情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

모바일 IPv6의 바인딩 갱신 기법에 관한 고찰

구 중 두*, 김 상 진**, 오 희 국*

요 약

바인딩 갱신 프로토콜은 이동노드가 홈 링크가 아닌 외부 링크로 이동했을 경우 기존 통신노드와 지속적인 연결을 유지하고 경로를 최적화하기 위한 목적으로 설계된 프로토콜이다. IETF의 모바일 IPv6 표준문서에는 RR(Return Routability) 기법을 이용해서 바인딩 갱신을 수행하도록 권장하고 있다. 하지만 RR 기법이 모바일 IPv6 보안 요구사항들을 전적으로 보장하지 않는다. 이 문제점을 해결하기 위해 IETF에서는 RR 기법에 IPsec을 이용하여 바인딩 갱신을 수행할 것을 권장하고 있다. 그러나 단기간의 연결 세션을 갖거나 저전력의 모바일 장치에 IPsec을 사용하는 것은 효율성이 떨어질 수 있다. 이 논문에서는 표준으로 제안된 RR 기법을 비롯하여, RR의 문제점을 해결하고자 제안된 여러 프로토콜을 살펴보고, 각 프로토콜의 안전성과 효율성을 분석한다.

Ⅰ. 서 론

유비쿼터스 환경에서 이동노드들은 물리적인 이동과 관계없이 기존에 통신하고 있던 노드와 끊임이 없이 그리고 수동적인 조작 없이 계속 통신을 할 수 있어야 한다. 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 이용하여 노드와 언제든지 통신할 수 있도록 해주어야 하는 상충되는 문제가 있다. 이 때 기존 응용에 영향을 주지 않고 이 문제를 해결해 주어야 바람직하다. 즉, 이것을 해결하는 메커니즘은 IP 계층보다 상위에 있는 계층에게는 투명하게 제공되어야 한다.

이 문제점을 해결하기 위해 모바일 IPv6가 등장하게 되었다. 모바일 IPv6는 IPv6 인터넷에서 노드들의 이동성을 보장하기 위한 IP 계층 프로토콜로서, IETF에서 표준화를 하고 있다. 모바일 IPv6에서 이동노드는 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[1]. 모바일 IPv6에서 이동노드는 외부 링크에 있을 때 자신을 대신하여 주는 홈 에이전트가 있다고 가정한다. 이동노드가 새로운 링크로 이동하여 새 의탁주소를 획득하게 되면, 이 주소를 자신의 홈 에이전트에 등록해야 한다. 이 등록을 통해 노드의 물리적인 위치와 상관없이 항상 다른 노드들은 이 노드의 홈주소를 이용하여 메시지를 전달할 수 있다. 이동노드가 홈 링크에 없을 때 도착된 메시지들은 홈 에이전트가 등록된 주소를 이용하여 전달하여 준다. 그런데 이 방식은 항상 모든 통신이 홈 에이전트를 통해 이루어지게 되므로 네트워크를 비효율적으로 사용하게 되는 결과를 초래한다. 이 문제를 해결하기 위해 모바일 IPv6에서는 홈 에이전트뿐만 아니라 대응노드에게도 새 의탁주소를 알려주어 홈 에이전트를 이용하지 않고 직접 통신을 할 수 있는 방법을 제공해 주고 있다. 이와 같이 홈 에이전트나 대응노드에게 새 의탁주소를 등록하는 과정을 "바인딩 갱신"이라고 한다.

IETF의 모바일 IPv6 표준에서는 RR 기법을 이용하여 바인딩 갱신을 수행하도록 권고하고 있다[1]. 그러나 바인딩 갱신 과정을 안전하게 수행하지 않으면

* 한양대학교 컴퓨터공학과 ({hkoh, jdkoo}@cse.hanyang.ac.kr)
** 한국기술교육대학교 인터넷미디어공학부 (sangjin@kut.ac.kr)

〔표 1〕 기존 바인딩 갱신 기법의 분류

	[1]	[4]	[5][6]	[7]	[8]	[9]
홈 에이전트 활용여부	△	×	○	○	○	○
대응노드의 이동성 고려여부	○	×	×	○	×	○
CGA 사용여부	×	○	○	×	○	×
공개키 사용여부	×	CGA 서명	CGA 서명 DH 키교환	DH 키교환	DH 키교환	×

서비스 거부(DoS, Denial-of-Service) 공격, 경로 변경(redirect) 공격, 이웃 폭격(neighbour bombing) 공격 등에 취약할 수 있다[2]. 따라서 바인딩 갱신은 다음과 같은 보안 요구 사항을 만족해야 한다.

- **요청자 인증**: 바인딩 갱신 메시지를 수신하는 노드는 반드시 요청자를 인증할 수 있어야 한다.
- **응답자 인증**: 바인딩 갱신을 요청하는 요청자는 응답자를 인증할 수 있어야 한다.
- **바인딩 갱신 정보의 무결성**: 바인딩 갱신 정보는 다른 공격자들로부터 보호되어야 한다.
- **요청자 위치 인증**: 응답자는 요청자가 현재 위치(의탁주소)에 존재하는지 검증할 수 있어야 한다.

RR 기법은 모바일 IPv6 보안 요구사항을 전적으로 만족하지 못하고 있다. 표준에 의하면, 이런 문제점을 극복하기 위해 RR기법에 IPsec을 사용하여 바인딩 갱신 과정을 안전하게 수행하도록 권장하고 있다[3]. 하지만 IPsec은 장기간 연결 관계가 형성되는 이동노드와 홈 에이전트 사이에는 효율적일 수 있으나 단기간 연결 관계가 형성될 수 있는 이동노드와 대응노드 간에 IPsec을 사용하는 것은 비효율적일 수 있다. 또한, IPsec의 내부 키 교환 프로토콜인 IKE를 수행하는데 드는 연산량이 적지 않기 때문에 저전력이며 한정된 계산량을 가진 통신 노드일 경우에는 부담이 될 수 있다. 따라서 IPsec을 사용하지 않고도 이동노드와 대응노드 간에 저렴한 비용으로 안전하게 바인딩 갱신을 수행하는 메커니즘이 요구되었다.

이 문제점을 해결하기 위해서 여러 프로토콜들이 제안되었다[4-9]. 이와 같은 프로토콜들은 다음과 같은 다양한 기준으로 분류할 수 있다. 첫째, 갱신 과정에서 홈 에이전트를 활용하는지 여부에 따라 분류할 수 있다. 둘째, 이동노드와 통신하고 있는 대응노드가 고정노드로만 한정하여 고려한 경우와 이동 가능한 경우까지 고려한 경우로 분류할 수 있다. 셋째, 암호학적으로 생성된 주소(CGA, Cryptographically Generated Address)[10]를 사용하는 방법과 그렇지 않은 방법으로 분류할 수 있다. 넷째, 공개키 연산을 사용하는 경우와 공개키 연산 없이 대칭키 연산과 MAC만을 사용하는 경우로 분류할 수 있다. 표 1은 이런 기준에 따라 기존 바인딩 갱신 기법들의 분류를 나타내고 있다. 각 기법들에 대해서는 2장에서 보다 자세히 설명한다.

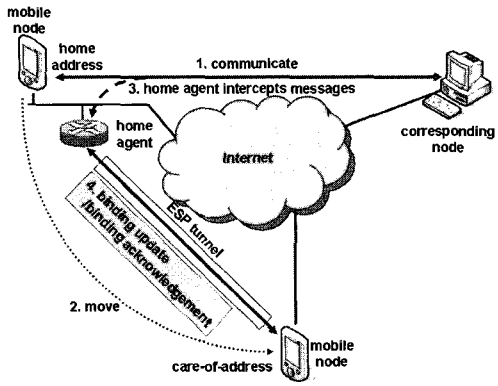
이 논문의 구성은 다음과 같다. 2장에서는 모바일 IPv6의 개요 및 기존 바인딩 갱신 프로토콜에 대해서 자세히 살펴본다. 3장에서는 모바일 IPv6를 안전하게 수행하기 위한 보안 요구사항과 이전 장에서 구체적으로 설명한 프로토콜들의 안전성 및 효율성에 대해 분석한다. 마지막으로 4장에서는 결론을 맺는다.

II. 모바일 IPv6

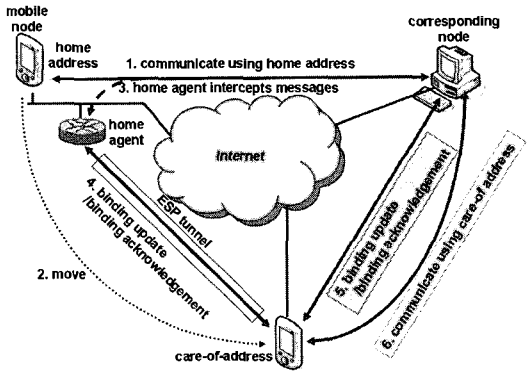
이 장에서는 모바일 IPv6의 개요 및 기존에 제안된 바인딩 갱신 프로토콜에 대해서 구체적으로 살펴본다.

2.1 모바일 IPv6의 개요

모바일 IPv6는 IPv6의 확장으로서 노드가 물리적으로 이동하여 사용하고 있는 기본 라우터가 변경되더라도 현재 진행 중인 세션을 계속 유지할 수 있도록 해주고, 이러한 변경을 모르는 다른 노드들이 이 노드에 접근할 수 있도록 해준다. 모바일 IPv6에서 이동노드는 노드의 현재 네트워크의 위치와 무관하게 변하지 않는 정적 주소인 홈주소와 이동노드가 현재 연결되어 있는 네트워크의 위치에 따라 변할 수 있는 동적 주소인 의탁주소를 갖는다. 이동노드가 홈주소를 갖는 이유는 자신과 통신하고자 하는 노드들이 이동노드의 실제 위치를 모르더라도 그 노드의 주소로 접근할 수 있도록 하기 위함이다.



〔그림 1〕 이동노드와 홈 에이전트 간의 바인딩 갱신



〔그림 2〕 경로 최적화를 이용한
이동노드와 대응노드 간의 바인딩 갱신

모바일 IPv6에서 노드들의 IP 주소 설정은 크게 비상태 자동 주소 설정 방법(stateless address autoconfiguration)[11]과 상태 주소 설정(stateful address configuration) 방법 중 하나를 이용한다. 전자의 방법은 라우터가 선전하는 네트워크의 프리픽스 정보와 자신의 독특한 인터페이스 식별자를 결합하여 IPv6 주소를 직접 생성하며, 후자는 DHCP (Dynamic Host Configuration Protocol)을 사용하여 주소를 설정한다.

이동노드가 외부 링크로 이동하여 기본 라우터가 변경될 경우, 노드는 기존 홈주소를 통해서 접근할 수 없다. 이 문제점을 해결하기 위해 이동노드는 외부 링크에 존재할 때 자신을 대신해 줄 수 있는 홈 에이전트를 사용한다. 이 에이전트는 노드가 홈 링크에 없을 때 이 노드의 홈주소로 전달된 메시지를 중계하여 준다. 이를 위해 이동노드는 외부 링크에서 새 의탁 주소를 획득할 때마다 자신의 홈 에이전트에 이를 등록하며, 이 과정을 바인딩 갱신이라 한다. 모바일 IPv6에서 홈 에이전트를 이용한 바인딩 갱신 과정은 그림 1과 같다. 외부 링크에 있는 이동노드가 또 다른 외부 링크로 이동하였을 경우에는 이를 빨리 감지하여 바인딩 갱신을 하여야 한다. 그 이유는 이동하여 갱신되기 전까지 외부 링크로 중계된 패킷들은 손실되기 때문이다.

이동성 보장을 위해 홈 에이전트를 이용할 경우 이동노드와 대응노드 간에 모든 패킷은 항상 홈 에이전트를 거쳐야 하는 삼각 라우팅 문제가 발생한다. 이 문제는 대응노드에서 이동노드로 전달되는 패킷뿐만 아니라 이동노드에서 대응노드로 보내지는 패킷 역시 홈 에이전트를 경유해야 한다. 그 이유는 현재 세션에서 사용하고 있는 소켓이 새 주소를 인식할 수 없기 때문이며, 이것을 역 터널링(reverse tunneling)이라 한다. 터널링이란 한 노드가 IPv6 패킷을 또 다른 IPv6 헤더에 캡슐화하는 것을 말하며, 가상 사설망을 구축할 때 많이 사용된다.

이동노드와 대응노드 사이에 모든 통신이 항상 홈 에이전트를 경유할 경우에는 다음과 같은 문제가 발생할 수 있다. 첫째, 통신 지연이 불가피하며, 둘째, 네트워크 대역폭을 비효율적으로 사용하게 되고, 셋째, 홈 에이전트가 단일 실패 점(single point of failure)이 될 수 있다. 이 문제점을 해결하기 위해 모바일 IPv6는 경로 최적화(route optimization) 모드를 제안하고 있다. 이 모드를 사용하면 이동노드는 대응노드와 최단 경로를 통해서 직접 통신할 수 있다.

경로 최적화를 위해 이동노드는 홈 에이전트뿐만 아니라 대응노드에게도 새 의탁주소를 알려주어야 한다. 이 과정은 현재 진행 중인 통신 세션과는 별도의 소켓을 형성하여 이루어진다. 홈 에이전트와 대응노드에서는 바인딩 갱신에 대한 정보를 저장하기 위해 바인딩 캐시를 유지하고, 이동노드에서는 바인딩 갱신 목록을 유지한다.

바인딩 갱신이 성립된 이후에 이동노드는 IPv6의 확장 헤더에 있는 홈주소 옵션(home address option) 필드에 홈주소를 기록하고 소스 주소를 의탁주소로 하여 모든 통신 메시지를 홈 에이전트 경유하지 않고 직접 대응노드로 전달한다. 대응노드의 IP층에서는 수신한 패킷에 홈주소 옵션이 설정되어 있으면 바인딩 캐시에 있는 정보와 헤더 있는 홈주소 및 의탁주소 정보가 일치하는지 확인한다. 확인이 되면 홈주소 옵션에 기록된 홈주소와 소스 주소를 바꾸어 상위 계층에 전달한다. 즉, 경로 최적화는 IP 층보다 상위

에 있는 층들에게는 투명하게 제공된다. 경로 최적화를 이용한 두 노드간의 바인딩 갱신 및 데이터 전송 과정은 그림 2와 같다.

이동노드는 모든 대응노드와 경로를 최적화할 필요는 없다. 특히, 단기간 연결 세션의 경우에 홈 에이전트를 경유하여 통신하여도 큰 문제가 되지 않으며, 이동노드의 위치에 따라서는 경로 최적화가 큰 효과가 없을 수 있다. 이 판단은 이동노드가 해야 하지만 이 판단이 쉽지 않으므로 보통 항상 경로 최적화를 하거나 전혀 하지 않는 방법을 선택한다. 또한, 모든 노드가 IPv6를 지원하지 않을 수 있기 때문에 이런 노드와는 경로 최적화를 할 수 없다.

바인딩 갱신 과정이 서론에서 언급한 보안 요구사항을 충족하지 않으면 다양한 공격이 가능하다. IETF에서는 이런 문제점을 해결하기 위해서 IPsec을 사용하도록 권고하고 있다. 하지만 IPsec은 장기간의 통신 세션을 갖거나 보안 연관(Security Association)을 맺는데 드는 비용이 부담되지 않는 경우에만 적합하다. 따라서 단기간의 통신 세션을 갖거나 저전력 및 한정된 계산능력을 갖은 모바일 장치에게는 적합하지 않다.

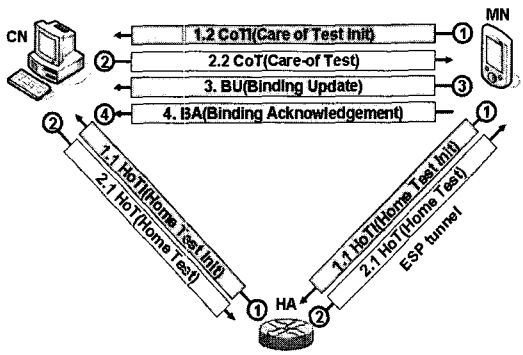
2.2 기존에 제안된 바인딩 갱신 프로토콜

바인딩 갱신 과정을 안전하게 수행하지 않았을 경우에 여러 공격이 가능하다. 이 절에서는 효율적이고 안전하게 바인딩 갱신을 하기 위해 제안된 대표적인 프로토콜들에 대해 구체적으로 살펴본다.

2.2.1 표기법

이 논문에서 설명하는 바인딩 갱신 프로토콜의 표기법은 다음과 같이 통일해서 기술한다. 이 때문에 각 프로토콜의 기술에 있어 생략된 부분도 있고, 원 논문과 다르게 표현되는 부분도 있을 수 있다.

- BU/BA: 바인딩 갱신/바인딩 응답 메시지
- MN/HA/CN: 이동노드/홈 에이전트/대응노드.
- HoA/CoA: 이동노드의 홈주소/의탁주소.
- A_{addr}: 노드 A의 주소.
- $+K_A/-K_A$: 노드 A의 공개키/개인키.
- K_A: 노드 A만이 알고 있는 대칭키.
- K_{A-B}: 노드 A와 B 사이에 공유된 대칭키.
- H(M): 메시지 M에 대한 해쉬 값.
- MAC(K,M): 비밀키 K를 이용한 메시지 M에 대한 MAC 값.
- T_A: 노드 A의 타임스탬프.
- L: 수명(lifetime).
- N_A: 노드 A의 난스(nonce).
- Seq_A: 노드 A의 일련번호.
- Sig(-K,M): 서명키 -K를 이용한 메시지 M에 대한 전자서명.
- $Cookie_A$: 노드 A의 쿠키.
- $M_1||M_2$: 메시지 M_1과 M_2의 비트 결합.



〔그림 3〕 RR 기법을 이용한 바인딩 갱신

2.2.2 RR 프로토콜

RR 기법은 이동노드가 대응노드에게 바인딩 갱신을 요청할 때 사용하도록 제안된 표준 프로토콜이다[1]. 이 기법은 대응노드가 이동노드의 바인딩 갱신 요청을 승인해주기 전에 이동노드의 HoA와 CoA를 사용하여 메시지를 수신할 수 있는지 확인할 수 있도록 해준다. 구체적인 프로토콜은 그림 3과 같다.

RR 기법은 MN이 HoTI(Home Test Init)와 CoTI(Care-of Test Init)로 이루어진 두 개의 독립적인 메시지를 보냄으로써 시작된다. HoTI 메시지의 소스 주소는 HoA이며, 이 메시지는 ESP 터널링 모드를 이용하여 HA를 통해 전달된다. 반면에 CoTI 메시지의 소스 주소는 CoA이며, HA를 경유하지 않고 직접 전달된다. 각 메시지에는 이동노드가 생성한 쿠키들이 포함되어 있다. 이 쿠키는 대응되는 회신 메시지를 식별하는 역할을 한다. 이 메시지를 수신한 CN은 각각의 주소를 이용하여 다음과 같은 두 개의 토큰을 생성한 후 HoTI와 CoTI의 응답 메시지로 $token_1$이 포함된 HoT와 $token_2$가 포함된 CoT 메시지를 전송한다.

$$token_1 = MAC(K_{CN}, HoA||N_{CN}^1||0)$$
$$token_2 = MAC(K_{CN}, CoA||N_{CN}^2||1)$$

이 메시지에는 HoTI와 CoTI에 전달된 쿠키가 각

각 포함된다. CN은 수신된 HoTI와 CoTI를 서로 연관시키지 않고 독립적으로 각각 처리한다. 이것은 연결 상태 정보를 유지하지 않기 위함이다.

MN은 HoT와 CoT를 모두 수신하였다는 것을 CN에게 입증하기 위해 두 메시지에 포함된 토큰을 이용하여 다음과 같이 키 K_{MN-CN}를 생성한다.

$$K_{MN-CN} = H(token_1||token_2)$$

MN은 이 키를 이용하여 다음과 같은 MAC을 계산한 다음,

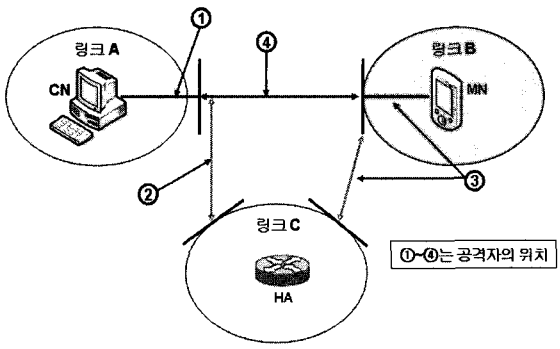
$$MAC(K_{MN-CN}, CoA||CN_{addr}||BU)$$

이 값을 BU 메시지에 포함하여 CN에게 전달한다. CN은 이 메시지에 있는 정보를 이용하여 MN과 동일한 키를 생성하여 이 메시지를 확인하고 응답 메시지를 보낸다.

MN이 새로운 CoA를 할당 받으면 보통 앞서 설명한 RR 과정을 전체를 수행해야 하지만(CoTI와 CoT만 사용할 수 있음), 외부 링크에 있던 MN이 홈 링크로 복귀했을 경우에는 CoA를 테스트 하는 CoTI와 CoT 메시지는 필요 없게 된다. 따라서 이 때에는 HoTI와 HoT 메시지만을 이용하여 CN의 바인딩 캐시에서 자신의 항을 삭제할 것을 요청하게 된다.

RR 기법은 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, 공격자 자신이 CN의 기본 라우터 행세를 하여 세션을 가로 챌 수 있다.

RR 기법에서 공격자의 위치에 따른 보안상 문제점은 그림 4와 같다. 공격자가 ①과 같이 대응노드와 같은 위치에 있을 경우에는 RR을 이용하지 않아도 다양한 공격이 가능하다. ②와 ④의 경로가 중첩되는 위치에 있으면 RR의 HoT와 CoT를 모두 접할 수 있으므로 다양한 공격이 가능하다. ②의 위치에 공격자 있을 경우에는 공격자가 CoT를 볼 수 없지만 HoT를 볼 수 있으므로 MN의 HoA를 이용하여 대신 CoTI

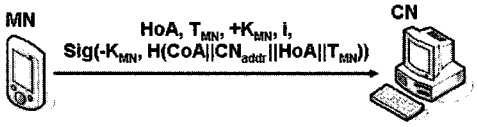


〔그림 4〕 RR에서 공격자 위치에 따른 공격

를 전달함으로써 바인딩 갱신을 요청할 수 있다. 공격자가 ③의 위치에 존재할 경우와 공격자가 ①과 ②의 위치일 때와의 차이점은 이 채널이 IPsec으로 보호된다는 것이다. 한 가지 가능한 공격은 MN의 CoA로 주소로 바인딩 갱신을 하여 자신의 데이터를 MN에게 보내는 폭격 공격을 할 수 있다는 것이다. 공격자가 ④의 위치에 있을 경우에는 HoT/HoTI를 볼 수 없으므로 RR을 활용한 추가적인 공격은 가능하지 않다.

공격자가 ②와 ④의 경로가 중첩되는 위치에 있으면 다양한 공격이 가능하지만 꼭 이 위치에 있어야만 가능한 것은 아니다. 예를 들어 이 위치에서 HoT, CoT를 이미 획득한 공격자는 다른 위치로 이동하여 공격할 수 있다. 이와 같은 문제점을 극복하기 위해 MN이 새 CoA를 할당받을 때마다 RR의 전체 절차를 매번 새롭게 할 수 있다. 하지만 이 방법은 키 갱신에 따른 통신 오버헤드 때문에 효율성이 떨어질 수 있다. 따라서 일정 유효기간을 두어서 그 기간 동안에는 CoTI/CoT만 사용하여 바인딩 갱신을 하는 방법이 더 바람직하다.

2.2.3 CAM 프로토콜



〔그림 5〕 CAM 프로토콜

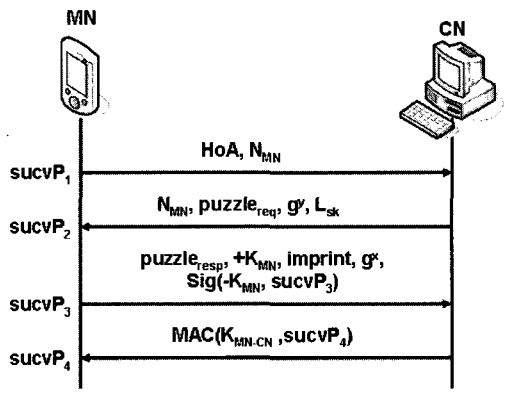
O'Shea와 Roe가 제안한 CAM(Child-proof Authentication for MIPv6) 프로토콜[4]은 CGA를 이용하여 바인딩 갱신을 수행한다. CGA 방식은 비상태 자동 주소 설정 방법으로 주소를 설정하는 방식이지만 기존의 방식과 달리 독특한 인터페이스 식별자 대신에 그 노드의 공개키를 해쉬한 값을 이용하여

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. CAM의 구체적인 프로토콜은 그림 5와 같다.

이 프로토콜에서 MN의 홈주소 HoA는 MN의 홈 링크의 프리픽스와 $H(+K_{MN}||i)$를 이용하여 생성된다. 여기서 i는 주소 충돌을 해결하기 위한 값이다. MN은 BU 메시지를 홈주소를 만들 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, MN의 HoA에 대한 인증만 제공된다. 즉, HoA에 포함된 공개키에 대응되는 개인키를 사용함으로써 HoA를 소유하고 있다는 것은 입증되지만 CoA를 소유하고 있다는 것은 입증되지 않는다. 셋째, 일방향 인증만 제공한다. 즉, CN에 대한 인증은 제공하고 있지 않다. 두 번째 문제는 논문에 언급되어 있지는 않지만 CoA도 CGA 방식으로 생성되었고, HoA와 동일한 공개키를 이용되었다면 이를 확인하여 해결할 수 있다.

2.2.4 CBID/SUCV 프로토콜



〔그림 6〕 기본 CBID/SUCV 프로토콜

Montenegro와 Castellucia가 제안한 CGA 방식을 사용하는 기본 CBID(Crypto-Based IDentifier) 프로토콜[5,6]은 수행과정은 그림 6과 같다. 이 프로토콜은 다른 말로 SUCV(Statistically Unique and Cryptographically Verifiable identifier) 프로토콜이라 한다.

MN은 CN에게 HoA, 난스 N_{MN} 등이 포함된 $sucvP_1$ 메시지를 전송하여 바인딩 갱신 요청을 한다. CN은 MN으로부터 수신한 난스, 서비스 거부 공격을 완화하기 위한 목적의 퍼즐, 세션키 생성을 위한 DH(Diffie-Hellman) 공개키 값, 세션키의 수명 L_{SK} 등이 포함된 $sucvP_2$ 메시지를 MN에게 전송한다. MN은 $sucvP_2$에서 자신의 난스를 확인한고, CN으로부터 수신한 DH 공개키 값, 난스, 전사 공격을 제한하기 위한 MN의 위치에 의존하는 64비트 크기의 imprint 값을 이용해서 다음과 같이 세션키 K_{MN-CN}를 생성한다.

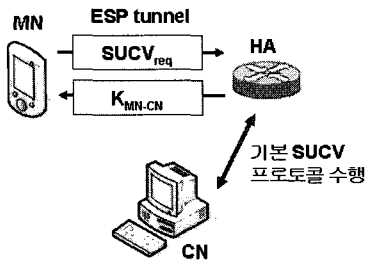
$$K = MAC(H(g^{xy}), N_{MN}||imprint)$$
$$K_{MN-CN}=MAC(K, g^{xy}||N_{MN}||imprint||0)$$

또한, 퍼즐에 대한 응답을 생성한다. 끝으로 HoA에 포함된 공개키 $+K_{MN}$에 대응되는 개인키를 이용하여 전체 메시지를 서명한 후에 CN에게 $sucvP_3$ 메시지를 전송한다. CN은 $sucvP_3$ 메시지를 수신하면 퍼즐에 대한 답, MN의 CGA 주소, 메시지에 포함된 서명을 확인한다. 그 다음 MN과 동일한 방법으로 세션키 K_{MN-CN}을 생성하여, 응답 메시지 sucvP4에 포함될 MAC 값을 계산하여 응답 메시지를 전달한다.

프로토콜 진행 메시지에 생략되어 있지만 이 과정에서 IPsec을 사용하기 위한 보안연관을 교환할 수 있으며, 이 경우에는 $sucvP_4$에 BA를 포함하여 IPsec을 이용하여 전달할 수 있다. 또한 향후 바인딩 갱신은 그림 6의 프로토콜 대신에 IPsec을 사용할 수 있다. 그런데 $sucvP_4$를 IPsec을 이용하여 전달하지 않으면 MN은 CN을 인증할 수 없으며, 누구나 CN 행세를 할 수 있다.

CAM 프로토콜은 MN이 저전력과 제한된 계산능력을 가진 모바일 장치라는 점에 대한 고려가 없다. 반면에 이 프로토콜에서는 이런 문제점을 보안하기 위해 확장 프로토콜을 제안하고 있다. 확장 프로토콜에서는 HA가 이동노드를 대신하여 지수연산과 같이 계산량이 많은 연산을 대신 처리해 준다. 구체적인 확장 CBID/SUCV 프로토콜은 그림 7과 같다.

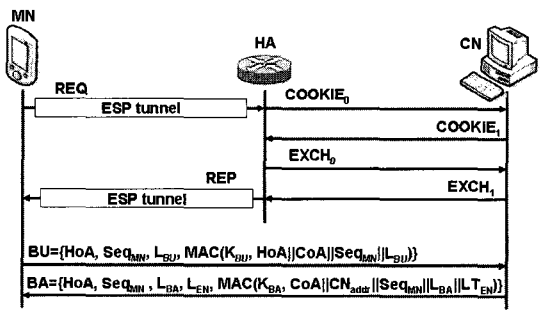
확장 CBID 프로토콜은 기존 CGA 방식과 달리



〔그림 7〕 확장 SUCV/CBID 프로토콜

이동노드의 공개키를 이용하여 CGA를 생성하지 않고, 서버의 공개키를 이용하여 CGA를 생성한다. 이를 위해 초기에 주소 설정 과정에서 홈 에이전트로부터 주소 생성에 포함될 공개키를 받아야 한다. 이동노드는 대응노드와 바인딩 갱신이 필요하면 HA에 이를 요청한다. HA는 이동노드의 CGA 주소에 포함된 공개키에 대응되는 개인키를 이용하여 이동노드를 대신하여 기본 프로토콜을 수행하여 바인딩 갱신을 처리해 준다.

2.2.5 ECBU 프로토콜



〔그림 8〕 ECBU 프로토콜

Qiu 등이 제안한 ECBU(Extended Certificated-based Binding Update) 프로토콜[7]은 인증 센터로부터 발급 받은 인증서를 통해 노드를 인증하는 방식을 사용하고 있다. 이 프로토콜은 확장 CBID 프로토콜과 같이 저전력의 MN를 고려해 HA가 프로토콜에 참가한다. HA는 세션키 생성에 필요한 여러 연산(계산량이 많은 서명, DH에 필요한 지수 연산 등)을 MN을 대신해서 처리해준다. 이렇게 함으로써, MN의 계산 부담을 줄여 준다. 구체적인 프로토콜의 수행 과정은 그림 8과 같다.

MN은 CN과 경로 최적화 과정을 수행하고자 할 때, HA에게 REQ 메시지를 전송한다. 이 메시지는 두 노드 사이의 안전한 ESP 터널을 통해 전송된다. 이 메시지를 수신한 HA는 자신과 CN 사이에 존재할 수 있는 서비스 거부 공격을 완화하기 위한 $COOKIE_0$과 $COOKIE_1$ 메시지를 주고받는다. 쿠키의 교환 이후 HA는 인증센터로부터 받은 인증서, 세션키 생성을 위한 DH 공개키 값 등이 포함된 $EXCH_0$ 메시지를 CN에게 전송한다. CN에서는 응답 메시지로 $EXCH_1$를 HA에게 전송한다. 이 두 메시지에는 서로를 인증하기 위한 서명이 포함되어 있다. 이런 과정이 끝나면, HA와 CN에서는 MN과 CN 사이에 사용할 세션키를 포함해서 기타 중요한 키들을 다음과 같이 생성한다.

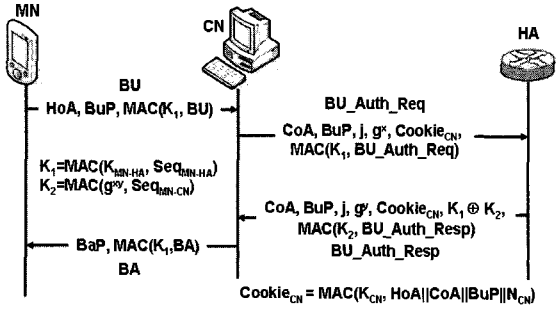
$$K = MAC(g^{xy}, N_1||N_2)$$
$$K_{BU}=MAC(K, N_1||N_2||0)$$
$$K_{BA}=MAC(K, N_1||N_2||1)$$
$$K_{EN}=MAC(K, N_1||N_2||2)$$

안전하게 키를 생성한 후, HA는 안전한 ESP 터널을 통해서 생성한 키를 MN에게 전송한다.

MN은 수신한 키를 이용하여 MAC 값을 생성하고 BU의 수명 및 재전송 공격을 방지하기 위해 시퀀스 넘버를 추가한 BU 메시지를 CN에게 전송한다. CN은 HA 사이에 생성한 세션키를 통해 MN에서 수신한 메시지를 검증한다. 검증 과정이 끝나면, CN은 자신의 바인딩 캐시에 MN의 HoA와 CoA에 대한 바인딩 정보를 저장한다. 또한, BA를 MN에게 전송한다.

이 프로토콜은 메시지가 수가 비교적 많다는 문제점이 있으며, 대응노드의 부담이 많기 때문에 대응노드가이동 가능한 노드이면 사용하기 어려운 프로토콜이다. ECBU는 이를 극복하기 위해 CN도 이동이 가능한 노드인 경우에는 CN의 홈에이전트까지 활용하는 프로토콜을 같은 논문에서 제안하고 있다.

2.2.6 강현선과 박창섭의 프로토콜



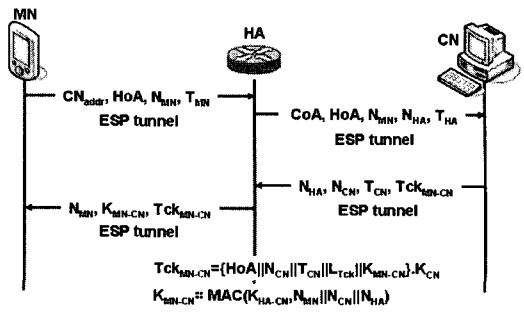
〔그림 9〕 강현선과 박창섭의 프로토콜

이 프로토콜[8]은 MN의 계산량과 통신량을 줄이기 위해 메시지가 교환되는 흐름을 기존 프로토콜과 다르게 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 세션키 분배센터의 기능을 수행한다. 이 프로토콜도 CGA 방식의 주소를 사용하지만 일반적인 CGA 방식과 달리 이동노드의 공개키가 아닌 HA가 생성한 공개키를 이용하여 생성한다. 즉, 이동노드는 주소에 포함된 공개키에 대응되는 개인키를 알지 못한다. 반대로 CN도 CGA 주소를 사용하는데, CN은 MN과 달리 자신의 공개키를 이용하여 생성한다. 이 프로토콜의 수행과정은 그림 9와 같다.

MN은 CN에게 BuP와 HA와 공유하고 있는 대칭키 K_{MN-HA}를 이용하여 생성한 MAC 값이 포함된 BU 메시지를 전송한다. BuP는 Seq_{MN-CN}와 L_{MN-CN}으로 구성된 BU 파라미터를 의미한다. 이 메시지를 수신한 CN은 BU 메시지를 인증하기 위해서 HA에게 수신한 BU 메시지를 전달한다. 이 때 DH 키 동의를 위해 자신의 주소에 포함된 공개키 g^x와 서비스 거부 공격을 완화하기 위한 쿠키를 함께 보낸다. 이 쿠키는 CN만이 알고 있는 대칭키 K_{CN}을 이용하여 생성된다. HA는 MN의 현재 CoA를 자신의 바인딩 캐시에서 확인하고, g^x를 이용하여 CN의 주소를 검증한다. 그 다음에 K_1을 생성하여 MN이 생성한 MAC 값을 확인한다. 모든 것이 확인되면 세션키 K_2를 계산하여 CN에게 응답 메시지를 전송한다.

응답 메시지를 수신한 CN은 먼저 메시지에 포함된 CoA, HoA, BuP가 쿠키 생성에 이용된 값과 일치하는지 검사한 후에, 일치하지 않을 경우 해당 메시지를 버린다. 그 다음에 g^y를 이용하여 MN의 CGA 주소를 확인하고, 세션키 K_2를 계산하여 MAC 값을 확인한다. 또한, 이 키를 이용하여 $K_1 \oplus K_2$로부터 K_1을 추출한다. 모든 것이 확인되면 CN은 바인딩 캐시에서 MN의 항을 생성 또는 갱신한 후 MN에게 응답 메시지를 전송한다.

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.



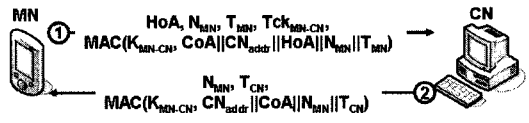
〔그림 10〕 티켓을 이용한 최초 바인딩 갱신 과정

2.2.7 티켓 기반 바인딩 갱신 프로토콜

티켓을 이용한 BU 프로토콜은 기존 프로토콜과 달리 매번 동일한 BU 과정을 수행하지 않고 티켓을 이용하여 첫 갱신 이후에는 보다 효율적으로 갱신할 수 있다[9]. 티켓은 CN만이 알고 있는 비밀키 K_{CN}으로 발급되며, 티켓에 MN을 인증하기 위한 세션키가 포함되어 있으므로 CN은 발급한 티켓들을 유지할 필요가 없다.

이 프로토콜은 MN과 HA, HA와 CN 간에는 IETF에서 권장하고 있는 IPsec을 사용한다. 저전력 MN이 IPsec을 사용하는 것이 비효율적일 수 있지만 HA와 MN은 지속적인 관계를 형성하고 있으므로 한 번 설정된 보안연관을 장기간 사용할 수 있다. 따라서 RR과 마찬가지로 HA와 MN 간에 IPsec의 사용은 정당하다. 또한, 이 프로토콜에서는 CN은 계산량과 전력 면에서 제한을 받지 않는 고정노드로 생각하고 있으므로 두 노드(HA와 CN) 사이의 IPsec 사용 역시 정당하다. 구체적인 프로토콜의 수행 과정은 그림 10과 같다.

MN은 HA 및 CN과 바인딩 갱신을 수행하기 위해 바인딩 갱신 요청 메시지를 안전한 ESP 터널을 통해 HA에게 전송한다. HA는 MN의 HoA와 CoA를 바인딩한 후에 이 정보를 바인딩 캐시에 저장한다. 그런 다음, MN에서 수신한 CoA, MN과 CN을 위한 세션키 생성에 필요한 파라미터를 포함한 티켓 발행 요청 메시지를 CN에게 전송한다. 이 메시지를 수신한 CN은 HA에서 수신한 파라미터와 자신의 파라미터를 이용해서 MN과 자신이 사용할 세션키를 생성한다. 그런 후에, 이동노드에게 발행해 줄 티켓을 생성한다. 티켓 안에는 MN의 HoA, 생성자의 난스 및



〔그림 11〕 차후 바인딩 갱신 과정

타임스탬프, 티켓의 수명, 두 노드 사이의 세션키가 포함되며 이런 파라미터들을 자신의 비밀키 K_{CN}으로 암호화한다. CN에서도 HA와 마찬가지로 바인딩 정보를 자신의 바인딩 캐시에 저장한다. CN은 발행한 티켓 및 바인딩 응답 메시지를 안전한 ESP 터널을 통해 HA에게 전송한다. 마지막으로, HA는 CN에서 수신한 티켓과 티켓에 포함된 세션키를 MN에게 전송한다. MN는 이 메시지를 확인하고 BU 과정을 마친다.

차후에, MN이 외부 링크로 이동했을 경우 또는 홈 링크로 되돌아 왔을 경우에는 그림 10의 과정을 반복하지 않고 티켓을 이용한 바인딩 갱신 메시지를 대응노드에게 직접 전송하여 바인딩 갱신을 요청한다. 구체적인 프로토콜은 그림 11과 같다.

CN이 이동 가능한 노드인 경우에는 그림 10에서 HA와 CN 사이에 추가적으로 CN의 HA가 참여하게 되며, 두 이동노드의 HA 간에는 IPsec을 사용한다.

2.2.8 Soliman의 프로토콜

Soliman은 바인딩 갱신 프로토콜의 모든 보안 요구사항을 가장 쉽게 충족시킬 수 있는 방법은 RR 기법과 CGA 방식을 결합하는 것이라고 주장하고 있다[12]. 즉, RR에서 이동노드가 HoT와 CoT를 수신한 다음에 BU 메시지에 원래와 같은 MAC 값뿐만 아니라 이동노드의 주소에 포함된 공개키에 대응되는 개인키로 BU 메시지를 서명한 값까지 포함하여 전달하는 방식을 주장하고 있다. 이렇게 프로토콜을 구성하면 RR의 문제점이 모두 해결되며, 추가적으로 주소에 대한 인증이 모두 명확해진다. 다만, BA를 통해 MN이 CN을 인증할 수 있도록 개선할 필요가 있다.

Ⅲ. 프로토콜의 안전성 및 효율성 분석

이 절에서는 먼저 바인딩 갱신 프로토콜의 특징에 대해 고찰을 한 다음에, 서비스 거부 공격, 경로 변경 공격, 이웃 폭격 공격에 대한 기존 바인딩 갱신 프로토콜의 취약성을 살펴본다. 그 후 기존 프로토콜의 바인딩 갱신 프로토콜의 보안 요구사항의 충족여부를 분석한다. 끝으로 라운드 수(메시지 수), 각 노드(MN, CN, HA)의 계산량을 통해 프로토콜들의 효율성을 분석한다.

3.1 바인딩 갱신 프로토콜의 특징

RR은 일반적인 경우에 수행하는 프로토콜, 수명이 끝났을 때 사용하는 프로토콜, MN이 홈 링크에 되돌아 왔을 때 사용하는 프로토콜을 구분하여 제시하고 있다. 하지만 RR을 개선하기 위해 제안된 많은 프로토콜들은 일반적인 경우에 사용되는 프로토콜만 제시되어 있고, 특수한 경우에 사용되는 프로토콜들은 제시되고 있지 않다.

대부분의 프로토콜은 대응노드를 이동을 하지 않는 고정노드로 간주하는 경우가 많다. 이동노드가 다른 이동노드와 통신하는 경우보다 어떤 고정된 서버와 통신하는 경우가 많을 것임에는 분명하다. 하지만 이동노드와 이동노드 간에 통신도 무시할 수 없기 때문에 이에 대한 고려가 필요하다. 하지만 RR, ECBU, 티켓 기반 프로토콜에서만 이를 고려하고 있다.

3.2 모바일 IPv6에서의 보안 요구사항

모바일 IPv6에서 안전하게 바인딩 갱신을 하기 위한 중요한 보안 요구사항은 다음과 같다. 이 요구사항들은 MN의 바인딩 갱신 요청의 상대방이 CN으로 가정하여 요구사항을 설명하고 있지만 요청의 상대방이 HA인 경우에도 동일하게 적용되어야 한다.

- □ **요청자의 인증**: HA와 CN은 MN의 바인딩 갱신의 요청을 승인하기 전에 주장된 HoA를 소유한 MN의 요청인지 확인할 수 있어야 한다. 이것이 확인되지 않으면 공격자는 정당한 MN으로 위장하여 바인딩 갱신을 하여 다양한 경로 변경 공격을 할 수 있다.
- □ **응답자의 인증**: MN은 바인딩 갱신 요청에 대한 응답 메시지가 자신이 현재 통신하고 있는 CN인지 확인할 수 있어야 한다. 이것이 확인되지 않으면 MN은 바인딩 갱신이 성공되었다고 착각할 수 있으며, 이 경우 경로 최적화를 통해 CN에게 직접 전달한 메시지들은 거부된다.
- □ **갱신 정보의 무결성**: MN이 바인딩 갱신 요청에서 주장하고 있는 CoA 정보에 대한 무결성을 제공해야 한다. 이것이 제공되지 않으면 공격자는 이것을 변경하여 다양한 공격을 할 수 있다.

□ **요청자의 위치 인증**: CN은 MN이 바인딩 갱신을 통해 주장하고 있는 자신의 현재 위치(의탁주소)에 실제로 존재하는지 검증할 수 있어야 한다. 이것이 확인되지 않으면 다른 노드의 주소를 이용하여 그 노드에 대한 폭격 공격을 할 수 있다.

3.3. 프로토콜의 다양한 공격에 대한 취약성 분석

이 절에서는 먼저 서비스 거부 공격, 경로 변경 공격, 이웃 폭격 공격에 대해 기존 기법들이 강건한지 여부를 분석한다.

□ 서비스 거부 공격

서비스 거부 공격은 적법한 사용자들이 프로토콜을 수행할 수 없도록 만드는 공격이다. 서비스 거부 공격은 크게 자원 소모 공격과 연결 소모 공격으로 나눌 수 있다. 전자의 경우는 서버의 계산 자원을 소모하기 위한 공격으로서 이동 노드와 같이 고정된 자원을 사용하지 않는 노드들을 대상으로 하는 공격이다. 후자의 경우는 서버가 허용할 수 있는 연결을 고갈하기 위한 공격이다. 서비스 거부 공격은 모든 통신 프로토콜에 대해 이루어질 수 있으므로 바인딩 갱신 프로토콜만이 꼭 해결해야할 문제는 아니다. 또한, 서비스 거부 공격을 완전하게 방지하는 것은 매우 어렵다. 더구나 이 공격은 경로 변경 공격이나 이웃 폭격 공격과는 달리 앞서 나열한 보안요구 사항이 충족되었다고 하여 해결할 수 있는 공격이 아니다.

서비스 거부 공격을 완화하기 위해 일반적으로 사용하는 기법은 다음과 같다. 첫째, 연결 상태 정보를 유지하는 버퍼의 고갈로 서비스가 거부되는 경우를 줄이기 위해 노드가 상태 정보를 유지할 필요가 없도록 프로토콜을 구성한다. 둘째, 불필요한 연결 상태 정보를 유지하는 경우를 줄이기 위해 통신 메시지들을 인증한다. 셋째, 공격자를 번거롭게 하기 위해 클라이언트 퍼즐을 사용한다. 두 번째 기법의 경우에는 메시지를 인증하기 위한 비용이 소요되므로 프로토콜이 진행됨에 따라 인증하는 비용을 점차적으로 늘리는 방법을 보통 사용한다.

기존에 제안된 바인딩 갱신 프로토콜들도 서비스 거부 공격에 대한 피해를 완화시키기 위해 이와 같은 방법들을 이용하고 있다. 예를 들어 RR은 CN이 RR 과정에서 연결 상태 정보를 유지할 필요가 없도록 하였으며, SUCV 프로토콜은 클라이언트 퍼즐을 사용하고 있다. 하지만 이들 기법을 사용하지 않는 프로토콜도 퍼즐이나 쿠키를 도입하는 것은 어렵지 않기 때문에 프로토콜들이 서비스 거부 공격에 취약하다고 말하는 것은 큰 의미가 없다. 다만, 가능하다면 연결 상태 정보를 유지할 필요가 없도록 프로토콜을 구성하는 것은 바람직하다. 예를 들어 티켓 기반 프로토콜에서 CN은 어떤 연결 상태 정보도 유지하지 않는다.

CAM과 같은 프로토콜은 전사서명을 통해 메시지가 인증되기 때문에 연결 상태 정보를 유지하는 버퍼의 고갈로 서비스가 거부되는 경우가 발생할 수 없지만 서명 확인 비용 때문에 자원 소모 공격에 취약하다. 하지만 CN이 보통 고정노드이므로 큰 문제가 된다고 할 수는 없다. SUCV도 이와 유사하게 전자서명을 사용하지만 퍼즐의 사용 때문에 CAM보다 서비스 거부 공격에 강건하다고 할 수 있다. CAM에도 퍼즐 사용을 추가할 수 있지만 이 경우에는 SUCV처럼 메시지 수가 더 필요하다.

□ 경로 변경 공격

경로 변경 공격은 바인딩 갱신을 조작하여 통신 메시지가 원래 목적지가 아닌 다른 목적지로 전달되도록 하는 공격이다. 이 공격은 바인딩 갱신의 요청자를 인증하지 않거나 바인딩 갱신 정보의 무결성이 보장되지 않으면 발생할 수 있는 공격이다. 경로 변경 공격은 세션을 훔치거나 서비스 거부 공격을 하기 위한 보조 공격 수단으로 활용될 수 있다. RR에서 최종 바인딩 갱신 메시지에 사용되는 대칭키는 HoT와 CoT 메시지를 도청할 수 있는 공격자이면 쉽게 얻을 수 있으므로 경로 변경 공격이 가능하다. 하지만 이 외에 기존 다른 기법들은 공격자가 적법한 노드의 바인딩 갱신 메시지를 위조하기가 어려우므로 경로 변경 공격이 성공하기가 어렵다. 특히, CGA 방식을 사용하는 기법들은 주소 생성에 사용된 공개키에 대응되는 개인키를 확보하지 않는 이상 공격하기가 어렵다. 티켓 기반 프로토콜 역시 티켓에 포함된 대칭키를 확보하지 않는 이상 공격하기가 어렵다.

□ 이웃 폭격 공격

이 공격은 경로 변경 공격의 한 종류라고 볼 수 있지만 일반적인 경로 변경 공격과 달리 공격자가 다른 노드의 바인딩 갱신 과정을 공격하여 경로를 변경하는 것이 아니라 적법한 노드가 자신의 의탁주소가 아닌

다른 노드의 의탁주소로 바인딩 갱신을 하여 특정 노드를 공격한다. 이 공격은 요청자에 대한 인증을 통해 해결할 수 없고, 요청자가 실제 주장하고 있는 의탁주소를 할당받고 있는지 확인해야 한다. 그러나 이것을 확인할 수 있는 방법이 아직까지 제시되고 있지는 않으며, 완벽하게 해결하기가 어려워 보인다. 다만, CGA 방식을 사용하는 경우에는 그 노드가 실제 주장하고 있는 CoA에 위치하고 있는지 확신할 수 없지만 특정 노드를 목표로 하는 이웃 폭격 공격은 어렵다. 노드들이 임의의 의탁주소를 언제든지 생성할 수 있지만 현재 다른 노드가 사용하고 있는 주소에 대한 소유권은 그 주소에 포함된 공개키에 대응되는 개인키를 알기 어렵기 때문에 가능하지 않다.

3.4. 프로토콜의 보안 요구사항 충족여부 분석

〔표 2〕 프로토콜의 보안 요구사항 충족여부

	상호인증		무결성	위치 확인
	MN	CN		
[1]	×	×	×	△
[4]	○	×	○	△
[5][6]	○	○*	○	△
[7]	○	○	○	△
[8]	○	○	○	△
[9]	○	○	○	△

*: IPsec을 활용할 경우에만 CN을 인증할 수 있다.
△: 모든 프로토콜에서 할당된 CoA에 실제로 MN이 있는지 확인할 수 없지만 이와 유사한 역할을 할 수 있는 장치들이 있다. 자세한 것은 이웃 폭격 공격부분 참조.

각 프로토콜의 보안 요구사항 충족여부는 표 2에 요약되어 있다. RR과 CAM을 제외하고는 요청자와 응답자 간에 상호인증을 제공하고 있다. 단, SUCV의 경우에 IPsec을 설정하는 경우에만 상호인증 된다고 볼 수 있다. ECBU, 강현선과 박창섭, 티켓기반 프로토콜 등은 HA의 도움을 받아 상호인증이 된다. 바인딩 갱신 요청을 서명하거나 안전하게 확립된 세션키를 암호화하여 전달한 경우에는 무결성이 보장된다고 볼 수 있다.

MN이 주장하고 있는 CoA에 실제 위치하고 있는지 안전하게 확인할 수 있는 방법은 없지만 모든 기법들이 이를 위한 어느 정도의 장치를 가지고 있다고 볼 수 있다. RR의 경우에는 CoT를 통해 MN이 의탁주소를 전달된 메시지에 대해 응답을 할 수 있는지 CN이 확인할 수 있도록 하고 있고, SUCV도 $sucvP_2$에 대한 응답 메시지인 $sucvP_3$를 통해 동일한 효과를 제공하고 있다. 하지만 CAM, ECBU, 강현선과 박창섭의 프로토콜, 티켓 기반 프로토콜은 주장된 의탁주소로 메시지를 수신할 수 있는지 직접 확인하고 있지 않다. 다만, CAM을 제외한 나머지 프로토콜은 HA가 자신에게 등록되어 있는 노드의 CoA 주소와 현재 주장하고 CoA 주소가 일치하는지 확인해주고 있으므로 유사한 효과를 제공하고 있다고 볼 수 있다.

3.5. 프로토콜의 효율성 분석

이 절에서는 프로토콜을 수행할 때 전송되는 총 메시지의 수 및 각 노드에서 처리하는 계산량을 토대로 프로토콜의 효율성을 분석한다. 전체적인 비교 분석은 표 3과 같다.

〔표 3〕 프로토콜의 효율성 분석

		[1]*	[4]	[5][6]*		[7]*	[8]	[9]*	
				CBID	ECBID			초기 BU	차후 BU
메시지 수		8**	1	4	6*	8	4	4	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	0	1
CN 계산	전자서명	0	1	1	1	2	1	1	0
	지수계산	0	0	2	2	2	1	0	0
	대칭키	1	0	0	0	0	0	0	0
	MAC	2	0	1	1	6	3	1	1
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	-

* : IPsec을 활용하는 프로토콜이며, IPsec 사용에 소요되는 비용은 이 표에 포함하지 않고 있다.
**: 터널링 되어 전달되는 메시지는 2개의 메시지로 계산하였다.

메시지 수 측면에서는 RR과 ECBU가 가장 많으며, CAM이 가장 적지만 CAM은 주장된 것과 달리 2개의 메시지가 필요하다. 메시지 수가 많다고 하여 각 참여자의 계산량이 비례하여 많이 소요되는 것은 아니다. RR 기법은 메시지의 수는 많지만 각 노드의 계산량은 다른 기법에 비해 적다. ECBID, ECBU, 강현선과 박창섭의 프로토콜, 티켓 기반 프로토콜들은 저전력인 이동노드를 고려하고 있지만 RR, CAM, CBID는 고려하지 않고 있다.

Ⅳ. 결 론

이 논문에서는 모바일 IPv6을 위한 바인딩 갱신 프로토콜의 최근 연구 동향을 분석하였다. 분석한 결과 앞으로의 연구방향은 CGA 주소 방식을 사용하는 경우와 사용하지 않는 경우로 나누어 진행되어야 할 것으로 보인다. CGA 주소 방식을 사용하는 경우에는 RR 기법에 BU 메시지와 BA 메시지를 서명하여 교환하는 방식보다는 모든 측면에서 우수해야 그 가치가 있을 것으로 판단된다. CGA 주소 방식을 사용한다는 것은 전자서명을 사용한다는 것을 의미하므로 이 비용이 허용되기 어렵다면 공개키 연산을 전혀 사용하지 않는 기법만이 가치가 있을 것으로 판단된다. 추가적으로 새로운 제안들은 일반적인 경우뿐만 아니라 이동노드가 홈으로 되돌아 온 경우처럼 특수한 경우에 사용될 프로토콜이 함께 제안되어야 하며, CN이 고정노드가 아닌 경우에도 효율적으로 사용할 수 있는 프로토콜도 제안되어야 한다.

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

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

[5] 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.

[6] G. Montenegro, C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address", ISOC Symp. on Network and Distributed System Security (NDSS 2002), Feb. 2002.

[7] Y. Qiu, J. Zhou, F. Bao, "Protecting All Traffic Channels in Mobile IPv6 Network", IEEE Wireless Communiations and Networking Conf., pp. 160-165, Mar. 2004.

[8] 강현선, 박창섭, "Redirect 공격과 DoS 공격에 안전한 MIPv6 바인딩 갱신 프로토콜", 한국정보보호학회 논문집, 제15권, 제5호, pp. 115-124, 2005년 10월.

[9] 구중두, 김상진, 오희국, "모바일 IPv6에서 확장된 티켓 기반의 바인딩 갱신 프로토콜", 한국정보보호학회 충청지부(CISC2005) 논문집, pp. 367-378, 2005년 10월.

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

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

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

〈著 者 紹 介〉

구 중 두 (Jungdoo Koo)
학생회원
2002년 2월: 호원대학교 컴퓨터학부(학사)
2004년 2월~현재: 한양대학교 컴퓨터공학과 석사 과정
관심분야: 정보보호, 센서네트워크 보안, 모바일 IPv6

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 (Oh heekuck)
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