상 진,[2†] 오 희 국[1‡]
[1]한양대학교, [2]한국기술교육대학교

Authenticated Ticket-based Binding Update Protocol for Mobile IPv6 Network

Jung-doo Koo,[1†] Sangjin Kim,[2†] Heekuck Oh[1‡]
[1]Hanyang University, [2]Korea University of Technology and Education

요 약

기존에 제안된 모바일 IPv6를 위한 바인딩 갱신 프로토콜은 이동노드가 홈 링크가 아닌 외부 링크로 이동할 때마다 동일한 프로토콜 과정을 반복한다. 뿐만 아니라 바인딩 갱신의 정해진 수명으로 인해 이동하지 않은 경우에도 동일한 과정을 수시로 반복해야 한다. 본 논문은 이 문제점을 해결하기 위해 티켓 기반의 바인딩 갱신 프로토콜을 제안한다. 제안하는 프로토콜은 대응노드가 발급한 티켓을 사용하여 빈번하게 발생할 수 있는 바인딩 갱신 과정을 최소화한다. 모바일 IPv6의 보안 요구사항과 기존에 알려진 공격에 대한 프로토콜의 안전성을 분석하였으며, 기존에 제안된 바인딩 갱신 프로토콜과 성능을 비교하여 효율성을 분석하였다.

ABSTRACT

Previous binding update protocols for Mobile IPv6 repeats the same protocol each time a mobile node moves to a foreign link. Moreover, mobile nodes repeats the same protocol whenever the lifetime of the current binding update expires. To improve the efficiency of binding updates, we propose a ticket-based binding update protocol for MIPv6. Our protocol minimizes the binding update cost using a ticket issued by the corresponding node. We have analyzed our protocol security against the security requirements of MIPv6 and existing attacks. Furthermore, we have also compared our protocol against previous binding update protocols.

Keywords : *Mobile IPv6 (MIPv6), binding update*

Ⅰ. 서 론

IP를 사용하는 기존 단말은 보통 고정된 IP 주소를 가지게 되는데, IP 주소는 연결되어 있는 네트워크 링크에 의해 결정되므로 단말의 물리적인 이동이 가능한 환경에서는 더 이상 고정된 IP 주소만을 사용할 수 없게 된다. 따라서 이동에도 불구하고 끊임이 없는 통신이 이루어지기 위해서는 동적으로 IP 주소가 변경되어야 한다. 그런데 그 단말의 고정된 IP 주소만을 알고 있는 노드들은 이 주소를 이용하

접수일: 2006년 5월 23일; 채택일: 2006년 8월 16일
* 본 연구는 한국과학재단 특정기초연구 지원으로 수행되었음. (R01-2006-000-10957-0)
† 주저자, jdkoo@cse.hanyang.ac.kr
‡ 교신저자, hkoh@cse.hanyang.ac.kr

여 노드와 언제든지 통신할 수 있도록 해주어야 하는 상충되는 문제가 있다.

이 문제점을 해결하기 위해 모바일 IPv6가 등장하게 되었다[1]. 모바일 IPv6에서 이동노드(MN, Mobile Node)는 노드의 물리적인 위치와 상관없이 변하지 않는 홈주소(HoA, Home Address)와 외부 링크로 이동했을 때 외부 링크에서 임시로 할당받은 의탁주소(CoA, Care-of Address)를 갖는다. 모바일 IPv6에서 MN은 외부 링크에 있을 때 자신을 대신하여 주는 홈 에이전트(HA, Home Agent)를 둔다. MN이 새로운 링크로 이동하여 새 의탁주소를 획득하게 되면, 이 주소를 자신의 HA에 등록해야 한다. 이 등록을 통해 노드의 물리적인 위치와 상관없이 항상 다른 노드들은 이 노드의 HoA를 이용하여 메시지를 전달할 수 있다. MN이 홈 링크에 없을 때 도착된 메시지들은 HA가 등록된 주소를 이용하여 전달하여 준다. 그런데 이 방식은 항상 모든 통신이 HA를 통해 이루어지게 되므로 네트워크를 비효율적으로 사용하게 되는 결과를 초래한다. 이 문제를 해결하기 위해 모바일 IPv6에서는 HA뿐만 아니라 대응노드(CN, Corresponding Node)에게도 새 의탁주소를 알려주어 HA를 이용하지 않고 직접 통신을 할 수 있는 방법을 제공해 주고 있다. 이것을 경로 최적화(route optimization)라 하며, 이것은 선택사항으로서 MN이 원하면 이루어지게 된다. 이와 같이 HA나 CN에게 새 의탁주소를 등록하는 과정을 "바인딩 갱신"이라고 한다.

모바일 IPv6의 표준문서에서는 MN이 외부 링크로 이동했을 경우에 RR(Return Routability) 과정을 이용하여 CN과 바인딩 갱신을 수행하도록 권고하고 있다[1]. 그러나 이 과정을 안전하게 수행하지 않을 경우 여러 공격 등에 취약할 수 있다. 따라서 바인딩 갱신은 아래와 같은 보안 요구사항[2,3]을 만족해야 한다.

- 요청자의 인증: 바인딩 갱신 메시지를 수신하는 노드는 반드시 요청자를 인증할 수 있어야 한다.
- 응답자의 인증: 요청자 역시 응답자를 인증할 수 있어야 한다.
- 바인딩 갱신 정보의 무결성: 바인딩 갱신 정보는 다른 공격자로부터 반드시 보호되어야 한다.
- 요청자의 위치 인증: 응답자는 요청자가 현재 위치(의탁주소)에 존재하는지 검증할 수 있어야 한다.

표준 방법인 RR 기법은 보안 요구사항을 전적으로 만족하지 못하고 있다. 이 문제점을 극복하기 위해 RR 기법에 IPsec을 사용하여 바인딩 갱신 과정을 수행하도록 표준문서는 권장하고 있다[4]. 그러나 IPsec은 장기간 연결 관계가 형성되는 MN과 HA 사이에는 효율적일 수 있으나 단기간 연결 관계를 갖는 MN과 CN 사이에는 비효율적일 수 있다. 또한, IPsec은 내부 키 교환 프로토콜인 IKE를 수행하는데 드는 연산량이 적지 않기 때문에 저전력이며 한정된 계산량을 갖는 통신 노드일 경우에는 부담이 될 수 있다. 따라서 IPsec을 사용하지 않고도 MN과 CN 간에 저렴한 비용으로 안전하게 바인딩 갱신을 수행하는 메커니즘이 요구되었다.

하지만 기존에 제안된 바인딩 갱신 프로토콜들은 MN의 접속 링크나 네트워크가 변했을 경우에 매번 동일한 프로토콜 과정을 반복한다. 특히 RR의 경우에는 공개 채널로 전달되는 키 생성 정보의 취약성을 최소화하기 위해서는 매번 전체 과정을 반복하는 것이 안전하다. 또 바인딩 갱신은 이동을 하지 않은 경우에도 수명이 끝나면 다시 갱신을 해야 한다. 이 경우에도 기존 전체 과정을 다시 반복해야 하면 효율성이 떨어진다.

본 논문에서는 이 문제점을 해결하기 위해 티켓을 이용한 바인딩 갱신 프로토콜을 제안한다. 티켓은 그것을 한번 획득하면 그것의 유효기간 동안에는 효율적으로 갱신할 수 있도록 해준다. 뿐만 아니라 공개키 연산을 이용하여 상호 인증하지 않고 티켓에 포함된 티켓키를 이용한 MAC 값을 통해 각 노드를 인증할 수 있기 때문에 계산 부담과 한정된 전력을 가진 MN에게 효율적이다. 더구나 티켓을 이용한 바인딩 갱신 기법은 다음과 같은 추가적인 장점을 갖는다. 첫째, 티켓은 CN만이 알고 있는 비밀키로 발급되며 MN을 인증하기 위한 필요한 정보가 모두 암호화되어 포함되어 있으므로 CN은 티켓에 대한 상태 정보를 유지할 필요가 없다. 둘째, CN이 발급하며 CN 만 발급된 티켓을 사용하므로 시스템 간에 클록 동기화가 요구되지 않는다. 셋째, HA가 동작하지 않는 환경에서도 MN과 CN은 바인딩 갱신을 수행할 수 있다.

제안하는 프로토콜은 MN과 CN 구간을 제외한 모든 구간에서 IPsec을 사용한다. MN과 HA는 장기간 관계를 형성하기 때문에 IPsec을 효율적으로 사용할 수 있다[4]. 또한 HA와 CN 간에 IPsec의 사용은 CN이 전력과 계산 능력에 제한을 받지 않는

표 1. 표기법

표 기	의 미
MN/CN/HA	이동노드/대응노드/홈 에이전트
HoA/CoA	MN의 홈 주소/의탁주소
A_{addr}	노드 A의 주소
$+K_A/-K_A$	노드 A의 공개키와 개인키
K_{A-B}	노드 A와 B사이의 대칭 키
T_A	노드 A가 생성한 타임스탬프
L_X	X의 수명
N_A	노드 A가 생성한 난스
$\{M\}.K$	비밀키 K를 이용한 메시지 M의 암호화
$MAC(K,M)$	비밀키 K를 이용한 메시지 M에 대한 MAC 값
$Sig(-K_A,M)$	개인키 -K를 이용한 메시지 M에 대한 서명값
$M_1 \| M_2$	메시지 M_1과 M_2의 비트 결합

고정노드라고 가정하기 때문에 가능하다. 물론 CN이 IPsec을 지원하지 않는 노드일 수도 있으며, HA와 CN이 다른 인증체계를 가지고 있어 서로 인증서를 확인하는 절차가 복잡할 수 있다. 하지만 CGA와 같은 공개키 방식을 배제할 경우에는 MN과 CN 사이에 신뢰 관계를 형성하는 것이 가능하지 않으므로 이것이 하나의 대안으로 충분히 고려할 가치가 있다. 즉, 본 논문에서는 IPsec을 제외한 어떤 공개키 연산을 사용하지 않고 효율적으로 바인딩 갱신을 할 수 있는 프로토콜을 제안한다.

이 논문의 구성은 다음과 같다. 2장에서는, 기존에 제한된 바인딩 갱신 프로토콜에 대해서 살펴보고, 3장에서는 제안하는 프로토콜에 대해 자세히 기술한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 끝으로 5장에서는 결론과 향후 연구방향을 제시한다.

II. 연구 배경

2.1 표기법

이 논문에서는 표 1에 기술된 표기법을 사용하여, 기존 연구와 제안된 프로토콜을 설명한다. 모든 주소는 비상태 주소 설정 방법(stateless address autoconfiguration)[5]을 사용하여 설정한다. 프로토콜에 따라 CGA(Cryptographically Generated Address) 방식[6]을 이용하여 주소가 생성될 수 있다. CGA 방식은 비상태 자동 주소 설정 방법으로 주소를 설정하는 방식이지만 기존의 방식과 달리 독특한 인터페이스 식별자 대신에 그 노드의 공개키를 해쉬한 값을 이용하여 주소를 생성한다. 따라서 주소에 포함된 공개키에 대응되는 개인키를 이용하여 메시지를 서명하여 교환하면 주소 소유자에 의해 전송된 메시지임을 증명할 수 있다. 공격자들은 자신의 공개키를 이용하여 CGA를 마음대로 만들 수 있지만 다른 노드가 이미 사용하고 있는 주소를 가로챌 수는 없다.

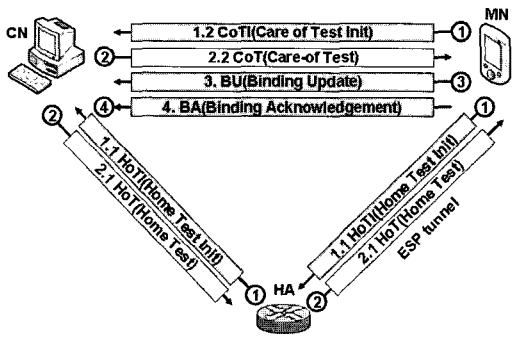


그림 1. RR 프로토콜

2.2 기존연구

본 절에서는 기존에 제안된 바인딩 갱신 프로토콜들에 대해 알아본다. 그림 1에 기술된 RR 기법[1]은 IETF에서 현재 표준으로 권고하고 있는 바인딩 갱신 프로토콜이다. 이 기법은 CN이 MN의 바인딩 갱신 요청을 승인해주기 전에 MN의 HoA와 CoA를 사용하여 MN이 메시지를 수신할 수 있는지 확인할 수 있도록 해준다. 하지만 RR 과정은 다음과 같은 몇 가지의 문제점을 가지고 있다. 첫째, 키를 생성하기 위한 정보가 공개 채널로 전달된다. 단, 공격자는 두 경로로 전달되는 HoT와 CoT 메시지를 모두 가로 챌 수 있어야 한다. 이 점은 여러 공격자들이 공모하면 그리 어려운 일은 아니며 CN과 같은 링크나 CN과 HA, MN과 HA의 경로가 중첩되는 링크에 접속되어 있어도 모든 메시지를 볼 수 있다. CN과 같은 링크에 있는 경우에는 BU 메시지를 공격하지 않아도 통신 세션을 가로챌 수 있다. 예를 들어, 공

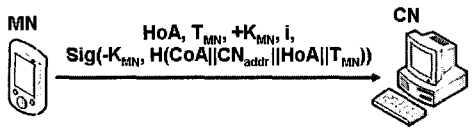


그림 2. CAM 프로토콜

격자 자신이 CN의 기본 라우터 행세를 하여 세션을 가로 챌 수 있다. 둘째, MN이 실제 주장된 CoA에 있는지 CN이 검증할 수 없다. 즉, MN은 항상 이웃 노드의 주소로 허위 갱신을 하여 이웃노드를 공격할 수 있다.

CAM(Child-proof Authentication for MIPv6) 프로토콜[7]은 CGA를 이용하여 바인딩 갱신을 수행하며, 프로토콜의 구성도는 그림 2와 같다. 이 프로토콜에서 MN의 HoA는 MN의 홈 링크의 프리픽스와 $H(+K_{MN}, i)$를 이용하여 생성된다. 여기서 i는 주소 충돌을 방지하기 위한 값이다. MN은 바인딩 갱신 요청 메시지를 HoA를 생성할 때 사용된 공개키에 대응되는 개인키로 서명하여 생성한다. 이 프로토콜은 기존에 제안된 바인딩 갱신 프로토콜과 다르게 하나의 메시지만으로 바인딩 갱신을 수행한다는 점에서 효율적이지만 바인딩 갱신 요청에 대한 응답은 어떤 형태로든지 필요하므로 논문의 주장과 달리 실제로는 최소 두 개의 메시지가 필요하다.

CAM은 크게 다음과 같은 문제점을 지니고 있다. 첫째, MN에서 메시지 서명 비용과 CN에서 이 서명을 검증하는 비용이 소요된다. 둘째, 일방향 인증만 제공한다. 즉, CN에 대한 인증은 제공하고 있지 않다.

CBID(Crypto-Based IDentifier) 프로토콜[8]은 다른 말로 SUCV(Statistically Unique and Cryptographically Verifiable identifier)[9] 프로토콜이라 하며, 프로토콜의 구성도는 그림 3과 같다. 이 프로토콜은 서비스 거부 공격을 완화하기 위해 퍼즐 개념을 도입하고 있다. 프로토콜 진행 메시지에 생략되어 있지만 이 과정에서 IPsec을 사용하기 위한 보안연관(SA, Security Association)을 교환할 수 있으며, 이 경우에 향후 바인딩 갱신은 IPsec을 사용할 수 있다. 그런데 이 프로토콜 역시 CAM과 마찬가지로 IPsec을 이용하지 않으면 MN은 CN을 인증할 수 없는 문제점을 가지고 있으며, 단기간 관계 형성을 하는 MN과 CN 사이에 IPsec의 사용은 현실적으로 어렵다.

CAM 프로토콜은 MN이 저전력과 제한된 계산능력을 가진 모바일 장치라는 점에 대한 고려가 없다. 반면에 이 프로토콜에서는 이 문제점을 보안하기 위해 확장 프로토콜을 제안하고 있다. 확장 프로토콜에서는 HA가 이동노드를 대신하여 지수연산과 같이 계산량이 많은 연산을 대신 처리해 준다. 확장 CBID 프로토콜은 기존 CGA 방식과 달리 MN의 공개키를 이용하여 CGA를 생성하지 않고, 서버의 공개키를 이용하여 CGA를 생성한다. 이를 위해 초기에 주소 설정 과정에서 HA로부터 주소 생성에 포함될 공개키를 받아야 한다. MN은 CN과 바인딩 갱신이 필요하면 HA에게 이를 요청한다. HA는 MN의 CGA 주소에 포함된 공개키에 대응되는 개인키를 이용하여 MN을 대신하여 CN과 기본 프로토콜을 수행하여 바인딩 갱신을 처리해준다.

Qiu 등이 제안한 ECBU(Extended Certificate-based Binding Update) 프로토콜[10]은 인증 센터로부터 발급 받은 인증서를 통해 노드를 인증하는

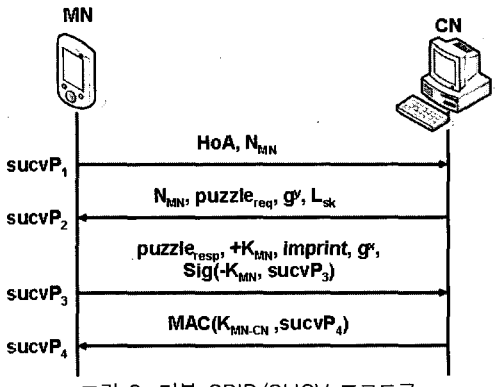


그림 3. 기본 CBID/SUCV 프로토콜

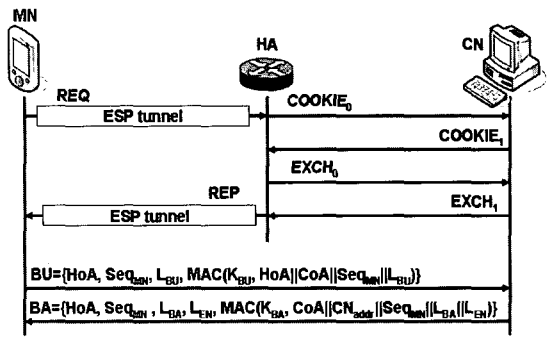


그림 4. ECBU 프로토콜

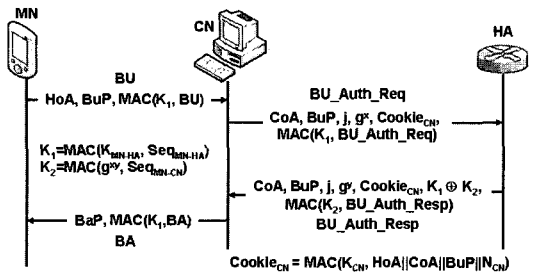


그림 5. 강현선과 박창섭의 프로토콜

방식을 사용하고 있다. 이 프로토콜은 확장 CBID 프로토콜과 같이 저전력의 MN을 고려해 HA가 프로토콜에 참가한다. 구체적인 프로토콜의 구성도는 그림 4와 같다. HA는 세션키 생성에 필요한 여러 연산(계산량이 많은 서명, DH에 필요한 지수 연산 등)을 MN을 대신해서 처리함으로써 MN의 계산 부담을 줄여주고 있다. 하지만 메시지가 수가 비교적 많다는 문제점이 있으며, CN의 부담이 많기 때문에 CN이 이동 가능한 노드이면 사용하기 어려운 프로토콜이다. ECBU는 이를 극복하기 위해 CN 역시 이동 가능한 노드인 경우에는 CN의 HA까지 활용하는 프로토콜을 같은 논문에서 제안하고 있다.

강현선과 박창섭이 제안한 프로토콜[11]은 MN의 계산량과 통신량을 줄이기 위해 기존 프로토콜과 다르게 그림 5와 같이 구성하고 있다. 이 프로토콜은 확장 CBID 프로토콜처럼 HA가 MN을 대신하여 공개키 연산을 수행한다. 하지만 MN이 HA에게 바인딩 갱신을 대신해 줄 것을 요청하는 형태가 아니라 CN이 바인딩 갱신 요청을 받으면 MN의 HA에게 이 요청의 유효성을 검증받는 형태로 구성되어 있다. 이 프로토콜에서 HA는 바인딩 갱신 메시지의 유효성을 확인하는 인증서버의 기능과 MN과 CN을 위한 키 분배 센터의 기능을 수행한다. 이 프로토콜도 CGA 방식의 주소를 사용하지만 일반적인 CGA 방식과 달리 MN의 공개키가 아닌 HA가 생성한 공개키를 이용하여 생성한다. 즉, MN은 주소에 포함된 공개키에 대응되는 개인키를 알지 못한다. 반대로 CN도 CGA 주소를 사용하는데, CN은 MN과 달리 자신의 공개키를 이용하여 생성한다.

이 프로토콜은 CGA를 사용하는 측면에 있어 다음과 같은 문제점이 있다. MN과 CN이 모두 CGA 방식의 주소를 사용하는데, 그 생성 방법이 서로 다르다. 따라서 CN이 고정노드가 아닌 이동 가능한 노드인 경우에는 현재의 프로토콜을 사용할 수 있다.

Ⅲ. 제안하는 프로토콜

본 논문에서 제안하는 프로토콜은 다음과 같은 가정을 한다.

- CN은 고정노드이며, IPsec을 지원하는 노드이다.
- MN과 HA 간에는 IPsec에 필요한 SA를 이미 형성하고 있고, 이것을 이용하여 MN은 HA와 바인딩 갱신을 완료한 상태이며, 이 SA를 이용하여 제안하는 프로토콜의 메시지를 교환한다.
- HA와 CN은 IPsec에 필요한 SA를 초기 바인딩 갱신 과정 이전에 형성하며, 이것을 이용하여 메시지를 교환한다.

3.1 바인딩 갱신 프로토콜

제안하는 바인딩 갱신 프로토콜은 초기 바인딩 갱신 과정과 차후 바인딩 갱신 과정으로 구분된다. 그림 6은 MN과 CN 사이의 초기 바인딩 갱신 프로토콜 진행 과정에 대해 보여주고 있다. 프로토콜에 대한 구체적인 설명은 다음과 같다.

3.2.1 최초 바인딩 갱신 프로토콜

메시지 1은 MN이 CN과 경로를 최적화하기 전에 티켓을 요청하기 위해 전송하는 메시지이다. 이 메시지는 IPsec ESP(Encryption Security Payload)을 이용하여 데이터를 안전하게 주고받는다[4]. 두 노드 사이에 이미 확립되어 있는 IPsec SA를 이용하여 메시지를 주고받기 때문에 각 노드에 대한 인증, 메시지 무결성, 주소 소유권에 대한 인증은 자동으로 제공된다. MN은 난스 N_{MN}을 생성하여 이것을 ESP의 페이로드 필드에 추가하여 HA에게 전송한다.

이 메시지를 수신한 HA는 SA에 해당하는 세션키로 ESP를 복호화 한다. 그 다음에 HA는 응답 메시지의 확인을 위한 난스 N_{HA}를 생성하여 IPsec

메시지 1	티켓 발행 요청 메시지			
IP헤더	소스주소	CoA	목적주소	HAaddr
ESP헤더	소스주소	HoA	목적주소	CNaddr
내 용	N_{MN}			

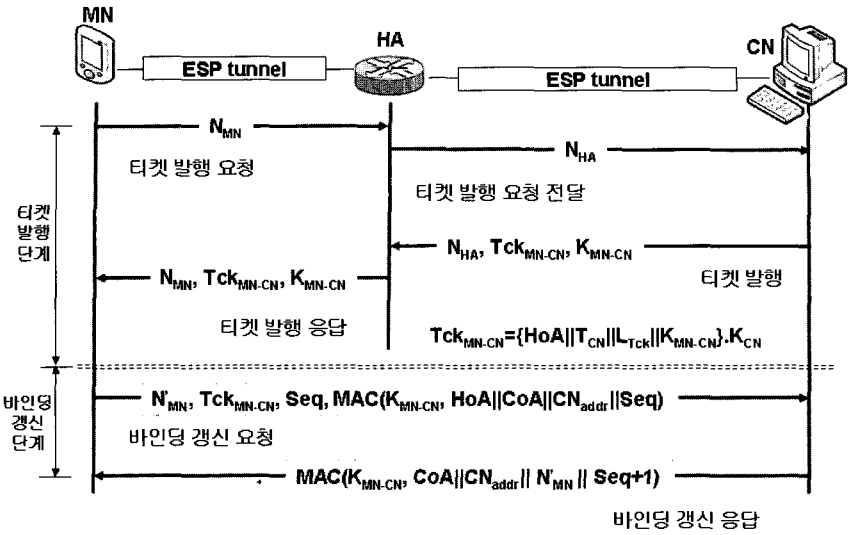


그림 6. 최초 바인딩 갱신 프로토콜

SA가 확립된 ESP 터널을 통해서 CN에게 전송한다. 이 과정에서 HA는 MN이 보낸 난스와 자신이 전송한 난스를 임시로 보관하여야 한다. 메시지 1과 2는 ESP 대신에 IPsec AH(Authentication Header)를 이용할 수도 있다.

메시지 2	티켓 발행 요청 전달 메시지			
IP헤더	소스주소	HAaddr	목적주소	CNaddr
ESP헤더	소스주소	HoA	목적주소	CNaddr
내 용	N_{HA}			

CN은 메시지 2를 수신하자마자 세션을 위한 적당한 SA가 존재하는지 확인하고 복호화에 실패할 경우 메시지를 버린다. 본 프로토콜은 이동 노드의 저전력과 한정된 계산 능력을 고려하여 공개키 연산을 전혀 사용하지 않는다. CN은 티켓키 K_{MN-CN}를 임의로 생성한 후에 MN을 위한 다음과 같은 티켓 Tck_{MN-CN}을 발행한다.

$$Tck_{MN-CN} = \{HoA||T_{CN}||L_{Tck}||K_{MN-CN}\}.K_{CN}$$

티켓은 MN의 HoA, 발행시간을 나타내는 타임스탬프 T_{CN}, 티켓의 수명 L_{Tck}, 티켓키 K_{MN-CN}로 구성되며, CN의 비밀키 K_{CN}으로 암호화된다. HoA가 포함된 이유는 티켓의 주인을 식별하기 위한 요소이고, 발행시간과 수명은 티켓의 유효기간을 나타낸다. MN은 차후 바인딩 갱신 때 이 티켓을 전송하여 바인딩 갱신을 요청한다. 따라서 CN은 자신이 발급한 티켓들을 저장할 필요가 없다. 단지 티켓을 발행할 때 사용된 비밀키만 안전하게 유지하면 된다. CN은 티켓, 티켓키, HA의 난스를 ESP 페이로드 필드에 추가하여 IPsec ESP 터널을 통해 HA에게 전달한다. 따라서 HA는 이 티켓이 MN이 요청한 CN이 발급한 것임을 확신할 수 있다.

메시지 3	티켓 발행 메시지			
IP헤더	소스주소	CNaddr	목적주소	HAaddr
ESP헤더	소스주소	CNaddr	목적주소	HoA
내 용	$N_{HA}, Tck_{MN-CN}, K_{MN-CN}$			

HA는 메시지 3을 수신한 후 자신의 난스를 확인한 다음에 MN의 난스로 바꾸어 이것을 MN에게 IPsec ESP를 이용하여 전송한다.

메시지 4	티켓 발행 응답 메시지			
IP헤더	소스주소	HAaddr	목적주소	CoA
ESP헤더	소스주소	CNaddr	목적주소	CoA
내 용	$N_{MN}, Tck_{MN-CN}, K_{MN-CN}$			

메시지 4를 수신한 MN은 암호화된 데이터를 복호화한 후에 난스 N_{MN}이 자신이 보낸 티켓 발행 요청 메시지에 포함한 것과 동일한지 검사한다. 그 다음에 티켓 Tck_{MN-CN}과 티켓키 K_{MN-CN}를 안전한 곳에 저장한다. MN이 HA를 신뢰하므로 수신한 티켓을 CN이 생성한 것이라고 확신할 수 있다.

메시지 5	바인딩 갱신 요청 메시지			
IP헤더	소스주소	CoA	목적주소	CNaddr
내 용	$N'_{MN}, Tck_{MN-CN}, Seq,$ $MAC(K_{MN-CN}, HoA\|\|CoA\|\|CN_{addr}\|\|Seq)$			

메시지 5는 CN과 라우팅을 최적화하여 두 노드 사이에 통신을 직접적으로 하기 위해 전송하는 메시지이다. MN은 수신한 티켓을 이용하여 MAC 값을 계산하여 자신이 티켓의 주인임을 입증한다. 여기서 일련번호 Seq는 티켓을 사용한 횟수를 나타내며, 사용할 때마다 하나씩 증가한다. CN은 이 메시지를 수신하면 먼저 티켓을 복호화하여 티켓의 유효기간을 확인한다. 그 다음에 티켓에 포함된 HoA, 헤더의 소스주소에 있는 CoA, 자신의 주소 CN_{addr}, 일련번호 Seq를 이용하여 MAC을 생성하여 수신된 MAC 값과 비교한다. 사용된 일련번호는 바인딩 갱신 캐쉬에 유지된다. 만약 이것이 첫 갱신이면 캐쉬에 MN을 위한 항이 없으므로 Seq는 0이어야 한다. 그 이후에 갱신은 바인딩 캐쉬에 유지된 일련번호보다 커야 한다. 자신이 생성한 MAC 값과 수신한 MAC 값이 일치하면 바인딩 갱신 캐쉬에 MN을 위한 바인딩 갱신 정보를 추가한다.

메시지 6	바인딩 갱신 응답 메시지			
IP헤더	소스주소	CNaddr	목적주소	CoA
내 용	$MAC(K_{MN-CN},$ $CoA\|\|CN_{addr}\|\|N'_{MN}\|\|Seq+1)$			

CN은 바인딩 갱신이 성공적으로 이루어졌다는 것을 알려주기 위해 메시지 6과 같은 응답메시지를 만들어 MN에게 전송한다. MN은 자신의 티켓키를 이용하여 이 MAC을 확인하고, 자신의 CN과 바인딩 갱신 정보를 바인딩 갱신 리스트에 추가한다.

차후 바인딩 갱신은 메시지 5와 6을 이용하여 처리한다. 즉, 메시지 1부터 4는 유효한 티켓을 MN이 가지는 있는 동안에는 사용되지 않는다. 만약 메시지 5를 수신한 CN이 티켓의 유효기간이 끝났음을 알게 되면 응답 메시지 대신에 실패 코드를 전달하여 준다. 이 경우 전체 과정을 다시 반복하여 티켓을 다시 발급받는다. 즉, 티켓의 유효기간이 만료된 후에 바인딩 갱신은 새 티켓을 발급받은 다음에 요청해야 한다. 또 MN이 이동하다 홈링크로 귀환한 경우에도 메시지 5와 메시지 6을 이용하여 바인딩 갱신 삭제를 요청을 한다. 즉, 메시지 5의 MAC을 확인할 때 티켓에 포함된 주소와 헤더의 소스주소가 일치하면 삭제요청을 인식한다.

Ⅳ. 분석

이 장에서는 제안된 프로토콜이 가지는 효율성과 안전성을 분석한다.

4.1 안전성 분석

안전성 분석을 위해 제안된 프로토콜에 대해 다음을 가정한다.

- IPsec을 이용한 메시지 교환은 안전하다. 즉, 프로토콜의 안전성을 분석할 때 IPsec 사용에 따른 보안 문제점은 고려하지 않는다.

4.1.1 모바일 IPv6 보안 요구사항

- 상호 인증(요청자와 응답자에 대한 인증): 티켓의 발급은 HA와 CN 사이에 IPsec을 이용한 상호인증이 확립된 이후에 이루어진다. HA와 CN 간에 IPsec SA가 확립하였다는 것은 둘 간에 안전하게 상호인증을 하였다는 것을 의미한다. 따라서 CN은 인증된 HA가 중계한 MN의 요청을 신뢰할 수 있다. 또한 MN은 HA 사이에 IPsec을 사용하므로 MN은 HA로부터 전달받은 티켓을 CN이 발급하였다고 신뢰할 수 있다. 티켓을 사용하기 위해서는 티켓키를 확보해야 한다. 티켓키는 티켓에 암호화되어 포함되어 있으며, MN에게 티켓키는 IPsec ESP 기능을 이용하여 CN으로부터 HA를 거쳐 전달되므로 제3자는 얻을 수 없다. 따라서 티겟을 이용한 바인딩 갱신 요청과 응답은 오직은 MN, HA, CN만 할 수 있다. 따라서 HA는 신뢰할 수 있으므로 MN과 CN 사이에 상호인증

이 제공된다.

- 갱신 정보의 무결성: MN의 바인딩 갱신 요청과 CN의 응답의 무결성은 MAC을 통해 제공된다.

- 요청자의 위치 인증(요청자의 주소 소유권 인증): CN은 MN이 외부 링크에서 획득한 CoA에 실제적으로 위치하고 있는지 확인할 수 있어야 한다. 이것이 확인되지 않을 경우 다른 노드의 주소를 이용하여 그 노드에 대한 폭격 공격을 할 수 있다. 하지만 제안하는 프로토콜은 CGA를 사용하는 프로토콜처럼 이웃이 사용하고 있는 주소로 바인딩 갱신하는 것을 막을 수 없다.

따라서 제안한 프로토콜은 상호인증 기능과 갱신 정보의 무결성을 제공하지만 요청자의 위치 인증은 제공하지 못한다. 현재 기술로는 요청자의 위치 인증은 CGA를 사용하지 않고는 제공하기가 어렵다. 하지만 본 논문은 공개키 연산의 사용을 배제하고 있으므로 요청자의 위치 인증을 위해 CGA의 사용을 고려하지 않고 있다.

서비스 거부 공격에 대한 강건성은 다른 프로토콜들에서 사용하는 여러 기법을 도입하여 제공할 수 있다. 예를 들어 공격자가 쓰레기 데이터를 MAC으로 위장하여 거짓의 바인딩 갱신 메시지를 지속적으로 CN에게 전송하여 서비스 거부 공격을 할 수 있다. 본 논문에서는 CN이 고정노드이므로 CN에 대한 자원 고갈 공격은 의미가 없다. 만약 이것이 문제가 되면 간단한 요청 메시지를 MN이 전송한 후에 CN으로부터 퍼즐을 받아 그 퍼즐에 대한 답을 티켓을 이용한 갱신 요청과 함께 보내도록 하여 공격을 완화시킬 수 있다.

4.2 효율성 분석

바인딩 갱신은 HA와 CN에게 MN이 새 주소를 통보하는 것을 말한다. 하지만 HA에게 새 주소를 통보하는 것은 IPsec을 통해 이루어지며, 이것에 대해서는 어떤 프로토콜에서도 이견이 없다. 반대로 CN에게 새 주소를 통보할 때에는 IPsec을 활용하는 경우도 있고 활용하지 않는 프로토콜도 있다. 하지만 HA에게 바인딩 갱신을 할 때는 IPsec을 활용해야 하므로 MN과 HA 사이에 IPsec을 사용하더라도 추가 비용이 소요된다고 말할 수 없다. 즉, 이 프로토콜을 위해 SA를 확립하는 것이 아니라 미리 확립된 여러 용도로 사용되고 있는 SA를 활용하기 때문이다. 따라서 효율성 분석에서 MN과 HA 사이에 IPsec 비용은 고려하지 않는다.

본 프로토콜은 HA와 CN 사이에도 IPsec을 활용한다. 기존 프로토콜 중 이 구간에서 IPsec을 활용하는 경우는 없다. 따라서 이 구간의 비용은 효율성 분석에서 고려되어야 한다. 하지만 이 구간의 비용도 갱신마다 소요되는 비용은 아니다. 전체 프로토콜을 다시 반복하더라도 다시 SA를 성립하지 않고 기존에 성립된 SA를 활용하기 때문이다. 따라서 MN과 CN 간에 통신 세션 중에 많은 바인딩 갱신이 이루어졌다면 이 부분도 비교에서 생략할 수 있다. 이와 같은 가정 하에 각 노드 입장에서 기존 프로토콜과 비교하면 다음과 같다.

- MN: 본 프로토콜에서는 IPsec의 사용을 고려하지 않으면 MN은 어떤 공개키 연산도 하지 않는다. 따라서 CGA를 사용하며 주소에 포함된 공개키에 대응되는 개인키로 서명하는 CAM, CBID와 비교하여 효율적이다. 또 MN의 연산량을 고려하여 HA가 대신 많은 연산을 수행하여 주는 ECBU나 강현선과 박창섭의 프로토콜이나 표준 프로토콜인 RR보다 효율성이 떨어진다고 볼 수 없다. 또 본 프로토콜은 티켓을 수신한 후에는 MAC을 통해 바인딩 갱신의 요청과 응답을 인증하기 때문에 이 비용은 CAM과 CBID보다는 저렴하며 기존 다른 프로토콜과는 차이가 없다. 하지만 티켓이 유효할 동안에는 전체 프로토콜을 반복하지 않고 메시지 5와 6만 사용하므로 항상 동일한 과정을 반복해야 하는 많은 다른 프로토콜들에 비해 매우 효율적이다.

- CN: MN과 마찬가지로 HA와 IPsec 확립 비용을 제외하면 CN은 어떤 공개키 연산도 사용하지 않는다. 따라서 공개키 연산방식으로 세션키들을 생성하는 CBID, ECBU, 강현선과 박창섭의 프로토콜에 비해 본 프로토콜은 효율적이다. 또한 서명을 확인해야 하는 CAM과 CBID보다 효율적이다.

- HA: 제안된 프로토콜에서 HA는 서로 신뢰하지 못하는 MN과 CN 사이에 신뢰를 형성시키주는

표 2. 각 프로토콜의 메시지 및 연산량 비교

		[1]	[7]	[8][9]		[10]	[11]	제안 프로토콜	
				BCBID	ECBID			초기 BU	차후 BU
메시지 수		8*	1	4	6	8	4	6*	2
MN 계산	전자서명	0	1	1	0	0	0	0	0
	지수계산	0	0	2	0	0	0	0	0
	대칭키	1	0	0	0	0	0	0	0
	MAC	2	0	1	0	2	2	2	2
CN 계산	전자서명	0	1	1	1	2	1	0	0
	지수계산	0	0	2	2	2	1	0	0
	대칭키	1	0	0	0	0	0	1**	1**
	MAC	2	0	1	1	6	3	2	2
HA 계산	전자서명	0	-	-	1	2	0	0	-
	지수계산	0	-	-	2	2	1	0	-
	대칭키	0	-	-	0	0	0	0	-
	MAC	0	-	-	1	4	2	0	-

* 터널링되어 전달되는 메시지는 2개의 메시로 계산한다.
** 티켓을 생성하고, 수신된 티켓을 복호화하는 비용을 나타내고 있다.

역할만 하고 있다. 따라서 MN을 대신하여 여러 연산을 수행하여 주는 ECBU나 강현선과 박창섭의 프로토콜에 비해 효율적이다.

기존 프로톨콜과 제안된 프로토콜의 연산량과 메시지 수는 표 2에 요약되어 있다.

V. 결 론

이 논문에서는 효율성을 향상시키고 전력 및 계산 능력에 제한이 있는 이동노드를 고려한 티켓 기반의 바인딩 갱신 프로토콜을 제안하였다. 제안된 프로토콜은 가정하는 IPsec의 사용을 제외하면 공개키 연산을 전혀 사용하지 않으며, 티켓을 이용하여 반복적으로 발생하는 바인딩 갱신을 매우 효율적으로 수행할 수 있다. 제안된 프로토콜은 CGA를 사용하지 않기 때문에 의탁주소에 대한 소유권을 확인할 수 없고, 이웃 노드 폭격 공격을 방어하기가 어렵다. 하지만 CGA를 사용하는 것이 비용 측면에서 수용하기 어렵다면 제안된 방식은 매우 효율적인 대안이라고 생각된다. 향후에는 CN도 이동이 가능한 노드인 경우를 고려할 예정이다.

참 고 문 헌

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, Jun. 2004.

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

[3] H. Soliman, *Mobile IPv6: Mobility in a Wireless Internet*, Addison Wesley, 2004.

[4] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," IETF RFC 3776, Jun. 2004.

[5] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration," IETF RFC 2462, Dec. 1998.

[6] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF RFC 3972, Mar. 2005.

[7] G. O'shea, M. Roe, "Child-proof Authentication for MIPv6 (CAM)," *ACM Computer Communication Review*, Vol 31, No. 2, pp. 4-8, Jul. 2001.

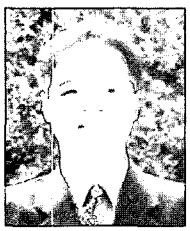
[8] G. Montenegro, C. Castelluccia, "Crypto-Based Identifiers (CBID): Concepts and Application," *ACM Trans. on*

Infomation and System Security, Vol. 7, No. 1, pp. 97-127, Feb. 2004.
[9] G. Montenegro, C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address," Proc. of the *Network and Distributed System Security (NDSS 2002)*, Feb. 2002.
[10] Y. Qiu, J. Zhou, F. Bao, "Protecting All Traffic Channels in Mobile IPv6 Network", *Proc. of the IEEE Wireless Communications and Networking Conf.*, pp. 160-165, Mar. 2004.
[11] 강현선, 박창섭, "Redirect 공격과 DoS 공격에 안전한 MIPv6 바인딩 갱신 프로토콜", *한국정보보호학회 논문집*, 제15권, 제5호, pp. 115-124, 2005.

〈著者紹介〉

구 중 두 (Jungdoo Koo) 학생회원
2002년 2월: 호원대학교 컴퓨터학부(학사)
2006년 8월: 한양대학교 컴퓨터공학과 (석사)
관심분야: 암호 프로토콜, 모바일 IPv6 보안

김 상 진 (Sangjin Kim) 종신회원
1995년 2월: 한양대학교 전자계산학과(학사)
1997년 2월: 한양대학교 전자계산학과(석사)
2002년 8월: 한양대학교 전자계산학과(박사)
2003년 3월~현재: 한국기술교육대학교 인터넷미디어공학부 조교수
관심분야: 암호기술 응용



오 희 국 (Heekuck Oh) 종신회원
1983년 2월: 한양대학교 전자공학과(학사)
1989년 2월: 아이오와주립대학교전자계산학과(석사)
1992년 2월: 아이오와주립대학교전자계산학과(박사)
1993년~1994년: 한국전자통신원 선임연구원
1994년~현재: 한양대학교 부교수
1998년~현재: 한국정보보호학회 이사
관심분야: 암호프로토콜, 네트워크 보안