Return Routability를 이용한 Fast Handovers for Mobile IPv6 인증기법☆

Authentication of Fast Handovers for Mobile IPv6 using Return Routability

신 태 일* 문 영 성**
Teail Shin Youngsong Mun

요 약

Fast Handovers for Mobile IPv6 (FMIPv6) 는 Mobile IPv6의 끊김 없는 핸드오버를 위해 제안된 프로토콜이다. 하지만 FMIPv6의 보안의 취약점을 보완할 수 있는 메커니즘은 현재 미비한 상태이다. FMIPv6의 인증을 위한 현재까지의 대부분의 연구는 Authentication Authorization Accounting (AAA) (5) 또는 공인인증서와 (6) 같은 비대칭 암호알고리즘을 활용하는 Public Key Infrastructure (PKI)와 같은 기술들에 집중 되어있다. 이러한 기술들은 한정된 서비스 도메인만 적용할 수 있거나 복잡한 암호 수식을 처리 하지 못하는 단말기에는 적용할 수 없다는 한계점을 가지고 있다. 따라서 본 논문은 Mobile IPv6의 기본 프로토콜인 Return Routability 만을 사용하여 인증에 필요한 별도의 인프라스트럭처나 많은 처리비용이 필요한 암호 알고리즘 없이 FMIPv6의 인증 메커니즘을 제공하는 방법을 제안한다.

Abstract

IETF has proposed Fast Handovers for Mobile IPv6 (FMIPv6) for efficient mobility management. FMIPv6 has no solutions to protect binding updates. Previous researches have mainly concentrated on using AAA, public certificates or cryptographic algorithms to secure binding updates. However the approaches need a particular infrastructure or a heavy processing cost to setup secure associations for handovers. Proposed scheme provides authentication for FMIPv6 without infrastructure and costly cryptographic algorithms by extending Return Routability Protocol. Also proposed scheme is able to be used for various existing handover mechanisms in IPv6 network.

☞ keyword : MIPv6, Fast Handover, Return Routability, Authentication

1. 서 론

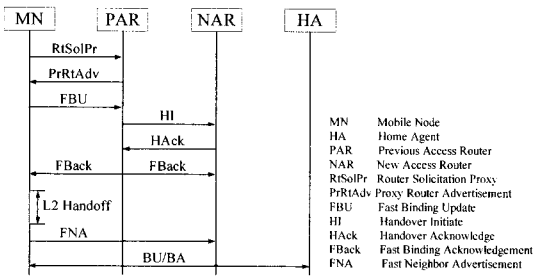
IETF (Internet Engineering Task Force)는 모바일 기기의 IP 계층 이동성을 지원하기 위해 Mobile IPv6 (MIPv6) [1]를 표준으로 정하였다. MIPv6는 단말기가 지금 서비스 받고 있는 Access Router (AR)를 떠나 다른 서브 넷의 AR로 핸드오버 했을 때 IP 상위 어플리케이션 계층의 세션을 재설정 할 필요 없이 유지시키기 위한 Mobility 프로토콜이다. MIPv6의 기본 아이디어는 MN의 영구적인 주소인 Home of Address (HoA)의 프록시 역할을 하는 Home Agent (HA)를 두어 MN이 다른 서브 넷으로 이동했을 때 HA가 MN의 HoA로 보낸 Correspondent Node (CN)의 패킷을 인터셉트해서 현재 MN이 위치하고 있는 CoA로 패킷을 포워딩 하는 것이다. MIPv6에서 IP 계층 상위의 TCP, UDP 등은 MN의 고정적인 식별자인 HoA를 IP 주소로 사용해서 MN가 이동해도 세션을 유지

* 준 회 원 : 숭실대학교 대학원 컴퓨터학과 박사과정
nullx@sunny.ssu.ac.kr
** 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@ssu.ac..kr(교신저자)
[2007/03/28 투고 - 2007/04/06 심사 - 2007/05/22 심사완료]
☆ 이 논문 또는 저서는 2006년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2006-005-J03802)

할 수 있다. 하지만 MIPv6의 핸드오버는 끊김 없는 서비스가 필수인 리얼타임 어플리케이션에 지연시간을 유발 시킨다. 그래서 IETF는 핸드오버 지연기간을 줄이기 위해 FMIPv6를 MIPv6의 핸드오버 프로토콜로 제안하였다. 하지만 FMIPv6는 핸드오버를 수행 할 때 필수적인 MN과 Previous Access Router (PAR) 사이의 보안에 대한 고려를 하지 않고 있다. 인증을 위한 아무런 보안 메커니즘 없이 MN이 FMIPv6의 핸드오버를 요청할 수 있다면 FMIPv6는 Denial of Service (DoS) 또는 DDoS과 같은 공격에 이용될 수 있다. 따라서 본 논문은 Return Routability 프로토콜을 이용하여 인증에 필요한 별도의 인프라스트럭처나 많은 처리 비용이 필요한 암호 알고리즘 없이 FMIPv6의 인증 메커니즘을 제공할 수 있는 방법을 제안한다.

2. 관련 기술

2.1 FMIPv6



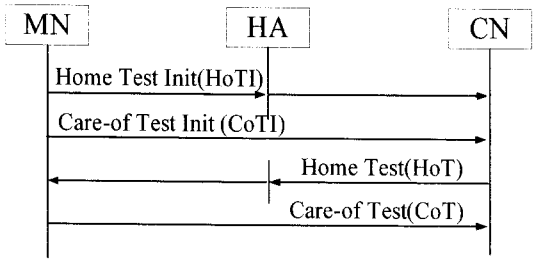
(그림 1) FMIPv6

FMIPv6는 Make Before Break 타입의 핸드오버 프로토콜로서 MN이 Access Point (AP)의 라디오 수신이 약해져서 핸드오버를 할 필요가 있을 때 발생하는 링크 계층의 트리거를 받으면 스캔을 통해 감지한 AP-ID를 RtSolPr에 넣어 보낸다. PAR은 AP-ID에 대응하는 NAR의 prefix와 NAR의 IP 주소를 PrRtAdv를 통해 보낸다. NAR의 prefix를 통해 MN은 NAR에서 사용할 NCoA (New CoA) 자동생성(Auto Configuration)하고 실제 핸드오버를 수행하기 위해 FBU를 보낸다. 이때 PAR과 NAR은 HI와 HAck를 통해 NCoA를 검증하고 (Duplicate Address Detection) MN을 위해 터널을 생성하고 버퍼링을 시작한다. MN이 링크 스위칭을 끝마치고 NAR에 접속하면 NAR에게 FNA를 보내 자신의 접속을 알려 그동안 버퍼링된 패킷의 수신을 요청하고 미리 생성한 NCoA를 HA에게 BU를 통해 등록할 때 까지 터널을 통해 PCoA (Previous CoA)로 통신을 계속한다. 이처럼 FMIPv6는 핸드오버전에 Mobile IPv6에서 필요한 Movement Detection을 링크 계층 트리거를 통해 수행하고 미리 IP address configuration을 통해 새로운 서브 넷에서 사용할 NCoA를 만들기 때문에 Binding Update (BU) 전에도 지연시간 없이 통신이 할 수 있다. 하지만 FMIPv6는 핸드오버를 수행 할 때 MN과 PAR 사이의 보안에 대한 고려를 하지 않고 있어서 공격자가 악의적인 FBU 메시지를 보내서 정상적으로 통신 중이던 노드의 트래픽을 가로채거나 다른 경로로 보내도록 조작하는 것이 가능하다. 그러므로 PAR은 반드시 FBU를 요청한 노드가 실제 그 PCoA를 소유한 노드로부터 온 것이라는 것을 확인 할 수 있는 Address Ownership에 대한 인증이 필요하다.

2.2 Return Routability

MIPv6는 기본적으로 MN이 HA를 거쳐 터널을 통해 CN과 통신하기 때문에 불필요하게 더 긴 경로로 통신해야 한다. 그래서 MIPv6는 MN과 CN이 직접 통신 할 수 있도록 Route Optimization (RO)을 지원한다. RO은 MN이 자신의 CoA를 CN에게 BU를 통해 등록함으로서 이루어진다. 이 때 MN이 CN에게 보내는 BU를 인증하기 위해 사용하는 메커니즘이 Return Routability (RR)이다. RR의 기본적인 아이디어는 HoA와 CoA의 바인딩을 요청하는 MN이 실제로 그 CoA에 존재하고 있는 노드가 맞는 것인지 테스트하는 것이다. 이를 위해 RR은 HoA Test와 CoA Test를 수행한다. 그림

2에서 MN은 RR의 두 가지 테스트를 시작하기위해 HA와의 터널을 통해 HoTI를 보내는 동시에 CN에게 직접 CoTI를 보낸다. 이 두 개의 메시지에 대해 CN은 각각 HoT와 CoT로 응답한다.



(그림 2) Return Routability Procedure

HoT는 nonce index, home keygen token을 가지고 있다. CoT는 nonce index, care-of keygen token을 가지고 있다. home keygen token과 care-of keygen token은 다음의 식과 같이 CN이 자신의 비밀키인 Kcn을 통해 생성한다.

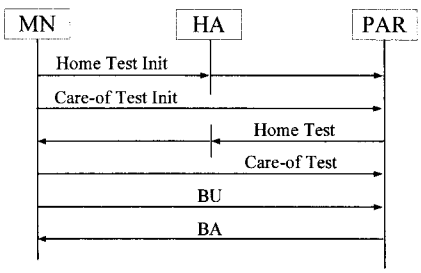
home keygen token =hash(Kcn | HoA | nonce | 0)
care-of keygen token =hash(Kcn | CoA | nonce | 1)

HoA Test를 수행하여 home keygen token을 획득하면 MN은 자신이 실제로 그 HoA에 존재하고 있다는 것을 CN에게 입증할 수 있고 CoA Test를 수행하여 care-of keygen token을 획득하면 MN은 자신이 실제로 그 CoA에 존재하고 있다는 것을 입증할 수 있다. nonce index는 MN이 CN에게 BU할 때 다시 보내서 CN이 두 개의 keygen token을 생성할 때 사용한 nonce를 찾는데 사용된다. 이와 같이 HoA Test와 CoA Test를 수행한 MN은 HoA와 CoA에 동시에 존재하고 있다는 것을 home keygen token과 care-of keygen token 통해 생성한 키인 Kbm으로 입증할 수 있다. Kbm은 MN이 RO를 위해 CN에게 BU할 때 사용된다.

Kbm=SHA1(home keygen token|care-of keygen token)

3. Extended Return Routability

RR은 RO에서 BU를 인증하기 위한 프로토콜이다. 본 논문은 RR 프로토콜을 FMIPv6의 핸드오버 프로토콜에 적용할 수 있는 방법을 제시하여 FMIPv6의 FBU를 인증한다. 본래 RR은 CN이 MN의 HoA로 보낼 트래픽을 현재 위치하고 있는 CoA로 보내는 것을 인가할 때 사용된다. 하지만 FMIPv6에서는 PAR이 MN의 PCoA로 보낼 트래픽을 NCoA로 보내는 것을 인가한다는 점에서 다르기 때문에 단순히 RR을 FMIPv6에 그대로 적용할 수 없다. 따라서 만약 RR을 그대로 FMIPv6에 적용한다면 타겟 호스트와 같은 서브 넷에 있는 공격자가 자신의 HoA를 이용해 home keygen token을 얻고 스푸핑을 통해 타겟 호스트의 care-of keygen token을 요청하고 응답 메시지를 스니핑하여 타켓 호스트로 위장하고 위조된 FBU 메시지를 생성할 수 있다. 이와 같이 RR은 MN의 HoA에 대한 소유권을 기반으로 현재 위치한 CoA로 패킷의 방향을 바꿀 수는 있지만 MN의 CoA에 대한 소유권은 완벽하게 증명할 수 없다. RR을 이용해서 MN이 실제 적법하게 FMIPv6에서의 PCoA에 대한 소유권을 가지고 있는지 입증할 수 있는 기술을 제공하기 위해 본 논문은 FMIPv6와 같은 핸드오버 프로토콜에서 RR이 특별하게 동작할 수 있도록 RR에 HoA와 CoA의 고유한 바인딩을 등록할 수 있는 방법을 제시한다. 이를 위해 RR에 새로운 타입을 정의하고 CN의 Binding Cache를 수정하였다.

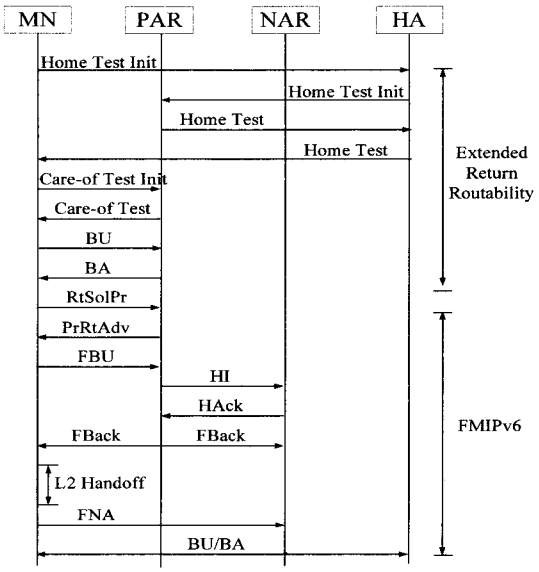


(그림 3) Extended Return Routability Procedure

그림 3이 논문에서 제안하는 Extended Return Routability (ERR)이다. MN이 처음 PAR의 서브 넷에 들어오면 가장 먼저 ERR을 수행한다. 기존의 RR과 같은 똑같은 방법으로 두 개의 keygen token을 수신한 MN은 두 개의 token을 통해 생성한 Kbm으로 사인한 MAC (Message Authentication Code)을 포함하고 ERR 플래그가 세팅된 BU를 PAR에게 보낸다. ERR 플래그가 세팅된 BU를 받은 PAR은 RO가 아닌 확장된 RR을 위한 작업을 수행한다. CN은 수신한 BU의 MAC을 검사하고 이상이 없으면 자신의 Binding Cache에서 MN이 요청한 CoA에 대한 CoA-HoA 바인딩이 존재하는지 확인하고 없다면 MN의 CoA-HoA 바인딩을 Binding Cache에 추가한다. 이렇게 생성된 CN의 Binding Cache의 MN에 대한 CoA-HoA 바인딩이 MN의 CoA에 대한 소유권을 보장한다. 이미 선점된 CoA-HoA 바인딩에 대하여 공격자 자신의 HoA로 타겟 호스트의 CoA와 바인딩을 생성하려는 공격은 불가능하기 때문에 나중에 핸드오버를 위한 FBU를 보낼 때 MAC과 CoA-HoA 바인딩을 통해 인증을 제공 할 수 있다.

FMIPv6에 ERR를 적용하기 위해서는 항상 ERR이 먼저 수행되어 완료되어야 한다. 대부분의 경우 ERR을 수행하고 다른 서브 넷으로 핸드오버까지에는 충분한 기간이 있을 것이다. 이럴 경우 ERR은 FMIPv6의 성능에 전혀 영향을 미치지 않는다. 하지만 MN이 빠른 속도록 자주 서브 넷을 이동할 경우 ERR은 FMIPv6 성능을 저하 시킨다. 다음 장에서 ERR이 FMIPv6 성능에 영향을 주는 두 가지 시나리오에 대해서 성능평가를 할 것이다. 첫 번째는 최적화된 동작을 수행 할 수 없는, MN이 home keygen token과 care-of keygen token을 모두 획득해야 할 normal ERR의 경우이고 두 번째는 MN이 다음 핸드오버할 AR의 home keygen token을 미리 가지고 있어 care-of keygen만 획득하면 되는 optimized ERR 경우이다.

그림 4에서처럼 ERR은 home keygen token을 얻기 위한 과정, care-of keygen token을 얻기 위한 과정, CoA-HoA 바인딩을 등록하기 위한 BU 과정, 크게 세 부분으로 나누어진다. MN의 HoTI와 CoTI는 그림 4에는 나타나지 않지만 동시에 독립적으로 수행된다. 더욱 더 긴 경로를 거쳐야하는 home keygen token을 얻기 위한 시간이 care-of keygen을 얻기 위한 시간보다 길고 ERR 지연시간의 대부분을 차지한다. 따라서 MN이 미리 다음 핸드오버할 AR의 home keygen token을 받아 놓는다면 ERR의 수행시간은 굉장히 짧아지게 된다. 이를 optimized ERR이라 한다.



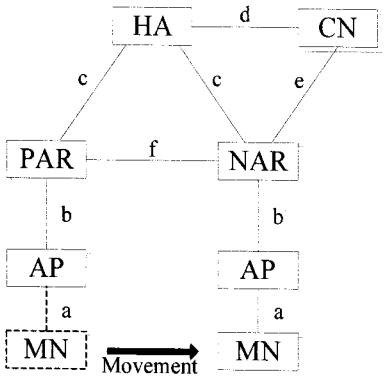
(그림 4) ERR 이 적용된 FMIPv6

4. 성능평가

4.1 시스템 모델

그림 5는 ERR의 성능평가를 위한 시스템 모델이다. CN은 MN에게 평균 λ로 데이터를 송신하고 MN은 평균 μ로 다른 서브 넷으로 이동한다고 가정한다. Packet to Mobility Ratio (PMR p)는 MN이 하나의 서브 넷에 머무르는 동안 CN으로부터 수신하는 패킷의 평균수로 $p=\lambda/\mu$이다.

시스템 모델에서 패킷을 전송하는 비용은 송신 노드와 수신 노드의 거리(Hop)에 비례하고 데이터 패킷을 전송하는 비용은 컨트롤 패킷을 전송하는 비용의 l배 ($l = l_d / l_c$)라고 가정한다. l_d는 데이터 패킷의 평균 크기이고, l_c는 컨트롤 패킷의 평균 크기이다. 컨트롤 패킷을 처리하기 위한 평균 처리 비용은 r이다. [3]



(그림 5) 시스템 모델

4.2 핸드오버 지연시간

핸드오버 지연시간은 링크 스위칭 지연시간, IP 재연결 지연시간, 위치 갱신 지연시간으로 구성된다. 링크 스위칭 지연시간은 링크계층의 핸드오프에 걸리는 시간이다. IP 재연결 지연시간은 MN이 Movement Detection을 수행하고 IP Address Configuration을 마치기까지의 시간이다. MN이 IP 재연결을 끝마친 후 새로운 CoA를 BU를 통해 HoA와 바인딩하는 시간이 위치 갱신 지연시간이다. MIPv6의 총 지연시간은 다음과 같다.

$$T_{L2} + T_{IPbasic} + T_{BUHA} + T_{BUCN}$$

T_{L2}는 링크 스위칭 지연시간이고 링크를 스캔하는 T_{L2Scan}와 실제로 링크 핸드오프를 수행하는 T_{L2exec}시간으로 나누어진다. $T_{IPbasic}$는 IP 재연결 지연시간으로 Movement Detection을 위한 T_{MD}와 Address Configuration을 위한 T_{AC}으로 나누어진다. T_{BUHA}는 HA에게 MN의 위치를 갱신하는데 걸리는 시간이다. T_{BUCN}는 CN에게 MN의 위치를 갱신하는데 걸리는 시간이다. FMIPv6의 총 지연시간은 다음과 같다.

$$T_{IP} + T_{L2exec} + T_{IPfast} + T_{BUHA} + T_{BUCN}$$

FMIPv6는 Movement Detection(T_{MD})과 IP Address Configuration(T_{AC})을 링크 스위칭 전에 미리 수행한다. FMIPv6는 T_{FtoH}와 T_{HtoF}를 통해 Movment Detection을 수행한다. T_{FtoH}는 MN이 FBU를 보내고 HI를 받는데 걸리는 시간이고 T_{HtoF}는 Hack를 보내고 FBack를 받는데 걸리는 시간이다. FMIPv6는 핸드오버전에 링크 스캔을 미리하기 때문에 링크 스위칭 지연시간은 T_{L2exec}이다. T_{IPfast}는 MN이 FNA 메시지를 보내는데 걸리는 시간이다.

본 논문이 제안하는 ERR의 총 지연시간은 FMIPv6를 시작하기 전에 ERR를 먼저 수행하는 시간(T_{ERR})외에는 FMIPv6와 동일하다. T_{ERR}은 T_{HT}, T_{CT}, T_{EBU}로 구성된다. T_{HT}는 MN이 home keygen token을 얻는 데 걸리는 시간이고 T_{CT}는 care-of keygen token을 얻는데 걸리는 시간이다. T_{EBU}는 MN이 Kbm를 통해 사인한 BU를 보내 CoA-HoA 바인딩을 생성하는 데 걸리는 시간이다. T_{HT}와 T_{CT}는 동시에 수행가능 하기 때문에 둘 중 더 오래 걸린 것을 지연시간으로 한다. normal ERR의 총 지연시간은 다음과 같다.

$$\max(T_{HT} + T_{CT}) + T_{EBU} + T_{IP} + T_{L2exec} + T_{IPfast} + T_{BUHA} + T_{BUCN}$$

optimized ERR에서 MN은 미리 home keygen token을 가지고 있기 때문에 총 지연시간은 다음과 같다.

$$T_{CT} + T_{EBU} + T_{IP} + T_{L2exec} + T_{IPfast} + T_{BUHA} + T_{BUCN}$$

4.3 비용분석

본 논문은 FMIPv6 대비 normal ERR과 optimized ERR의 성능을 Overall Cost (CO)를 통해 비교한다. CO는 시그널링 비용과 전송 비용으로 나누어지고 다음 식 1과 같다.

$$CO = CS + CD \tag{1}$$

CS는 모든 시그널링 메시지 비용의 총 합이고 CD는 핸드오버 수행 중에 일반 데이터를 전송하는 비용의 총 합이다. FMIPv6와 ERR에서의 시그널링 비용은 다음 식과 같다.

$$CS_{FMIPv6} = CS_{fast} + CS_{IPfast} + CS_{BUHA} + CS_{BUCN} \tag{2}$$

$$CS_{ERR} = CS_{HT} + CS_{CT} + CS_{EBU} + CS_{fast} + CS_{IPfast} + CS_{BUHA} + CS_{BUCN} \tag{3}$$

각각의 CS_{IPfast}, CS_{fast}, CS_{BUCN} 등은 핸드오버 지연시간에서 설명한 동작을 수행하는데 드는 시그널링 비용이다. 전송비용은 포워딩 비용과 손실 비용으로 나누어지며 다음 식과 같다.

$$CD_{FMIPv6} = P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6Handover} \tag{4}$$

$$CD_{ERR^1} = P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{ERR^1} + T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6Handover} \tag{5}$$

$$CD_{ERR^2} = P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{ERR^2} + T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6Handover} \tag{6}$$

CD_{preNet}은 CN이 MN이 이동하기전의 PAR 서브 넷으로 데이터를 전송할 때의 비용이고 CD_{newNet}는 CN이 MN이 이동한 새로운 NAR 서브 넷으로 데이터를 전송할 때의 비용이다. $CD_{newNetTunnel}$은 FMIPv6 핸드오버 동안에 PAR과 NAR 사이의 터널을 통해서 데이터를 전송할 때의 비용이다. FMIPv6 핸드오버의 성공률은 $P_{suc.}$이고 실패율은 P_{fail}이다 [3]. η은 패킷 손실로 인한 재전송 비용의 가중치이다. FMIPv6가 실패했을 경우 핸드오버 동안의 모든 패킷은 손실되고 MN은 MIPv6 핸드오버를 대신해서 수행한다. CD_{FMIPv6}와 CD_{ERR}은 ERR을 수행하는데 걸리는 시간인 T_{ERR}을 빼고 동일하며 normal ERR과 optimized ERR의 전송비용을 CD_{ERR^1}과 CD_{ERR^2}로 나누어서 성능평가를 진행하였다.

4.4 성능평가 결과

MN, CN, AR이 유선과 무선으로 연결 된 시나리오를 위해 [4]의 empirical communication delay model을 사용하여 수집된 데이터의 회기 분석 결과 도출된 식 7, 8을 참조 하였다.

$$T_{wired-RT}(h,k) = 3.63k + 3.21(h-1) \tag{7}$$

$$T_{wireless-RT}(k) = 17.1k \tag{8}$$

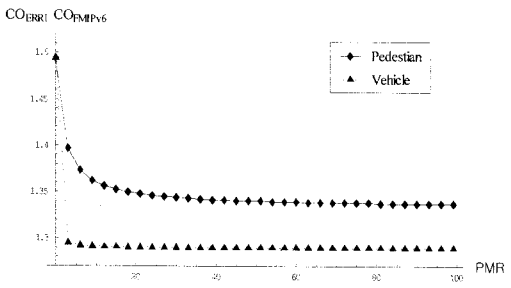
k는 패킷의 크기로 KB단위이다. h는 홉의 수이다. $T_{wired-RT}$은 round-trip 시간(ms)이다. MN이 보행자 속도(3.6km/H: $\mu = 0.01$)로 이동할 때와 빠

른 속도(108km/H: $\mu = 0.5$)로 이동할 때의 전체 비용을 식 1을 통해 FMIPv6 대비 normal ERR의 성능과 FMIPv6 대비 optimized ERR의 성능으로 계산한 결과가 다음 식 (9), (10)이다.

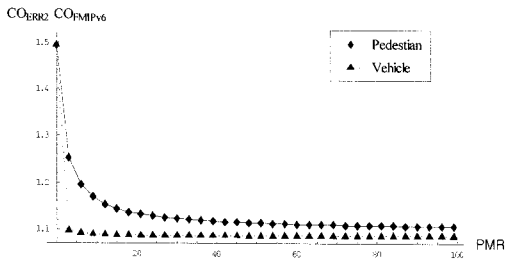
$$\lim_{p\to\infty}\frac{CO_{ERR^1}}{CO_{FMIPv6}} = \lim_{p\to\infty}\frac{CS_{ERR}+CD_{ERR^1}}{CD_{FMIPv6}+CD_{FMIPv6}} \approx 1.337 \quad (9)$$

$$\lim_{p\to\infty}\frac{CO_{ERR^2}}{CO_{FMIPv6}} \lim_{p\to\infty}\frac{CS_{ERR}+CS_{ERR^2}}{CD_{FMIPv6}+CD_{FMIPv6}} \approx 1.106 \quad (10)$$

그림 10과 11에 보듯이 MN이 108Km/h로 이동할 때 normal ERR은 FMIPv6에 비해 33%의 오버헤드가 있으며 optimized ERR은 10%의 오버헤드가 발생한다. 이처럼 제안된 기법은 PAR에서 바로 핸드오버 하는 경우에도 약간의 오버헤드를 통해 MN의 인증을 제공할 수 있고 MN이 미리 핸드오버할 NAR 주소를 알 수 있는 optimized ERR을 수행 할 수 있는 환경이라면 오버헤드는 미미한 것을 확인 할 수 있다.



(그림 10) MIPv6 타이밍 다이어그램



(그림 11) MIPv6 타이밍 다이어그램

5.결론

FMIPv6의 인증을 제공하기 위한 현재까지의 대부분의 연구는 AAA를 이용하거나 공인인증서를 적용한 비대칭 암호기법을 사용하는 방법을 주로 모색해 왔다. 이러한 방법은 특정한 도메인에서만 적용 가능하다는 단점과 인증을 위한 지연시간이 길다는 단점이 있다. 본 논문은 인증을 위해 복잡하고 처리시간이 오래 걸리는 새로운 프로토콜을 정의 하지 않고 IETF의 기본 프로토콜인 RR을 FMIPv6에 적용할 수 있는 방법을 제시함으로써 짧은 지연시간을 갖고 인프라스트럭처가 필요 없는 인증기법을 제공한다.

참 고 문 헌

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

[2] Koodli, R.: Fast Handovers for Mobile IPv6, RFC 4068, 2006

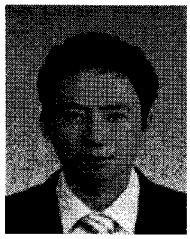
[3] Jain, R., Raleigh : Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers, in Proc. ICC'98 Conf., pp1690-1695, 1998

[4] Vatn, J.: An experimental study of IEEE 802.11b handover performance and its effect on voice traffic, Telecommunication Systems Laboratory Department of Microelectronics, 2003

[5] V. Narayanan: Handover Keys using AAA, Draft, 2007

[6] Gabriel Montenegro, Claude Castelluccia : Crypto-based identifiers (CBIDs): Concepts and applications, ACM Transactions on Information and System Security (TISSEC), 2004

◐ 저 자 소 개 ◑



신 태 일(Teail Shin)
2005년 숭실대학교 컴퓨터학부 졸업(학사)
2007년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
2007~현재 숭실대학교 대학원 컴퓨터학과 박사과정
관심분야 : Mobile IPv6, IPv6, 3GPP
E-mail : nullx@sunny.ssu.ac.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