Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.397

호스트 기반 분산형 이동성 관리 기술에서 안전하고 효과적인 바인딩 업데이트*

이 세 영,† 최 형 기,‡ 김 이 진
성균관대학교

Secure and Efficient Binding Updates in Host-Based Distributed Mobility Management*

Seyeong Lee,† Hyoung-Kee Choi,‡ EJin Kim
Sungkyunkwan University

요 약

모바일 트래픽이 급격히 증가함에 따라 모바일 기기가 끊김 없이 통신하기 위한 이동성 관리 기술로써 DMM (Distributed Mobility Management)이 제안되었다. DMM은 코어 네트워크에서 엣지 네트워크로 이동성 관리를 분산하여 낮은 지연으로 안정적인 바인딩 업데이트를 가능하게 한다. 그러나 DMM 시스템에는 여전히 네트워크상의 지연 문제와 세션에 대한 보안상의 문제가 존재한다. 본 논문에서는 기존 DMM 시스템에 존재하는 문제점을 지적하고, 이를 해결하기 위해 MN (Mobile Node)이 직접 인증에 참여하여 올바른 상호 인증이 이루어지는 새로운 프로토콜을 제안한다. 또한, 성능 분석을 통해 보안상의 향상뿐만 아니라 성능상의 향상이 존재함을 확인하였다.

ABSTRACT

As mobile traffic increases rapidly, DMM (Distributed Mobility Management) has been proposed as a mobility management technology for seamless communication of mobile devices as mobile traffic increases rapidly. the DMM distributes mobility management from the core network to the edge network, enabling stable binding updates with low latency. However, the DMM still have network delay and security problems for sessions. In this paper, we point out the problems existing in the DMM and propose a new protocol in which the MN (Mobile Node) directly participates in authentication and mutual authentication is correctly performed to solve this problem. We demonstrate not only security improvements but also performance improvements with performance analysis

Keywords: DMM (Distributed Mobility Management), CMM (Centralized Mobility Management), (BU) Binding Update, MIPv6 (Mobile IPv6), QR (Quadratic Residue)

I. 서 론

최근 모바일 기기의 수가 급격히 증가함에 따라 함께 증가할 것으로 예측되는 모바일 트래픽을 처리하기 위해 네트워크 성능을 향상시키기 위한 다양한 기술이 제안되고 있다. 새로운 기술은 지연이 최소화된 네트워크 트래픽을 전달할 수 있으며, 가용성, 신뢰성 및 응답이 보장되어 유비쿼터스 환경에 적합해야 한다는 조건들을 만족해야 한다.

모바일 네트워크에서 MN (Mobile Node)이 이동하여 새로운 액세스 네트워크에 연결하고자 할 경우, MN의 IP 주소는 새로운 네트워크 주소를 반영

Received(02. 28. 2017), Modified(04. 05. 2017), Accepted(04. 05. 2017)
* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.NRF-2014M3C4A7030648).
† 주저자, lsyvist@gmail.com
‡ 교신저자, meosery@skku.edu(Corresponding author)

하여 변경되어야 한다. 주소가 변경되어도 MN과 통신을 수행하는 개체 (entity)는 MN의 움직임에 따른 변화를 알아채지 못해야 하며, 세션이 지속되어야 한다. IETF (Internet Engineering Task Force)는 모바일 기기의 이동성 효율적인 처리를 위해 MIPv6 (Mobile IP version 6)[1], PMIPv6 (Proxy IPv6)[2] 등의 다양한 이동성 관리 기술을 제안한다.

이동성 관리 기술에 대한 초기 방식은 모두 MA (Mobile Anchor)가 코어 네트워크의 중앙에 위치하여 MN과 관련된 데이터 트래픽을 관리하는 CMM (Centralized Mobility Management) 방식의 중앙 집중형 구조를 기반으로 한다. CMM의 문제점은 엣지 네트워크에서 발생한 모든 데이터 트래픽이 코어 네트워크로 집중된다는 것이다. 이러한 방식의 라우팅은 코어 네트워크가 매우 큰 오버헤드를 부담해야 하며 대규모 네트워크 환경에서 이러한 오버헤드는 매우 빠르게 증가한다. DMM (Distributed Mobility Management)은 엣지 네트워크 근처에 MA를 배치하여 이러한 CMM의 한계를 극복하고자 제안되고 있다[3]. 단일 MA에게 집중되었던 이동성 관련 업무가 MN이 접속하는 여러 네트워크의 AR (Access Router)에게로 분산되어 코어 네트워크를 거치지 않고도 통신을 수행할 수 있다.

그러나 이러한 DMM에도 네트워크상의 지연 문제 및 보안상의 문제가 존재한다. MN의 IP 주소가 변경되면 통신 중에 있는 세션에 대한 하이재킹 (hijacking)을 방지하기 위해 MN의 움직임에 따른 인증을 수행하여야 한다. 현재 제안된 DMM은 CMM에서 사용하는 인증 프로토콜을 거의 그대로 상속받아 네트워크 단에서 발생하는 지연 문제 및 인증에 대한 문제를 그대로 가진다.

본 논문에서는 기존 DMM에 존재하는 문제점에 대해 언급한다. 추가적으로 기존 DMM의 문제를 해결하고, 시그널링 (signaling) 트래픽을 줄이고, 공격자의 악의적인 공격을 방어하기 위한 새로운 프로토콜을 제안한다. 제안하는 프로토콜은 기존 DMM과 달리 MN이 위치를 변경하여도 MN에 대한 세션 소유권 (session ownership)을 보장하며, 새로운 위치에서도 이전에 통신이 이루지고 있던 세션을 끊김 없이 사용할 수 있다. 이는 공격자가 세션 하이재킹 공격 등의 공격을 수행하여도 안전하게 동작한다.

또한, 단순히 보안상의 향상만이 이루어진 것이 아니라 네트워크상의 지연 또한 기존 DMM에 비해 제안하는 프로토콜이 향상되었음을 성능 분석을 통해 증명하였다.

본 논문의 구성은 다음과 같다. 제 2장에서는 이동성 관리 기술에 대해 설명하고, DMM이 어떤 방식으로 MN의 이동성을 업데이트하는지에 대해 설명한다. 제3 장에서는 안전하고 효과적인 MN의 이동성 업데이트를 위해 고려해야 할 공격 모델 및 보안 요구 사항에 대해 정의한다. 제 4장에서는 본 논문에서 새롭게 제안하는 프로토콜에 대해 자세히 설명한다. 제 5장에서는 제안된 프로토콜이 기존 DMM보다 보안상뿐만 아니라 통신비용 및 계산 지연 면에서도 효율적임을 성능 분석을 통해 증명한다. 제 6장에서는 이동성 관리를 안전하고 효과적으로 진행하기 위해 진행되었던 기존 연구에 대해 언급한다. 마지막으로 제 7장에서 결론을 맺는다.

II. 시스템 모델

2.1 이동성 관리 기술

MIPv6는 중앙의 MA가 등록된 모든 MN의 라우팅 및 이동 관련 정보를 관리하는 중앙 집중형 구조를 가진다. CMM에서는 HA (Home agent)가 MA의 역할을 수행하며, 다수의 MN을 관리하기 위해 코어 네트워크에 존재한다.

MA는 MN의 위치와 MN의 IP 주소를 연결하는 데이터베이스를 관리한다. MN과 통신하고자 하는 CN (Corresponding Node)은 MN과의 통신을 위해 반드시 MA를 거쳐야 하는데, 이는 MN의 위치에 따른 주소를 파악하기 위함이다.

MIPv6에서, MN이 위치를 변경하여 다른 네트워크에서 통신을 수행하여도 통신이 이루어지고 있는 CN과의 세션을 끊김 없이 지속적으로 유지할 수 있어야 한다. 이를 위해 MN은 두 종류의 주소를 할당받는다. 첫 번째 주소는 CN이 MN을 식별하기 위해 사용하는 HoA (Home of Address)로, MN이 이동해도 변경되지 않는 주소이다. 두 번째 주소는 MA가 MN의 현재 위치를 파악하기 위해 사용하는 CoA (Care of Address)로, MN의 위치에 따라 변경되는 임시 주소이다. MN이 새로운 네트워크에 방문함에 따라 CoA에 대한 변경이 이루어지면 MN은 즉시 MA와 CN에게 현재 자신의 위치와 새로운 CoA를 알려야 한다. 이를 위해, MIPv6는 MA와

CN 각각에 대해 바인딩 업데이트 (binding update)를 수행한다.

바인딩 업데이트는 2가지 목적을 위해 수행된다. 바인딩 업데이트는 MA에서 관리하는 MN의 CoA를 업테이트한다. 바인딩 업데이트 메시지를 변조하는 공격을 막기 위해 MN과 MA 간의 통신은 IPsec (IP security)로 설립된 안전한 채널을 통해 이루어진다. 또한, 바인딩 업데이트는 CN에게 새로운 CoA를 알려 MN이 새로운 위치에서도 CN과 여전히 통신이 가능하다는 것을 보장한다.

CMM은 구조적으로 성능상의 문제와 단일 장애점 문제를 가진다. MA는 코어 네트워크에 존재하므로 MA에게 과도한 트래픽이 집중되는 경우가 빈번하게 발생할 수 있다. 이 경우, 같은 MA를 공유하는 모든 MN의 통신에 문제가 발생할 수 있다. 또한, 항상 MA를 거치는 라우팅 경로는 최적의 경로가 아니므로 통신상의 지연이 발생한다. 두 가지 문제점으로 인해 기존 DMM은 네트워크에 연결된 MN과 그에 따른 트래픽이 증가하는 확장된 환경에 적합하지 않다.

CMM의 확장성 문제를 해결하기 위한 대체 수단으로 DMM이 제안되었다. DMM의 핵심은 중앙 HA에 집중된 MA의 역할 및 기능을 엣지 네트워크에 위치한 AR로 분산시켰다는 것이다. DMM은 MA의 역할을 다수의 AR이 나누어 수행하므로 CMM보다 확장된 환경에 적합하다. AR은 MN과 가까이에 위치하여 MN과 CN의 최적의 라우팅 경로를 형성한다. CMM에서의 HA 역할과 DMM에서 추가적으로 요구하는 기능을 수행하는 AR을 AMA (Access Mobility Anchor)라고 한다.

2.2 DMM에서의 바인딩 업데이트

DMM은 CMM과 마찬가지로 MN의 위치와 주소에 대한 정보를 MA에게 알리기 위해 바인딩 업데이트를 진행하며, 두 개의 주소 HoA, CoA를 사용한다. 그러나 CMM과 달리 DMM에서 MN은 경로 최적화를 위해 CN과의 바인딩 업데이트를 진행하지 않아도 되는데, 이는 이미 수평형 (flat) 구조를 구현함으로써 경로 최적화가 만족되었기 때문이다. CN은 MN의 CoA를 업데이트하지 않아도 MN의 HoA만으로 MN과의 통신을 수행할 수 있다.

Fig. 1은 DMM에서의 바인딩 업데이트 절차를 나타낸다. AMA_1 네트워크에서 처음으로 접속하는

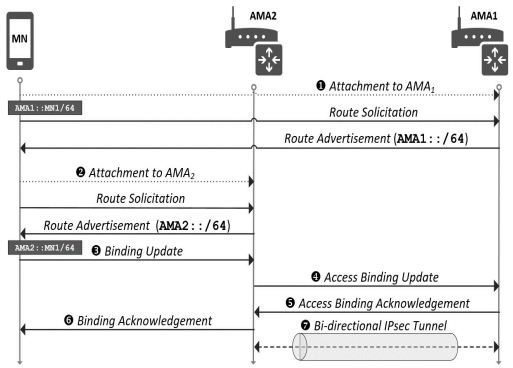

Fig. 1. Message flows of binding updates in DMM.

MN_1은 IP 주소로 AMA1::MN을 할당받는다. MN_1이 CN_1과 통신을 시작할 경우, 현재 세션의 서빙 (serving) AMA는 AMA_1이며, 통신에 대한 세션이 처음 발생한 네트워크의 AMA_1을 기존 (original) AMA로 취급한다. MN_1이 CN_1과의 통신 중에 두 번째 네트워크로 이동하면 MN_1은 새로운 AR인 AMA_2로부터 새로운 주소인 AMA2::MN을 부여받는다. MN_1은 AMA_2에게 기존 AMA와 관련된 정보와 MN_1이 이전 네트워크에서 사용한 IP 주소의 목록을 포함하는 BU (Binding Update) 메시지를 전송한다.

AMA_2는 ABU (Access Binding Update) 메시지를 기존 AMA에게 전송한다. 이 메시지는 MN_1의 새로운 위치의 전달과 기존 AMA와의 IPsec 터널을 설립을 위한 요청을 위한 것이다. 기존 AMA는 ABA (Access Binding Acknowledgment) 메시지를 통해 IPsec 터널을 설립한다. AMA_2는 MN_1에게 BA (Binding Acknowledgement) 메시지를 통해 응답한다. 이러한 과정을 통해 AMA_2 네트워크에서의 MN_1 등록 절차가 완료되며, 이와 동시에 MN_1은 서빙 AMA를 AMA_2로 변경한다. 이때 기존 AMA인 AMA_1과 서빙 AMA인 AMA_2 사이에는 IPsec 터널이 설립된다.

CN은 MN의 이동을 탐지하지 못한다. MN_1이 이동을 알아채지 못하는 CN_1은 MN_1과의 통신을 위해 AMA1::MN을 목적지로 하여 전송하고자 하는 데이터 패킷를 전송한다. CN_1이 전송한 패킷을 수신한 AMA_1은 바인딩 캐시를 탐색하여 MN_1이

AMA_2의 네트워크에 위치해 있음을 확인하고, IPsec 터널을 통해 CN_1이 전송한 데이터 패킷을 AMA_2에게 전송한다. AMA_2는 바인딩 캐시를 탐색하여 MN_1이 자신의 네트워크에 위치해 있음을 확인하고 CN_1이 전송한 데이터 패킷을 MN_1에게 전송한다. MN_1이 CN_1에게 전송한 데이터 패킷은 같은 경로에서 순서만 뒤집어진 형태로 전달된다.

MN_1이 두 번째 네트워크에서 CN_2와 새로운 통신을 시작할 때, MN_1은 두 번째 네트워크에서의 IP 주소로 AMA2::MN을 사용한다. CN_2와의 통신에서 기존 AMA는 현재 AR인 AMA_2이다. MN_1이 세 번째 네트워크로 이동할 경우 바인딩 업데이트 절차는 Fig. 1.과 유사하게 진행된다. MN_1의 서빙 AMA는 AMA_3으로 변경되며, AMA_3은 CN_1과의 통신을 끊김 없이 유지하기 위해 AMA_1과의 IPsec 터널을, CN_2과의 통신을 유지하기 위해 AMA_2와의 IPsec 터널을 설립한다. 이후, AMA_1은 CN_1과의 통신을 위해 맺었던 AMA_2와의 IPsec 터널을 해제한다.

III. 시스템 설계 목표

안전한 DMM 시스템을 설계하는 과정에서 고려해야할 보안상의 요구 사항이 몇 가지 존재한다. 이러한 요구 사항들은 현실적인 구현상의 문제나 성능상의 문제를 고려한 것이다.

3.1 공격 모델

DMM에서는 기존의 보안 메커니즘을 사용하여 바인딩 업데이트 메시지의 조작 또는 세션의 소유권에 대한 취약점을 극복하고 있다.

IPsec은 두 노드가 서로를 인증한 후, IKEv2 (Internet Key Exchange version 2)를 사용하여 키를 공유함으로써 두 노드 사이에 안전한 터널을 설립한다. IPsec 터널은 서빙 AMA와 기존 AMA 사이의 라우팅 경로를 지나는 패킷을 보호하기 위해 사용된다. 또한, 대부분의 엣지 네트워크는 외부에서 접속하고자 하는 기기에 대해 링크 계층 프로토콜에 따라 성립되는 적절한 보안 후에만 자신의 네트워크에 접속할 수 있는 권한을 부여한다. 즉, MN과 서빙 AMA 사이의 라우팅 경로는 안전한 채널이다.

IPsec과 링크 계층 보안이 적용되어 있음에도 DMM에서의 바인딩 업데이트 과정에는 여전히 MN과 기존 AMA에 관련된 보안상의 문제점이 존재한다. 이는 DMM의 보안 모델이 MN과 AMA를 모두 고려한 하나의 보안 메커니즘이 아닌 MN과 AMA에 대해 개별적인 보안 메커니즘을 적용하는 과정에서 발생한다. 통합된 보안 모델 부족은 두 종류의 보안상 위협을 야기한다.

첫째로, 통신이 이루어지고 있는 세션에 대한 세션 하이재킹 공격의 위험성이 존재한다. IPv6에서의 IP 주소는 주로 현재 속해있는 네트워크 주소와 MN의 MAC (Medium Access Control)의 조합으로 구성되기 때문에, 공격자는 특정 네트워크에서 비교적 공격 대상이 되는 MN의 IP 주소를 쉽게 알아낼 수 있다. 특정 네트워크에서 공격 대상 MN의 IP 주소를 알아낸 공격자가 새로운 네트워크에서 MN의 새로운 IP 주소로 바인딩 업데이트를 수행할 경우, 기존 AMA는 MN의 위치가 변경되었다고 인식하여 기존에 통신이 이루어지고 있는 세션에 대한 패킷을 새로운 네트워크의 AMA로 전송한다. 즉, 공격자는 MN으로 위장하여 통신이 이루어지고 있는 세션을 탈취할 수 있다. 이는 기존 AMA가 MN의 세션 소유권에 대한 인증을 수행하지 않기 때문이다.

두 번째로, DoS (Denial-of-Service) 공격인 N-점프 (N-jump) 공격에 취약하다. MN은 통신이 이루어지고 있는 모든 세션에 대한 IP 주소 목록을 유지한다. 이는 이전에 방문한 N개의 네트워크 각각에 대해 진행 중인 세션이 하나라도 존재할 경우, N개의 IP 주소를 모두 저장하고 있다는 것을 의미한다. MN은 N개의 서로 다른 세션을 지속하기 위해 서빙 AMA와 N개의 기존 AMA 사이에 N개의 IPsec 터널을 유지한다.

여러 세션이 활성화될 경우, 각 세션이 사용하는 IP 주소를 유지하기 위한 저장소와 세션을 처리하기 위한 오버헤드를 이용하여 공격을 수행할 수 있다. 공격자는 MN으로 위장하여 통신이 이루어지고 있는 세션에 대한 N개의 기존 AMA 및 해당 세션에서 사용한 IP 주소에 대한 정보를 포함하는 바인딩 업데이트 메시지를 AR에게 전송한다. 서빙 AMA는 N개의 세션에 대한 기존 AMA에게 MN의 위치가 서빙 AMA의 네트워크로 변경됨을 알린다. 서빙 AMA와 N개의 기존 AMA 사이의 IPsec 터널이 재설립되며, 이전 서빙 AMA에서 유지되던 MN에 대한 IPsec 터널은 해제된다.

공격자가 간단히 만들어낸 위조된 바인딩 업데이트 메시지의 양에 따라, 서빙 AMA와 해당 네트워크에 부과되는 오버헤드가 비례하여 증가한다. 이 공격은 모바일 트래픽과 MA의 역할이 여러 MA에게 분산되어 있어 바인딩 업데이트 메시지에 대한 유효성을 검증하기가 어렵다는 문제점에 기초한다. AR은 물리적 공격에 취약한 엣지 네트워크에 위치하므로 공격자는 쉽게 중간자 공격 (man-in-the-middle attack)을 적용할 수 있다.

3.2 보안 요구사항

DMM의 바인딩 업데이트 절차에는 보안상의 문제를 야기하는 세 가지 취약점이 존재한다.

- 세션 소유권 (session ownership): 서빙 AMA의 변경에 대한 요청에 대해 해당 요청이 기존에 통신이 이루어지고 있는 세션에 참여하던 MN으로부터의 요청인지에 대한 확인이 불가능하다.
- MN의 인증에 대한 적극적 참여: MN과 기존 AMA가 바인딩 업데이트 과정에서 보안 매개변수를 협상하기 위해 직접 통신하는 것이 안전하다. 그러나 DMM에서는 MN이 서빙 AMA에게 협상에 대한 권한을 위임하여 인증이 수행되므로 기존 AMA와 MN 간의 안전한 채널이 형성되지 않는다.
- 위치에 따른 도달 가능성: 기본적으로 IP는 이동성을 고려하지 않고 설계된 프로토콜이므로 IP 주소와 패킷의 송신자에 대한 연결이 보장되지 않는다. 이것은 DMM에서 공격자가 원하는 위치로 MN의 위치를 조작할 수 있다는 취약점을 야기한다.

IV. 제안하는 프로토콜

제안하는 프로토콜은 정보 등록 절차와 정보 검증 절차, 두 단계로 구성된다. 이 프로토콜은 적은 오버헤드로 바인딩 업데이트 절차를 진행하기 위해 비용이 많이 발생하는 IPsec 터널을 제거하였다. 비밀키를 안전한 방식으로 공유하기 위해 이차잉여 문제 (quadratic residue problem)[4]를 도입하였으며, 이차잉여에서 고유한 제곱근을 빠르게 찾아내기 위해 라빈 공개키 암호화 (Rabin public key encryption)[5]를 사용한다.

4.1 이차잉여 문제

일반적으로, 암호학에서 비대칭키를 사용함에 따라 발생하는 계산에 대한 비용은 그 암호 시스템을 사용하는 기술의 성능에 영향을 끼칠 수 있다. 예를 들어, RSA는 암호화와 복호화를 위해 지수 연산을 수행하는데, 이로 인해 RSA의 암호화 및 복호화는 상당한 계산 비용을 소모한다. 디피 헬만 키 교환 (Diffie-Hellman key exchange) 방식 또한 세션키를 생성하기 위해 지수 연산을 수행해야 한다. 반면에, 이차 잉여 문제는 단순히 $\bmod n$ 상에서의 제곱 연산을 수행함에 따라 발생하는 문제로, 이는 지수 연산에 비해 계산 비용이 적게 소모됨에도 암호학적으로 충분히 해결하기 어려운 문제이다.

$r^2 \equiv Q \pmod n$을 만족하는 $r \in Z_n$이 존재할 경우, $Q \in Z_n$는 $\bmod n$ 상에서의 이차잉여 (quadratic residue)이다. 만족하는 r이 존재하지 않을 경우, Q는 $\bmod n$ 상에서의 이차 비잉여 (quadratic nonresidue)이다. 이차잉여 문제란 임의의 정수 $a \in Z_n$가 $\bmod n$ 상에서 이차잉여인지 판단하는 문제를 말한다.

소수 p와 q에 대해 $n = p \cdot q$이며 $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$를 만족할 경우, $\bmod n$ 상에서의 모든 이차잉여는 네 개의 제곱근으로 가진다. p와 q를 알고 있는 경우, 이차잉여 $a \equiv r^2 \bmod n$의 제곱근을 중국인의 나머지 정리 (Chinese remainder theorem)를 이용하여 쉽게 구해낼 수 있다.

중국인 나머지 정리에 의해 $a \equiv r_p^2 \bmod n$에서 $a \equiv r_q^2 \bmod n$와 $a \equiv r^2 \bmod n$을 도출해낼 수 있다. r_p와 r_q는 각각 $\bmod p$와 $\bmod q$ 상에서 이차잉여의 제곱근이다. 이차잉여 a는 $\bmod p$ 상에서 두 개의 제곱근 (r_{p1}, r_{p2})과 $\bmod q$ 상에서 두 개의 제곱근 (r_{q1}, r_{q2})을 가진다. 오일러 정리 (Euler's criterion)를 통해 수식 (1)을 도출해 낼 수 있으며, 수식 (2-1), (2-2)과 같이 이차잉여 a에 대한 네 개의 제곱근을 구할 수 있다.

$$(\pm a^{(p+1)/4})^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \cdot a \equiv a \bmod p \quad where\ a^{(p-1)/2} \equiv 1 \bmod p \tag{1}$$

$$r_p \equiv \pm a^{(p+1)/4} \bmod p \tag{2-1}$$

$$r_q \equiv \pm a^{(p+1)/4} \bmod q \tag{2-2}$$

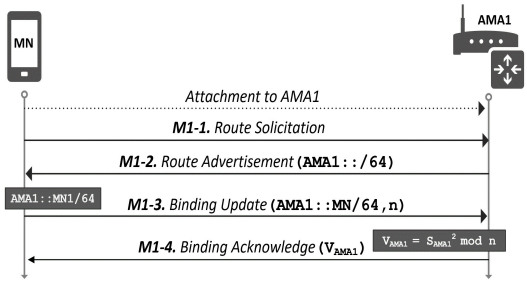

Fig. 2. Message flows in first phase

큰 소수 p와 q를 알지 못하는 경우, 인수 분해의 어려움에 의해 제곱근을 구하는 것은 어려운 문제이다. 이차잉여의 제곱근을 찾아내는 것에 대한 어려움은 라빈 공개키 암호화를 포함한 많은 암호화 시스템에서 사용되고 있다.

라빈 공개키 암호화 시스템에서 개인키 (p,q)를 통해 공개키 $n=p \cdot q$을 생성한다. 메시지 M은 $C \equiv M^2 \bmod n$으로 암호화를 수행한다. 암호문 C는 $\bmod n$ 상에서 평문 M의 이차잉여이다. 복호화는 암호문의 제곱근을 구하는 방식으로 이루어진다. 결과적으로 네 개의 제곱근을 구해낼 수 있다. 네 개의 평문 중 올바른 평문을 결정하기 위해 제곱근에는 사전에 결정된 불필요한 값들이 포함되어 있다. 라빈 시스템에서 암호화는 단순히 하나의 모듈러에 대한 제곱만 수행하므로 효과적이다. 복호화의 경우, 암호화보다 오랜 시간이 소요되지만, RSA나 디피 헬만 키 교환 방식과 같은 비대칭키 암호 시스템에 비해 적은 비용을 소모함에도 암호학적으로 안전한 강력한 암호 시스템이다.

4.2 단계 1: 정보 등록 절차

정보를 등록하기 위한 첫 번째 단계는 세션이 시작하는 순간부터 수행된다. 이 단계는 MN과 기존 AMA 사이의 세션을 위한 비밀값을 공유하기 위한 것이다. Fig. 2는 첫 번째 단계에서 교환하는 4개의 메시지를 나타낸다.

M1-1, M1-2: AMA_1의 네트워크에 연결을 위해 MN은 AMA_1과 RS (Router Solicitation) 메시지와 RA (Router Advertisement) 메시지를 통해 해당 네트워크에서의 주소 AMA1::MN/64를 할당받는다.

M1-3: Fig. 2와 같이, MN은 기존 AMA인 AMA_1에게 IP 주소와 홀수 소수인 $n=p \cdot q$를 포함하는 BU 메시지를 전송한다. 이때, p와 q는 MN이 생성하여 비밀리에 보관하는 값이다.

M1-4: AMA_1은 이후에 MN이 다른 네트워크에서 바인딩 업데이트 절차를 수행할 때의 MN이 현재 정보 등록 절차를 수행하는 MN과 동일함을 보장하기 위해 수식 (3)의 V_{AMA1}를 MN에게 전송한다. $S_{AMA1}(1 < S_{AMA1} < n)$은 n과 서로소로 AMA_1이 비밀리에 보관하는 값이며, V_{AMA1}은 $\bmod n$ 상에서의 이차잉여이다.

$$V_{AMA1} \equiv S_{AMA1}^2 \bmod n \tag{3}$$

BA 메시지를 수신한 MN은 $\bmod n$ 상에서의 이차잉여인 V_{AMA1}에 대한 네 개의 제곱근을 계산한다. S_{AMA1}은 MN이 계산하여 구한 제곱근 중 하나일 것이다. 네 개의 제곱근에는 비밀값을 공유하기 위해 사전에 결정된 불필요한 값들이 포함되어 있어, S_{AMA1}을 쉽게 결정하는 것이 가능하다. 이러한 방식을 통해 MN과 기존 AMA는 비밀값 S_{AMA1}을 공유한다.

4.3 단계 2: 정보 검증 절차

두 번째 단계는 MN이 새로운 네트워크에서 통신을 시작하고자 할 때 발생한다. 공격자로부터 MN의 바인딩 업데이트 절차를 보호하기 위해 기존 AMA와 MN은 시도 응답 (challenge-response) 교환 방식을 사용하여 같은 비밀값 S_{AMA1}을 공유하는지 확인한다. 이를 통해 MN의 세션 소유권에 대한 검증이 이루어진다. 또한, MN과 기존 AMA는 MN이 새로운 위치에서도 서로에게 도달 가능하다는 것을 확인할 수 있다. Fig. 3은 두 번째 단계에서의 메시지 교환을 나타낸다.

M2-1, M2-2: MN이 새로운 네트워크에 연결하고자 할 때 MN은 새로운 서빙 AMA인 AMA_2와 라우팅 정보를 교환하여 새로운 IP 주소인 AMA2::MN/64를 할당받는다.

M2-3: MN은 새로운 서빙 AMA에게 MN의 난수인 R_{MN}^i, 통신이 이루어지고 있는 세션에 대한 이전 주소 및 현재 주소에 대한 정보 등을 포함하는 총 5개의 매개 변수를 전송한다. MN은 새로운 네트워크에서만 유효하게 사용하기 위한 비밀값인 $S_{MN}^i(1 < S_{MN}^i < n)$과 $V_{MN}^i (\equiv (S_{MN}^i)^2 \bmod n)$을

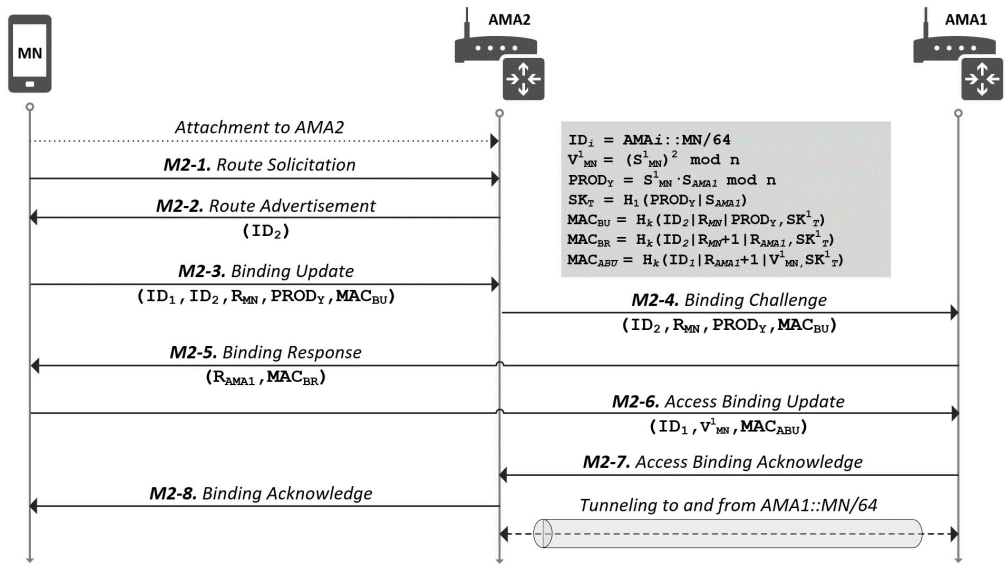

Fig. 3. Message flows in second phase for MN's ith movement in the network.

선택한다. S_{MN}^{i}은 기존 AMA에게 공유된 비밀값 S_{AMA1}을 노출 없이 전송하기 위하여 수식 (4)과 같이 두 값에 대해 곱하는 형태로 사용된다. 공유된 비밀값은 수식 (5)와 같이 SK_T^i을 통해 전송되는데, 이는 새로운 네트워크에서 공유되는 비밀값을 변경하여 비밀키의 새로움 (freshness)과 순방향 비밀성 (forward secrecy)를 제공하기 위함이다. 수식 (6)과 같이 비밀값 SK_T^i를 키로 하는 해시를 사용하여 생성된 MAC_{BU}는 BU 메시지의 매개 변수를 인증하기 위해 사용된다.

$$PROD_Y \equiv S_{MN}^{i} \bullet S_{AMA1} \bmod n \tag{4}$$

$$SK_T^i = H_1(PROD_Y, S_{AMA1}, R_{MN}^i) \tag{5}$$

$$MAC_{BU} = H_k(ID_2 | R_{MN}^i | PROD_Y, SK_T^i) \tag{6}$$

M2-4: 서빙 AMA는 MN의 주소를 확인하여 기존 AMA에게 BU 메시지에 네 개의 파라미터를 포함하여 전달한다.

M2-5: 기존 AMA는 MAC_{BU}를 통해 BC (Binding Challenge) 메시지에 대한 변조되지 않았으며, 공유된 비밀값 S_{AMA1}을 소유한 MN이 생성한 값임을 확인한다. 기존 AMA는 수식 (7)과 같이 MAC_{BR}을 R_{AMA1}과 함께 MN에게 전송한다.

$$MAC_{BR} = H_k(ID_2 | R_{AMA1} | R_{MN}^i + 1, SK_T^i) \tag{7}$$

M2-6: MN은 MAC_{BR}을 통해 BR (Binding Response) 메시지를 인증한 후, 수식 (8)과 같이 MAC_{ABU}를 계산하여 MN의 이전 IP 주소 및 MN의 비밀값 S_{MN}^{i}에 대한 $\bmod n$ 상에서의 이차잉여인 V_{MN}^{i}와 함께 기존 AMA에게 전송한다.

$$MAC_{ABU} = H_k(ID_1 | R_{AMA1} + 1 | V_{MN}^i, SK_T^i) \tag{8}$$

M2-7: 기존 AMA는 최종적으로 ABU 메시지를 통해 MN의 이동에 대한 응답을 전송한다.

$$Y \equiv V_{MN}^{i} \bullet V_{AMA1} \bmod n \tag{9}$$

수식 (9)의 매개변수 Y는 BC 메시지에서 수신한 $PROD_Y$를 제곱한 값과 비교하여, 두 값이 같으면 기존 AMA는 MN이 가지는 현재 세션의 소유권을 인정한다. 기존 AMA는 서빙 AMA와의 IPsec 터널을 맺기 위한 ABA 메시지를 전송한다.

M2-8: 서빙 AMA는 바인딩 캐시에 MN의 이동성 관련 정보를 업데이트한 후, BA 메시지를 전송

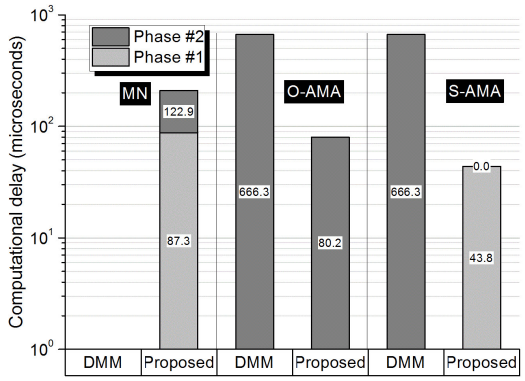

Fig. 4. Communication delays of two protocols.

한다. BA 메시지를 수신한 MN 또한 자신의 바인딩 캐시에 이동성 관련 정보를 업데이트한다.

바인딩 업데이트 절차를 완료하면 기존 AMA와 서빙 AMA 사이에는 안전한 터널이 설립된다. 기존 AMA와 서빙 AMA가 공유하는 비밀키는 수식 (5)에서 계산된 SK_T^i이다. MN과 서빙 AMA와의 비밀키는 MN이 모든 바인딩 업데이트 절차가 종료된 후 안전한 링크 계층 프로토콜을 통해 공유한다. 이 비밀키는 네트워크마다 다른 값을 가지므로 이전 서빙 AMA는 현재 서빙 AMA의 비밀키에 접근할 수 없다.

V. 성능 분석

제안하는 프로토콜이 보안 요구 사항을 만족하고 위협 모델에 대한 방어가 적절히 이루어지는지를 통해 검증하였다, 또한, 통신비용 및 계산 지연이 어느 정도의 오버헤드를 가지는지를 측정하였다.

5.1 보안성 분석

- 세션 소유권 (session ownership): 제안하는 프로토콜은 MN의 위치 변경에 대해 기존 AMA에게 알릴 때마다 매번 해당 세션의 소유권에 대한 상호 검증을 수행한다. 세션의 정보 등록 절차에서 MN과 기존 AMA는 비밀값 S_{AMA1}을 공유한 후, 세션 소유권에 대해 공유된 비밀값을 알고 있는지를 확인하는 인증이 이루어진다(**M2-4**, **M2-6**). 기존 AMA는 공유된 비밀값을 생성하여 $\bmod n$ 상에서 공유될 비밀값 S_{AMA1}의 이차잉여 V_{AMA1}를 전송한다. n을 올바르게 인수 분해할 수 있는 MN만이 비밀값 S_{AMA1}을 유도해낼 수 있다.
- 인증에 대한 MN의 적극적 참여: MN은 3방향 핸드셰이크 (three-way handshake)를 통해 기존 AMA와 직접적으로 이동과 관련한 매개변수를 협상하여 인증을 수행한다(**M2-3**, **M2-4**, **M2-5**, **M2-6**). 이때, **M2-3**, **M2-4**는 MN과 기존 AMA의 통신 면에서는 하나의 메시지로 볼 수 있다.
- 위치에 따른 도달 가능성: 위치가 변함에 따른 도달 가능성을 검증하기 위해서는 일반적으로 한 개체가 다른 개체에게 암호학적 토큰을 전송하여 토큰을 수신한 개체가 해당 토큰을 알고 있는지를 확인하는 방식을 사용한다. 제안하는 프로토콜에서는 난수를 보냈을 때 응답 메시지에 해당 난수에 대한 안전한 해시 값이 포함되는지를 확인하여 도달 가능성을 검증한다(**M2-4**, **M2-5**, **M2-6**).

5.2 성능 평가

제안하는 프로토콜이 보안상으로 안전하며, 사전 공유키 (pre-shared key)를 사용하는 IPsec이 적용된 기존의 DMM에 비해 통신비용과 계산 지연 면에서 더 우수함을 보이기 위하여 해당 항목들에 대한 비교를 수행하였다.

5.2.1 통신비용 (Communication costs)

통신비용은 MN과 통신이 이루어지고 있는 세션 N개의 주소 N개에 대해 모든 바인딩 업데이트를 수행할 때 네트워크에 전송되는 비트 (bit)의 수로 정의한다. 이에 대한 계산은 메시지에 포함되는 매개변수 및 연산 종류에 따라 Table 1을 기반으로 수행하였다. Table 2는 통신비용을 계산하기 위한 메시지들의 종류와 크기에 대한 목록이다.

제안하는 프로토콜의 정보 등록 절차에 대한 통신비용은 처음 바인딩 업데이트 절차가 수행되는 시점에 대해서 계산하였다. 기존 DMM은 Fig. 4의 **M1-3**, **M1-4**를 제외하고 제안하는 프로토콜과 같은 메시지를 교환한다. 제안하는 프로토콜은 기존 DMM에 비해 $\bmod n$ 상에서의 이차잉여 V_{AMA1}와 같은 추가적인 파라미터가 존재한다.

정보 검증 절차에서 제안하는 프로토콜은 여덟 개

Table 1. Parameters for measurements of communication costs.

Protocol	Parameters	Details
DMM	Initial Vector and Nonce	32 bits
	Encryption	AES-128-CBC
	MAC and PRF	HMAC-SHA1-96
	DH Group	Alternate 1024-bit MODP group
Proposed	ID	128 bits
	Random numbers (R_x)	32 bits
	n, S_{MN}, S_{AMA}	Alternate 1024-bit MODP group
	$H_1()$	SHA256
	$H_k()$	HMAC-SHA256

Table 2. Messages for binding updates and their sizes[6].

Notation	Description	Size in bytes
S_{RS}, S_{RA}	Size of RS/RA messages	52, 80
S_{BU}, S_{BA}	Size of the BU/BA messages	56, 56
S_{ABU}, S_{ABA}	Size of the ABU/ABA messages	56, 56
$S_{BINDING\ CHALL}$	Size of the BINDING CHALLENGE message	168
$S_{BINDING\ RES}$	Size of the BINDING RESPONSE message	92
S_{TU}, S_{MO}	Size of the tunneling header and mobility option	40, 20
S_{MAC}	Size of message authentication code	12
$S_{IKE\ INIT\ REQ}$	Size of the IKE INIT REQUEST message	298
$S_{IKE\ INIT\ RES}$	Size of the IKE INIT RESPONSE message	298
$S_{IKE\ AUTH\ REQ}$	Size of the IKE AUTH REQUEST message	568
$S_{IKE\ AUTH\ RES}$	Size of the IKE AUTH RESPONSE message	568

Table 3. Messages for a single binding updates in two protocols.

DMM	$S_{IKE\ INIT\ REQ}+S_{IKE\ INIT\ RES}+S_{IKE\ AUTH\ REQ}+S_{IKE\ AUTH\ RES}+S_{ABU}+S_{ABA}+4S_{MAC}+2S_{TU}+2S_{MO}$
Proposed	$S_{BINDING\ CHALL}+S_{BINDING\ RES}+S_{ABU}+S_{ABA}+2S_{TU}+2S_{MO}+44$

Table 4. Communication costs of the BU for two protocols with two addresses.

bits	M2-1	M2-2	M2-3	M2-4	M2-5	M2-6	M2-7	M2-8	M2-9	M2-10	Total
DMM	416	640	1,728	1,344	736	1,184	928	96			7,936
Proposed	416	640	704	2,384	2,384	4,640	4,640	1,024	1,024	448	18,304

의 메시지를, 기존 DMM은 열 개의 메시지를 교환한다. 서로 다른 N개의 주소에 대해 바인딩 업데이트 절차를 수행할 경우, 제안하는 프로토콜은 $4+3(N-1)$개의 메시지를 교환하며, 기존 DMM은 $4+6(N-1)$개의 메시지를 교환한다. Table 4는 두 개의 주소에 대해 바인딩 업데이트 절차를 수행할

Table 5. Average elapsed time of cryptographic atomic operations for comparing computational delay.

Operations	Symbol	Delay in microseconds
Diffie-Hellman parameter	$T_{DH\,param}$	221.94
Diffie-Hellman shared key	$T_{DH\,share}$	244.84
Nonce	T_{nonce}	1.26
Pseudo random function	T_{PRF}	11.18
AES-128-CBC	T_{AES}	12.1
HMAC-SHA1-96	T_{HMAC}	9.52
Quadratic residue parameter	$T_{QR\,param}$	6518.68
Quadratic residue encryption	$T_{QR\,enc}$	43.8
Quadratic residue decryption	$T_{QR\,dec}$	87.34
SHA-256	T_{SHA256}, $T_{HNAC-256}$	15.28
Addition of nonce	T_{add}	0.38
Multiplication in modulo	T_{mul}	1.08

Table 6. Atomic operations consisting of the computational delay for MN, original AMA, and serving AMA for two protocols.

Protocol	Entity	Phase 1	Phase 2
DMM	MN	-	-
	Original AMA	-	$T_{DH\,param}+T_{DH\,share}+T_{nonce}+8\,T_{PRF}+4\,T_{AES}+4\,T_{HMAC}$
	Serving AMA	-	$T_{DH\,param}+T_{DH\,share}+T_{nonce}+8\,T_{PRF}+4\,T_{AES}+4\,T_{HMAC}$
Proposed	MN	$T_{QR\,dec}$	$T_{QR\,enc}+T_{nonce}+T_{add}+T_{mul}+T_{SHA256}+4\,T_{HNAC-256}$
	Original AMA	-	$T_{add}+T_{nonce}+2\,T_{mul}+T_{SHA256}+4\,T_{HNAC-256}$
	Serving AMA	$T_{QR\,enc}$	-

때 두 프로토콜의 통신비용을 비교한 것이다. 두 프로토콜은 두 번째 메시지까지는 같은 비용이 발생한다. 네 번째 메시지부터 기존 DMM이 제안하는 프로토콜보다 더 많은 데이터와 메시지를 생성한다. DMM의 전체 통신비용은 18,304비트로 제안하는 프로토콜보다 세 배 이상의 비용이 발생한다. 모든 메시지를 처리하기 위해 발생하는 전체 통신비용은 Table 3에 나타내었다.

5.2.2 계산 지연 (Computational delay)

Crypto++ 라이브러리[7]로 암호학적 연산 수행에 소요되는 시간을 측정하였다. 측정은 Intel Quad Core 3.60 GHz, 8 gigabyte RAM을 탑재한 리눅스 커널 버전 3.19를 기반으로 하는 우분투 (Ubuntu) 14.04 운영체제에서 수행하였다.

Table 5는 12개의 프로토콜에 사용되는 암호학적 기본 연산에 대한 수행 시간을 나타낸다. 두 프로토콜을 수행할 때 MN과 AMA에서 소요되는 계산 지연 시간에 대해 비교한 수식은 Table 6에, 그래프는 Fig. 4에 나타난다. 정보 등록 절차에서 MN이 수행하는 연산은 $T_{QR\,param}$와 $T_{QR\,dec}$으로 6606.02초가 소요되어야 한다. 그러나 $T_{QR\,param}$은 MN이 바인딩 업데이트 절차를 수행하기 전 계산할 수 있는 연산이다. 따라서 MN이 정보 등록 절차에서 수행해야 하는 연산은 $T_{QR\,dec}$ 뿐이며, 소요되는 시간은 87.34초이다.

대화형 (interactive) 프로토콜의 경우, 연산에 필요한 매개변수가 실시간으로 결정되므로 사전에 계산을 수행할 수 없다. 기존 DMM에서 사용하는 디피 헬만 키 교환 방식에서 서빙 AMA와 기존 AMA

사이의 IPsec 터널에 대한 키를 갱신하기 위해 필요로 하는 매개변수들이 이에 해당한다.

기존 DMM의 경우, 정보 등록 절차에서 MN과 AMA는 암호학적 연산을 전혀 필요로 하지 않는다. 또한, 정보 검증 절차에서도 마찬가지로 MN은 암호학적 연산을 수행하지 않으나, 서빙 AMA와 기존 AMA는 암호학적 연산을 위해 각각 666.3초의 시간을 소요한다. 이는 서빙 AMA가 MN을 대신하여 기존 AMA와 IPsec 터널을 생성하기 때문이다.

제안하는 프로토콜은 정보 등록 절차에서 MN은 87.34초, 서빙 AMA는 43.8초의 시간이 소요된다. 정보 검증 절차에서 기존 AMA는 다섯 번의 해시 연산, 두 번의 곱셈, 한 번의 덧셈, 그리고 한 번의 난수 생성을 수행함에 따라 80.2초의 연산 시간이 소요되나 서빙 AMA는 암호학적 연산을 수행하지 않는다. 기존 DMM에서 기존 AMA가 수행하는 연산은 제안하는 프로토콜에서 기존 AMA가 수행하는 연산보다 여덟 배 이상의 시간이 소요된다. MN의 경우 QR 암호화를 제외하면 기존 AMA와 비슷한 연산을 수행하며 총 122.9초가 소요된다.

VI. 관련 연구

[8]에서 Chuang *et al.*은 PMIPv6의 인증과 핸드오버 절차의 인증을 향상하기 위한 기법을 제안하였다. PMIPv6는 네트워크를 기반으로 하는 이동성 관리 기술로, MN이 이동성 관리에 참여하지 않으므로 MN에 부과되는 시그널링 오버헤드가 감소한다. 그러나 PMIPv6는 효과적이지 않은 인증 절차, 패킷 손실, 보안상의 위협 등의 문제에 직면해 있다. 바이캐스팅 (bicasting) 스키마를 통해 패킷 손실을 막고 순서가 올바르게 오지 않은 패킷에 대한 처리가 가능하다. [8]에서 제안된 프로토콜은 대칭키의 사용과 해시 계산만으로 인증 지연을 제거하였으나, 여전히 IPsec을 사용함에 따라 발생하는 비용이 존재한다. 또한, 모든 MA가 인증 서버와 같은 사전 공유키를 공유하므로 하나의 MA라도 공격자가 제어할 수 있는 경우 시스템 전체가 위험에 노출될 수 있다. 본 논문에서는 IPsec의 사용 및 인증 서버 없이 MN과 AMA 가 상호 인증을 수행하므로 추가 비용이 적게 발생한다.

[9]에서 Lee는 DMM에서 동적 터널링을 통한 MN과 분산된 앵커 사이의 안전한 인증을 제안하였다. 제안된 스키마에서는 어떤 분산 앵커가 LMA (Local Mobility Anchor)에 대한 터널을 관리할 것인지 세션-이동성 비율 (session to mobility ratio)을 통해 결정한다. 세션-이동성 비율이 높으면 분산 앵커는 MN이 CN으로 전송하는 데이터 패킷에 대한 터널을 설립한다. 그렇지 않으면, 분산 앵커 간에 설립된 터널이 계속 사용된다. [9]에서 제안하는 프로토콜은 MN을 인증하기 위한 상호 인증 방식으로 일반적인 서버 클라이언트 모델을 사용하지만, 본 논문은 인증 서버를 거치지 않고 서로를 인증하는 피어 투 피어 (peer-to-peer) 인증 방식을 사용하므로 인증 서버를 거쳐야 하는 추가 비용이 발생하지 않는다.

VII. 결 론

본 논문에서는 기존 DMM의 네트워크상의 지연 및 보안상의 문제점을 해결하는 새로운 프로토콜을 제안하였다. 기존 DMM에서 바인딩 업데이트는 MIPv6의 보안 매커니즘을 그대로 계승했기 때문에 보안 및 지연과 관련하여 고려해야 할 여러 문제점이 존재한다. 제안된 매커니즘은 바인딩 업데이트 절차에 참여하는 MN과 기존 AMA가 비밀 토큰을 공유하여 MN이 새로운 네트워크로 이동하였을 때에도 상호 인증을 가능케 하여 DMM의 보안성을 향상시킨다.

바인딩 업데이트 절차에 관련하여 응답 지연을 향상시키기 위해 연구해야 할 문제가 아직 많이 남아있다. DMM을 5G (fifth generation) 촉각 인터넷 (tactile Internet) 등의 새로운 서비스 환경에 적용하였을 때 어떤 시스템 상의 문제가 발생할 수 있는지에 대해 고려해 볼 필요가 있다.

References

[1] C.Perkins, D.Johnson, and J.Arkko, "Mobility support in IPv6," *RFC 6275*, July 2011.

[2] S.Gundavelli et al., "Proxy mobile IPv6," *RFC 5213*, Aug 2008.

[3] D.Liu and *et al.*, "Distributed mobility management: current practices and gap analysis," *RFC 7429*, Jan 2015.

[4] D.Dummit, E.Dummit, and H. Kisilevsky, "Characterizations of quad-

ratic, cubic, and quartic residue matrices," *Journal of Number Theory*, Vol. 168, pp. 167-179, Nov. 2016.
〔5〕 M.Elia, M.Piva, and D.Schipani, "The Rabin cryptosystem revisited," *Applicable Algebra in Engineering, Communication and Computing*, Vol. 26, No. 3, pp. 251-275, Jun. 2015.
〔6〕 J.Lee, J.Bonnin, I.You and T. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1077-1088*, March. 2013.
〔7〕 Crypto++ Library 5.6.3, available at http://www.cryptopp.com/.
〔8〕 M. Chuang, J. Lee, and M. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Systems Journal*, Vol. 7, No. 1, pp. 102-113, March. 2013.
〔9〕 J. Lee, "Secure authentication with dynamic tunneling in distributed IP mobility management," *IEEE Wireless Communications*, Vol. 23, No. 5, pp 38-43, Oct. 2016.

〈저자소개〉

이 세 영 (Seyeong Lee) 정회원
2014년 2월: 성균관대학교 컴퓨터공학과 졸업
2016년 2월: 성균관대학교 IT융합학과 석사
2016년 2월~현재: 삼성전자 근무
〈관심분야〉 모바일 디바이스 인증, 사물인터넷 보안

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사
2001년~2004년: Lanscope 근무
2004년 3월~현재: 성균관대학교 소프트웨어대학 교수
〈관심분야〉 네트워크보안, 리버싱 엔지니어링

김 이 진 (EJin Kim) 학생회원
2016년 2월: 서울여자대학교 정보보호학과 졸업
2016년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 모바일 디바이스 인증, 사용자 인증 및 보안