Modified Return Routability를 이용한 Hierarchical Mobile IPv6 Handover 인증 기법

Authentication of Hierarchical Mobile IPv6 Handover Using Modified Return Rotability

김 정 환* 유 기 성** 박 병 연*** 노 민 기**** 문 영 성*****
Junghwan Kim Kisung Yu Byungyeon Park Minki Noh Youngsong Mun

요 약

Hierarchical Mobile IPv6는 Binding Update를 지역적으로 관리함으로써 기존의 Mobile IPv6의 성능을 향상시킨 메커니즘이다. 이렇게 향상된 Handover Delay로 인하여 지연에 민감한 서비스들의(예를 들어, VoIP나 비디오 스트리밍(Video Streaming)) 지원이 좀 더 실현 가능해졌다. 하지만 기존 MIPv6와 비교해 볼 때, HMIPv6에서는 Local Binding Update와 관련된 보안 위협 사항이 새로이 생겨나게 되었으며 이는 반드시 해결되어야 할 문제임에도 불구하고 정확한 표준이 제시되지 않은 상황이다. 또한 많은 연구의 초점이 AAA나 인증서 기반의 PKI 등에 맞춰져 있는데, 이러한 Infrastructure 기반의 인증 방법은 실제 네트워크에 도입되었을 때 범용적으로 사용하기에는 문제점이 있다. 이에 본 연구에서는 수정된 Return Routability메커니즘을 적용하여 Local Binding Update를 인증하는 방안을 제안하며 아울러 이동 노드로 하여금 단말기의 파워(power)를 절약하게 하는 방안도 제공한다.

Abstract

Hierarchical Mobile IPv6 improves performance of Mobile IPv6 by managing Binding Update in terms of location. With improved handover delay, realization of delay-sensitive services (e.g. VoIP or video streaming) has become more persuadable. Comparing with Mobile IPv6, however, Hierarchical Mobile IPv6 brings security threats related to Local Binding Update to mobile network. In the RFC 4140, specific methods to authenticate Local Binding Update message are not explicitly presented. It is essential that design secure architecture to address problems related to authenticating Local Binding Update. Many secure suggestions for Local Binding Update, however, concentrate on infrastructure-based solutions such as AAA, PKI. These approaches may cause scalability problem when the suggested solutions are applied to real network. Therefore we suggest authentication method that doesn't require infrastructure. In addition to authentication of Local Binding Update, our method also provides mobile node with power saving ability.

☞ keywords : HMIPv6, Authentication, Return Routability

1. 서 론

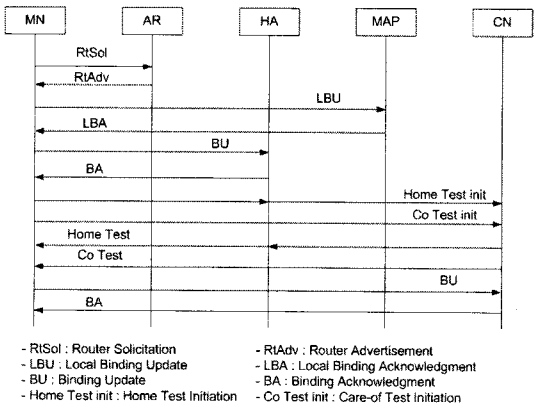
휴대 가능한 기기가 점점 보편화되고 무선 네트워크로의 접속이 용이해짐에 따라, IETF는 이동 노드의 이동성을 지원하기 위해 Mobile IPv6 (MIPv6)를 제안하였다. 하지만 핸드오버시 발생하는 지연 시간은 끊김 없는 통신을 방해하였고 이를 해결하기 위한 방법 중 한가지로 Hierarchical MIPv6 (HMIPv6)[2]가 제안되었다. HMIPv6는 Binding Update (BU)를 지역적으로 관리함으로써 기존의 MIPv6의 성능을 향상시킨 메커니즘이다.

* 준 회 원 : 숭실대학교 대학원 컴퓨터학과 재학(석사)
marubazz@sunny.ssu.ac.kr
** 정 회 원 : 한국과학기술정보연구원 초고속연구망 사업실장 ksyu@kisti.re.kr
*** 정 회 원 : 한국과학기술정보연구원 선임연구원
bypark@kisti.re.kr
**** 정 회 원 : 한국과학기술정보연구원 선임연구원
mknoh@kisti.re.kr
***** 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@ssu.ac.kr(교신저자)
[2007/05/08 투고 - 2007/05/11 심사 - 2007/08/02 심사완료]

이렇게 향상된 Handover Delay로 인하여 지연에 민감한 서비스들의(예를 들어, VoIP나 비디오 스트리밍(video streaming)) 지원이 좀 더 실현 가능해졌다. 하지만 기존 MIPv6와 비교해 볼 때, HMIPv6에서는 Local Binding Update (LBU)와 관련된 보안 위협 사항이 새로이 생겨나게 되었으며 이는 반드시 해결되어야 할 문제임에도 불구하고 정확한 표준이 제시되지 않은 상황이다. 또한 많은 연구의 초점이 AAA나 인증서 기반의 PKI 등에 맞춰져 있는데, 이러한 인프라 기반의 (Infrastructure-based) 인증 방법은 실제 네트워크에 도입되었을 때 범용적으로 사용하기에는 문제점이 있다. 이에 본 연구에서는 수정된 Return Routability(RR) 메커니즘을 적용하여 LBU를 인증하는 방법을 제안하며 아울러 이동 노드로 하여금 단말기의 파워(power)를 절약하게 하는 방안도 제공한다.

2. 관련 연구

2.1 HMIPv6



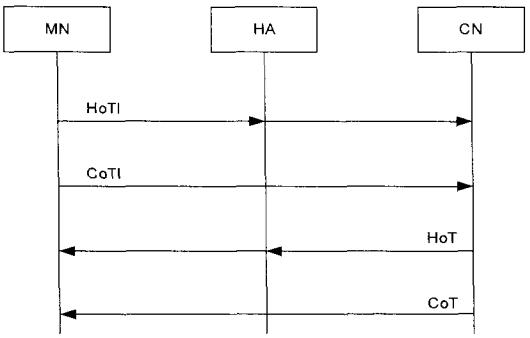
(그림 1) FMIPv6

HMIPv6[2]는 Home Agent (HA)와 Correspondent Node (CN)으로 BU 하는데 필요한 시그널의 개수와 시간을 줄임으로 인해서 MIPv6[1]의 성능 향상을 이끌어 낸다. 기본적으로 MIPv6에서 이동노드(Mobile Node, MN)는 Access Router (AR)가 바뀔 때마다 HA에게 Care-of Address (CoA)의 변화를 알려줘야 한다. 이러한 BU 과정은 MN으로 하여금 지연 시간을 갖게 하며 끊김 없는 통신에 방해가 된다. 더욱이 이런 지연은 MN과 HA, CN 사이의 거리가 멀수록, CN의 개수가 많을수록 심각해진다. [2]에서 새로이 소개된 LBU 과정은 이러한 비효율성을 BU를 지역적으로 관리함으로써 해결한다.

지역적인 HA로 작동하는 Mobile Anchor Point (MAP)의 영역에 새로이 진입한 MN은 AR로부터 MAP의 정보를 포함하여 RA 메시지를 받는다. 이 메시지에 담긴 정보를 바탕으로 MN은 Local CoA (LCoA)와 Regional CoA (RCoA)를 생성한다. 그 후 MN은 LCoA와 RCoA를 바인딩(Binding)하여 MAP에게 LBU를 실행한다. MN은 MAP 내부에서는 LCoA로 구분되며 MAP 외부로부터는 RCoA를 사용하여 접근된다. LBU 과정을 마치고 나면 MN은 HA와 CN에게 Source Address를 RCoA로 하여 BU 과정을 수행한다. 성공적으로 LBU 과정이 마치게 되면 MAP은 MN의 지역적인 HA로서 동작하게 되며 MN이 동일 MAP 내에서 AR을 변경하더라도 MAP에게만 BU하면 되며 MAP 외부로의 BU는 MAP이 변경되었을 때만 발생한다. 외부 네트워크로부터 MN으로 향하는 트래픽(Traffic)이 들어오게 되면, MAP은 Entry List를 검색하여 해당 노드(Node)에게 Forwarding 한다. HMIPv6는 (그림 1)에 나타난다.

하지만 HMIPv6는 새로이 생겨난 LBU 때문에 기존 MIPv6와 비교하여 보안 위협 사항이 추가되었다. MIPv6에서는 HA로의 BU를 인증하기 위해 IPsec을 사용하며 CN으로의 BU는 RR 메커니즘을 사용하여 인증한다. 하지만 현재 HMIPv6[2] 표준에서는 LBU를 인증하기 위한 뚜렷한 방법을 제시하지 않고 있다.

2.2 Return Routability



(그림 2) Return Routability Procedure

MIPv6는 MN으로부터 CN으로 전송되는 BU 메시지를 인증하기 위해 RR를 사용한다. RR을 수행함으로써 MN과 CN은 서로가 적합한 통신 상대인지 인식할 수 있게 된다. RR을 사용함으로써 얻을 수 있는 장점 중 한 가지는 Scalability Issue를 피할 수 있다는 것이다. 인증서 기반 PKI나 AAA 같은 인증 방법들이 일정 Infrastructure를 필요로 하는 반면 RR는 MN과 CN으로 하여금 어떠한 Infrastructure나 사전에 성립된 Security Association (SA)을 요구하지 않는다. 이러한 RR의 특징으로 인해서 Scalability Issue를 피할 수 있게 된다. RR은 MN으로부터 CN으로의 메시지 쌍인 <HoTI, CoTI>와 그에 대한 CN으로부터의 응답인 <HoT, CoT> 두 개의 메시지 쌍으로 이루어진다. RR을 시작하기 위해 MN은 Home Init Cookie를 포함하고 있는 Home Test Init (HoTI)과 Care-of Init Cookie를 포함하고 있는 Care-of Test Init (CoTI) 메시지를 CN에게 보낸다. 이 때 HoTI는 HA를 거쳐서 전송되어 IPsec으로 보호되며 CoTI는 직접 CN에게 전송된다. 이렇게 각 Init 메시지의 전송 경로를 달리 함으로써 공격자로부터의 위협 요소를 줄이는 효과를 얻을 수 있다. HoTI와 CoTI를 받은 후에 CN은 응답으로서 Home Test (HoT)와 Care-of Test (CoT) 메시지를 전송한다. HoT는 Home Init Cookie, Home Keygen Token, Home Nonce Index를 담고 있으며, CoT는 Care-of Init Cookie, Care-of Keygen Token, Care-of Nonce Index를 포함하고 있다. 전송받은 HoT와 CoT 메시지의 Cookie들을 확인함으로써 MN은 적합한 CN으로부터 온 응답 메시지임을 확인할 수 있으며 Home Keygen Token과 Care-of Keygen Token을 사용하여 K_{bm}을 얻을 수 있게 된다. 이 K_{bm}은 MN과 CN 사이의 BU를 인증하는데 사용된다. K_{bm}은 두 개의 Keygen Token을 입력으로 SHA1 해쉬 함수를 사용하여 얻어진다.

$$K_{bm} = SHA1(home\ keygen\ token \| care-of\ keygen\ token) \quad (1)$$

$$home\ keygen\ token = First(64, HMAC\_SHA1(K_{cn}(Home\_address \| nonce \| 0))) \quad (2)$$

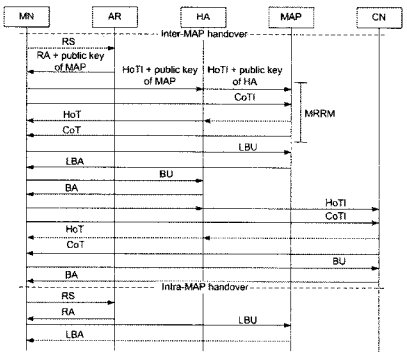
$$care-of\ keygen\ token = First(64, HMAC\_SHA1(K_{cn}(co\_address \| nonce \| 1))) \quad (3)$$

CN은 MN으로부터 BU 메시지를 받았을 때 K_{bm}의 유효성 여부를 판단함으로써 적합한 MN인지를 판단 할 수 있게 된다.

여러 장점에도 불구하고 RR은 HA와 CN 사이의 패스(path)에 있는 공격자에게 보안적으로 취약한 약점을 가지고 있다. HA와 CN 사이의 통신은 보호가 안되기 때문에 공격자는 MN의 HoTI를 가로채 자신의 CoA를 사용하여 CN에게 적합하지 않은 BU를 할 수 있다. 특히 통신 환경이 이동 통신으로 변화하면서 공격자로 하여금 HA와 CN 사이의 경로에 잠시 머무르면서 생성한 Binding Cache Entry (BCE)를 사용하여 이동 중에도 공격 할 수 있게 되었다. 이러한 공격을 Time Shifting Attack이라고 한다[1][3][5]. MIPv6는 RR을 기반으로 한 인증 환경에서 이러한 Time Shifting Attack의 위험을 줄이고자 K_{bm}의 Lifetime을 제한한다. 이렇게 제한된 Lifetime 으로 인해 주기적으로 K_{bm}을 Refresh해야 하는 번거로움이 있다.

3. 제안 사항

MN이 새로이 어떤 MAP 도메인에 진입했을 때 그 MN은 Router Solicitation (RS) 메시지를 보내게 되는데 이때 MAP의 Public Key를 같이 요청한다. Public Key를 포함한 Router Advertisement (RA) 메시지를 받게 되면 MN은 Modified Return Routability with MAP (MRRM) 과정을 시작한다. 이 때 중요한 것은 HoTI 메시지를 보낼 때 MAP의 Public Key를 같이 HA에게 전송하는 것이다. HA는 MN으로부터 중간자 역할을 요청받게 되면 HoTI 메시지를 MAP의 Public Key로 암호화하여 자신의 Public Key와 같이 전송한다. MRRM은 RR과 마찬가지로 <HoTI, CoTI>와 <HoT, CoT> 두 개의 쌍으로 이루어지며 각각의 쌍은 병렬적으로 동시에 수행된다. HA로부터 HoTI 메시지와 HA의 Public Key를 전송 받은 MAP은 응답으로서 HA의 Public Key로 HoT 메시지를 암호화하여 HA에게 전송한다. CoTI 메시지와 CoT 메시지는 그 대상만 MN과 MAP일 뿐 수행 과정은 RR과 동일하다. 이렇게 MRRM 과정이 끝나게 되면 LBU와 Local Binding Acknowledgment (LBA) 과정이 실행되며 그 이후의 과정은 HMIPv6[2]와 동일하다. HA와 MAP 사이의 메시지 교환에 각자의 Public Key가 사용되는 이유는 HA와 MAP 사이에 위치한 공격자로부터 메시지를 보호하기 위해서이다. 이러한 보호로 인하여 MN은 MAP내에서의 Handover 후에도 기존의 K_{bm} 을 별도의 추가 과정 없이 그대로 사용할 수 있다.

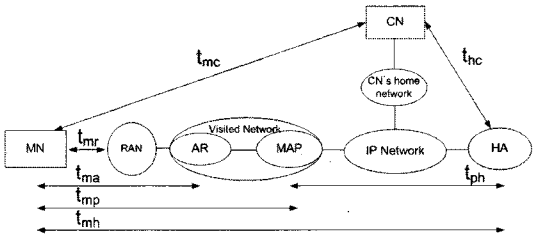


(그림 3) 제안 기법의 수행 과정

4. 성능 평가

4장에서는 제안된 방법의 Disruption Delay를 분석하고 수치적 결과를 평가한다. 4.1에서는 시스템 모델과 그에 따른 Delay가 분석되며, 4.2에서는 무선 구간의 Frame Error Rate (FER) 를 고려한 성능평가를 보인다. 마지막으로 4.3에서는 네트워크 구성요소(Network Entity)들 사이의 전송 시간과 Backoff Timer, Packet Size등을 고려하여 수치적으로 비용을 비교 분석한다

4.1 System Model and Delay Analysis



(그림 4) System Model

분석을 위해 [4]에서 소개된 시스템 모델을 사용한다. HMIPv6에는 두가지 Handover 경우가 있다. 첫째 경우인 Intra-MAP Handover에서 MN은 RS 메시지를 보내고 그에 따른 응답으로 RA를 받게 되면 LBU 메시지를 MAP에게 보낸다. 최종적으로 MAP으로부터 LBA 메시지를 받게 되면 Intra-MAP Handover는 성공적으로 마치게 된다. 이를 위한 Delay는 식 (4)에 나타난다. 다른 한가지 Handover인 Inter-MAP Handover는 MRRM과정과 HA, CN으로의 BU 과정에 필요한 메시지 교환들이 추가로 필요하다. Inter-MAP Handover 과정의 Delay는 식 (5)에 나타난다.

$$t_{MRRM}^{Intra-MAP} = 2t_{ma} + 2t_{mp} \quad (4)$$

$$t_{MRRM}^{Inter-MAP} = 2t_{ma} + 6t_{mh} + 2t_{ph} + 2t_{mp} + 2t_{hc} + 2t_{mc} \quad (5)$$

4.2 Frame Error Rate

무선 구간의 전송과 관련된 지연 시간을 분석하기 위해 FER을 고려한다[4][5]. p를 무선 구간에서 하나의 Frame이 에러가 날 확률이라고 가정하자. 하나의 패킷이 k개의 Frame으로 이루어져 있다면 패킷 손실 비율(Packet Loss Rate)은 $(1-(1-p)^k)$이다. τ는 연속적인 두 개의 Frame 사이의 시간 간격이며 D는 Frame이 Radio Access Network (RAN)을 통해 전송되는 Propagation Delay이다. 그러므로 MN으로부터 RAN으로 어떤 MIP 관련 시그널링 메시지의 Propagation Delay는 $D+(k-1)\tau$이다.

1) Retransmission Timer: MIPv6 기반 프로토콜의 Retransmission Timers는 Exponential Backoff 메커니즘을 따른다. 그러므로 i번째 전송을 위한 Backoff Timer인 $Tr(i)$는 $Tr(1)$을 Initial Backoff Timer라고 할 때 식 (6)과 같이 나타난다.

$$Tr(i) = 2^{i-1} * Tr(1) \tag{6}$$

2) Retransmission Probability: q는 패킷 송수신의 실패로 인하여 발생되는 재전송 확률이다. 이러한 재전송은 첫 번째 패킷(RS나 HoTI같은 Request Message)의 전송이 실패하거나, 첫 번째 패킷 전송은 성공하였더라도 그에 대한 응답 메시지(RA나 HoT같은 Reply Message)가 실패하는 경우에 발생한다. 그러므로 q는 식 (7)과 같이 나타내어진다.

$$q = 1-((1-p)^{k_1+k_2}) \tag{7}$$

3) Average Transmission Delay: Nm을 전송하는 최대 회수라고 하자. 이때 i번째 Request 시그널링(signaling)의 무선 구간에서의 평균 지연 시간 $Tt(i)_{MIP}$는 식 (8)과 같다.

$$\begin{aligned} Tt(i)_{MIP} &= \frac{1}{1-q^{Nm}} * [(1-q)(D+(k-1)\tau) \\ &\quad + (1-q)q(Tr(1)+D+(k-1)\tau) \\ &\quad + (1-q)q^2(3Tr(1)+D+(k-1)\tau) \\ &\quad + \cdots + (1-q)q^{Nm-1}((2^{Nm-1}-1)Tr(1) \\ &\quad + D+(k-1)\tau)] \\ &= D+(k-1)\tau - Tr(1) \\ &\quad + \frac{(1-q)(1-(2q)^{Nm})}{(1-q^{Nm})(1-2q)} \cdot Tr(1) \end{aligned} \tag{8}$$

$i+1$번째 응답 메시지 전송(즉 Reply / Advertisement / Acknowledgement)은 i번째 Request 메시지 전송이 성공적으로 이루어져야 실행된다고 하면, 응답 메시지의 평균 전송 지연 시간은 식 (9)와 같이 표현된다.

$$Tt(i+1) = D+(k-1)\tau \tag{9}$$

최종적으로, Handover에 필요한 시그널링 메시지가 N개라면 평균적인 핸드오버 지연시간 Tt_{MIP}는 식 (10)과 같이 표현된다.

$$Tt_{MIP} = \sum_{i=1}^{N} Tt(i)_{MIP} \tag{10}$$

그러므로 MRRM을 사용한 HMIPv6의 Inter /Intra-MAP 핸드오버 딜레이는 각각 식 (11)과 (12)에 주어진다.

$$\begin{aligned} Tt_{MRRM}^{inter-MAP} &= Tt(RS)+Tt(RA+public) \\ &\quad + Tt(HoTI+public)+Tt(HoT) \\ &\quad + Tt(LBU)+Tt(LBA)+Tt(BU-H) \\ &\quad + Tt(BA-H)+Tt(HoTI)+Tt(HoT) \\ &\quad + Tt(BU-C)+Tt(BA-C) \\ &\quad + 2t_{rc}+2t_{ra}+6t_{rh}+2t_{ph}+2t_{rp}+2t_{hc} \end{aligned} \tag{11}$$

$$\begin{aligned} Tt_{MRRM}^{intra-MAP} &= Tt(RS)+Tt(RA)+Tt(LBU) \\ &\quad + Tt(LBA)+2t_{ra}+2t_{rp} \end{aligned} \tag{12}$$

t_{rc}, t_{ra}, t_{rh}, t_{rp}는 각각 RAN과 CN, AR, HA, MAP 사이의 Delay이며 t_{ph}는 MAP과 HA사이, t_{hc}는 HA와 CN 사이의 Delay이다.

4.3 Numerical Result

표 1. Backoff Timers

	Backoff Timer in Second	Max Backoff Timer in Seconds
Inter-MAP HMIPv6		
Rt. Solic.	1	32
HoT / CoT Init	1	32
BU	1.5	32
Intra-MAP HMIPv6		
Rt. Solic.	1	32
BU	1.5	32

t_{mr}, t_{ma}, t_{mp}는 [4]와 [7]을 참조하여 각각 10ms, 11ms, 12ms로 잡는다. IP 코어(core)망을 지나는 유선 구간의 전송 지연 시간은 여러 변인과 이종 기계들 사이의 차이로 인해 일반화 시키기 어려운 관계로 [4]를 참조로 하여 100ms로 잡는다. 그러므로t_{ph}, t_{hc}, t_{mc}, t_{mh} 는 각각 100ms, 114ms, 124ms, 112ms 이다. 성능 평가를 위해 [1][2][6]에서 얻어진 Backoff Timer와 메시지 크기(Message Size)를 (표 1)과 (표 2)에서 보여주고 있으며 이를 활용하여 도출된 본 제안사항의 성능을 (그림 5)와 (그림 6)에서 보여주고 있다.

표 2.. Message Sizes

Messages	Length (bytes)
Rt. Solic.	52
Rt. Adv.	80
Home/Co Test Init	64
Home/Co Test	74
BU (MAP)	56
BU (HA)	56
BA (CN)	66
BA (MAP)	56
BA (HA)	56
BA (CN)	66

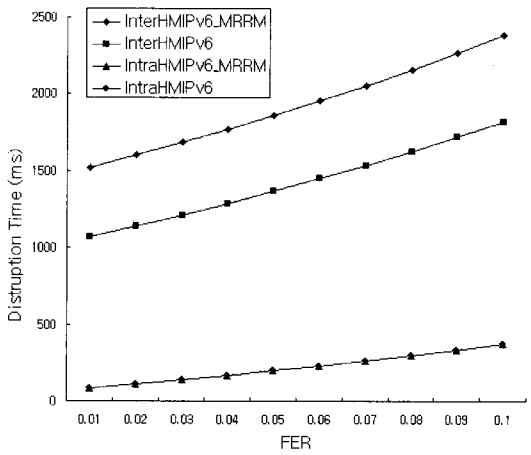


그림 5. FER 변화에 따른 disruption time

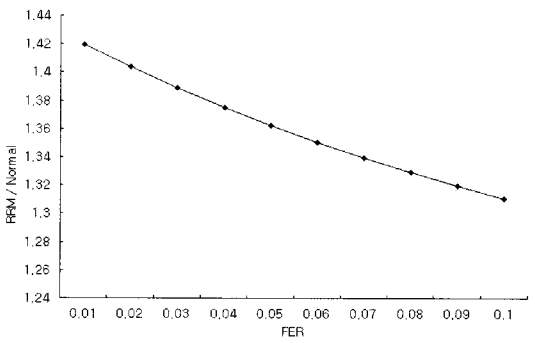


그림 6. HMIPv6와 제안 사항의 성능 비교

(그림 5)를 보면 Frame이 에러가 날 확률이 1%에서 10%까지 변할 때 Inter-MAP HMIPv6의 핸드오버로 인한 Disruption Time은 1070ms에서 1816ms까지 증가하며 제안 기법을 적용한 Inter-MAP HMIPv6는 1519ms에서 2378ms 까지 증가하는 것을 볼 수 있다. Inter-MAP 핸드오버와는 달리 Intra-MAP 핸드오버는 두가지 방법 모두 동일한 Disruption Time을 보임을 알 수 있다. (그림 6)에서는 HMIPv6와 제안 기법의 성능을 비율로 보여주고 있는데 FER이 0.01에서 0.1까지 변할 때 제안 기법은 HMIPv6의 1.41배에서 1.31배의 성능 변화를 보여주고 있다.

5. 결론

본 논문에서는 안정적으로 HMIPv6를 운용하기 위해서 선결되어야 할 LBU 메시지를 인증하는 기법에 대해서 다루었다. 기존의 많은 연구들이 AAA나 인증서 기반 PKI 사용 등의 Infrastructure를 요구하는 반면에 본 제안 기법은 MIPv6의 기본 인증 방법인 RR를 HMIPv6 환경에 알맞도록 수정하여 보안 성능을 향상시키므로 어떠한 Infrastructure나 사전에 약속된 SA을 요구하지 않는다. 또한 IETF 표준문서 [1]에서 제공하는 RR 기법을 HMIPv6 환경에 도입함으로써 새로운 보안 위협 사항을 불러일으키지도 않는다. 이동노드의 HA와 MAP 사이에서의 비대칭키 사용은 기존 RR이 지니고 있던 보안적 취약점을 상당 부분 해소하였으며 결과적으로 이동노드로 하여금 LBU 인증에 필요한 키(Key)를 Refresh하는 수고를 덜게 하여 이동노드가 휴면상태에 들어가는 것을 방해하지 않아 전력을 절약하는데도 유용하다. 비대칭키의 암/복호화 과정은 고성능을 기대할 수 있는 HA와 MAP에서만 일어나므로 제안 기법으로 인해 이동노드에게 추가로 발생하는 성능상의 제한이나 부담은 없다.

참 고 문 헌

[1] Charles E. Perkins and David B. Johnson, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] H. Soliman, C. Castelluccia, K. El Malki and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

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

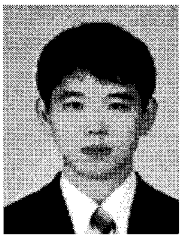
[4] Hanane Fathi, Shyam S. Chakraborty and Ramjee Prasad, "Optimization of Mobile IPv6-Based Handovers to Support VoIP Services in Wireless Heterogeneous Networks", IEEE Transaction on Vihicular Technology, January 2007.

[5] Hanane Fathi, SeongHan Shin, Kazukuni Kobara, Shyam S. Chakraborty, Hideki Imai, Ramjee Prasad, "Leakage-Resilient Security Architecture for Mobile Ipv6 in Wireless Overlay Networks", IEEE JOURNAL in communications, VOL23, NO. 11, November 2005.

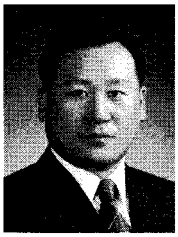
[6] C. Perkins, IP Mobility Support, Aug. 2002. IETF RFC 3344.

[7] T.T. Kwon, M. Gerla, and S.Das, "Mobility management for VoIP service: MobileIP vs .SIP," IEEE Trans. Wireless Commun., vol.9, no.5, pp.66-75, Oct.2002.

◐ 저 자 소 개 ◑



김 정 환(Junghwan Kim)
2006 년 숭실대학교 컴퓨터학부 졸업(학사)
2006~현재 숭실대학교 대학원 컴퓨터학과 재학 (석사)
관심분야 : Mobile IP, Security, IPv6, Grid
E-mail : marubazz@sunny.ssu.ac.kr



유 기 성(Kisung Yu)
2004.년 성균관대학교 공과대학 정보공학 석사
2004년~현재 성균관대학교 공과대학 컴퓨터공학과 박사과정
1991년 시스템공학연구소 입소
1998년~1999년 한국전자통신연구원 선임연구원
1999년~ 현재 한국과학기술정보연구원 초고속연구망사업실장
E-mail : ksyu@kisti.re.kr

박 병 연(Byungyeon Park)
1993년 대전산업대학교 재료공학 학사
2004년 공주대 교육정보대학원 교육정보학 석사
2006년~현재 공주대 바이정보학과(정보보호) 박사과정
1990.5~현재 한국과학기술정보연구원 선임연구원
E-mail : bypark@kisti.re.kr

노 민 기(Minki Noh)
2000년 공주대학교 교육정보학 석사
2000년~ 현재 한국과학기술정보연구원 선임연구원
E-mail : mknoh@kisti.re.kr

문 영 성(Youngsong Mun)
1983년 연세대학교 전자공학과(학사)
1986년 Univ. of Alberta 전자공학과 졸업(석사)
1993년 Univ. of Texas, Arlington 전산학과 졸업(박사)
1994년 ~ 현재 숭실대학교 컴퓨터학부 교수
관심분야 : Mobile IP, Security, IPv6, Grid
E-mail : mun@ssu.ac.kr