# Proxy Mobile IPv6 네트워크에서 포워딩 모드를 지원하는 인증기법의 성능분석☆

# Performance Analysis of Proxy-AAA Authentication Scheme in PMIPv6 Networks with Forwarding Mode Supporting

이 승 현* 신 동 렬** 정 종 필***
Seung-Hyun Lee Dong-Ryeol Shin Jongpil Jeong

**요 약**

모바일 IP 환경 내 MN의 이동 과정에서 인증은 초기화되고, 이러한 시작점으로부터 과도한 비용이 발생한다는 전제하에 현재까지 연구는 특정 상황에서의 비용 감소의 요구사항을 명확히 제시하지 못하고 있다. 본 논문에서는 이런 점에 착안한 제안 기법은 계층적 AAA (Authorization, Authentication, Accounting)로부터 발전되어 빠른 인증과 Diameter 프로토콜 기반의 모바일 IP를 지원하며, AAA 서버는 LMA (Local Mobility Anchor)에 배치하여 짧고 간단한 빠른 이동 인증과 계층적 인증을 통해 도메인 내 인증에서의 비용을 줄여준다. 제안하는 Proxy-AAA 기법은 기존 인증기법들과 바인딩 업데이트 기법들을 개선하였으며 도메인 내 이동과 인증뿐만 아니라 도메인 간에서도 적용된다. 이를 수학적 모델링과 성능 평가를 통해 기존의 단점을 보완할 수 있음을 보여준다.

**ABSTRACT**

Mobile IPv6 (MIPv6) is a host-based protocol supporting global mobility while Proxy Mobile IPv6 (PMIPv6) is a network-based protocol supporting localized mobility. This paper makes its focus on how to reduce the longer delay and extra cost arising from the combination of authentication, authorization and accounting (AAA) and PMIPv6 further. Firstly, a novel authentication scheme (Proxy-AAA) is proposed, which supports fast handover mode and forwarding mode between different local mobility anchors (LMAs). Secondly, a cost analysis model is established based on Proxy-AAA. From the theoretical analysis, it could be noted that the cost is affected by average arrival rate and residence time.

☞ keyword : 프록시, 모바일 IPv6, 포워딩, 인증, Proxyl; mobile IPv6, forwarding, Authentication

## 1. 서 론

무선 액세스 네트워크를 위한 사용자 인증 과정에서는 문자열의 노출로 인해 보안 이슈는 중요하다. AAA (Authentication, Authorization, Accounting) 기술은 모바일 환경에서 인증과정에서 발생되는 지연 문제를 해결하는 최적의 기법으로 알려져 있다 [1]. 그러나 AAA 기술이 수년 동안 발전했음에도 불구하고 이동성 측면에서의 연구는 아직 완전하지 않다. 즉, 기존의 AAA 보안성과 이동성 관리 프로토콜(MIPv6, PMIPv6 등)의 결합은 완전하지 않은 상태이다. 예로서 UDP 기반의 RADIUS 프로토콜은 빠른 이동성 제공에 있어 적합하지 않다는 단점을 들 수 있다. 그래서 등장하게 된 향상된 RADIUS 버전인 Diameter 프로토콜은 실패 복구, 보안, 신뢰성 부분에서 강화된 능력을 보인다 [2].

현재 보안과 이동성에 관한 이슈에 대해 관련 단체나 연구소에서 많은 연구를 수행 중이다. IETF(Internet Engineering Task Force)는 AAA 기술과 이동성 관리를 결합한 응용 모델인 AAA를 위한 모바일 IP 응용을 제안하였다. 그러나 역시 몇 가지 문제점이 지적되고 있다. 그 중 몇 가지 사례를 나열하면 IETF의 WG에서는 MN (Mobile Node)의 암호처리 과정의 오버헤드를 줄이고 보안강도를 높이기 위한 방법으로 RR(Return Routability) 기법을 사용하도록 권고하고 있다. 그러나, RR 기법은 송수신 패킷 자체에 암호학적인 연산이 없는 패킷의 상

* 정 회 원 : 성균관대학교 일반대학원 전기전자컴퓨터공학과 박사수료 lshyun0@ece.skku.ac.kr
** 정 회 원 : 성균관대학교 정보통신공학부 교수 drshin@ece.skku.ac.kr
*** 정 회 원 : 성균관대학교 정보통신공학부 졸업(공학박사) jpjeong@skku.edu
[2011/09/20 투고 - 2011/09/22 심사 - 2011/12/26 심사완료]
☆ 본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행한 것임.(2011-0027030)

태로 전달 경로 상에 공격을 가하는 경우, 쉽게 패킷의 내용을 확인할 수 있다는 단점을 가지고 있다. [4]에서는 MIPv6 환경에서 메시지 기반 MIPv6 기술과 결합된 Diameter 프로토콜을 설명하고 있다. 이 기술은 상호작용 수와 오버헤드를 줄이기 위해 이동 요청 정보에 AAA 프로토콜 메시지를 압축한다. 그러나 이 기법은 도메인 내에서의 이동 시에만 적용된다. 이동하는 사용자가 급속히 증가하면서 인증 메시지의 수도 증가한다. 각 인증은 지연을 줄이기 위해 높은 조건으로 홈 네트워크들과 소통을 필요로 한다. [5]는 L2 기반의 빠른 변환 아이디어를 제안한다. [5]에서 제시한 방안은 링크계층에서 연결해제 시간을 이용하여 인증 요청 메시지의 전송 시 전체적인 지연시간과 시그널링 비용을 상당히 줄여준다. 그러나 이 기법은 도메인 간 이동 시에만 적용된다는 단점을 가지고 있다. [6]의 연구에서는 HMIPv6(Hierarchical Mobile IPv6)와 AAA 기술을 결합하여 AAA 인증 기반의 최적화된 HMIPv6를 보여준다. 이 기법은 사용자에 의한 네트워크 인증 요구는 배제하고 네트워크에 의한 사용자 계정 인증 요구만 적용된다. 즉, 한번의 상호 인증이 고려되었으며 추가적인 상호작용이 반드시 필요하다. [7]의 HMIPv6 네트워크에서의 빠른 인증을 지원하며 더 나아가 도메인 내 인증의 비용을 줄이는 방법을 제시한다. 그러나 도메인 간 인증을 지원하지는 않는다. 다른 이동성 관리 프로토콜에 비해 네트워크 주도의 이동성 관리 프로토콜인 PMIPv6(Proxy Mobile IPv6) 역시 많은 주의를 끌었다. PMIPv6는 MIPv6에서 강화된 것이며 모바일 장치들을 지원하는 네트워크 기반의 로컬 이동성 관리를 제공한다. 이들의 다른 특징 때문에 PMIPv6는 MIPv6와 함께 사용된다. 사례로는 Giaretta의 제안을 들 수 있으며, MIPv6는 글로벌 이동성에 사용되고 PMIPv6는 로컬 이동성에 사용된다 [8]. 이 경우, 각 도메인 내외에서 접근 시 서로 다른 프로토콜에 따른 추가적인 비용 부담이 야기될 수 있다는 단점을 가지고 있다.

본 논문에서는 앞에서 언급한 기법들의 단점을 보완하기 위한 방안으로 PMIPv6 내에서의 Proxy-AAA 인증 기법을 제시한다. AAA 서버는 LMA에 배치되며 짧고 간단한 빠른 이동 인증과 계층적 인증을 통해 도메인 내 인증에서의 비용을 줄여준다. 그리고 도메인 간의 이동과 인증 과정에서 AAA 서버 기반의 세션키를 재사용하며 LMA들간 직접 전송하도록 유도하여 전체 시스템의 시그널링 오버헤드를 줄여준다. 그리고 기존 MIPv6와 Proxy-AAA 기법의 성능을 평가하여 적절한 프로토콜의 선택을 제공한다. 즉, 네트워크의 상태와 이동성 매개변수 값들에 따라 보다 나은 프로토콜을 선택할 수 있다. 성능평가 결과, 제안하는 Proxy-AAA 기법의 시그널링 오버헤드가 기존 AAA기법보다 항상 작은 값임을 확인할 수 있다. 그리고 MN이 홈 도메인으로부터 멀어질수록 제안기법이 기존 AAA기법보다 효율성이 좋으며 전체 오버헤드 역시 Proxy-AAA기법이 항상 적게 나타나며, 이는 도메인간 이동의 경우 기존 AAA기법에 비해 상당히 효율적임을 나타낸다.

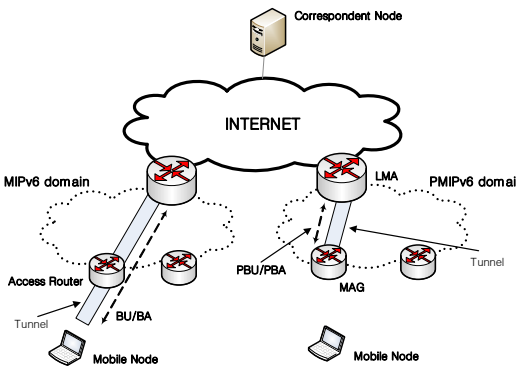
본 논문의 구성은 다음과 같다. 2장에서는 MIPv6와 PMIPv6에 대해 설명하며, 3장에서는 제안하는 Proxy-AAA 기법과 프로토콜 선택 기법에 대해 제시한다. 그리고 4장에서 기존 AAA기법과 제안하는 Proxy-AAA 기법의 성능을 비교하고 평가하며, 마지막으로 5장에서 결론을 논한다.

## 2. 관련 연구

본 장에서는 제안 기법의 설명에 앞서 MIPv6와 PMIPv6의 동작과정에 관해 설명한다.

### 2.1 MIPv6

MIPv6는 IETF에 의해 표준화된 글로벌 이동성을 지원하는 단말들을 위한 이동성 관리 프로토콜이다. 그러나 MIPv6는 MN의 호스트 기반 이동성 지원이 요구되며 MN의 잦은 서브넷간 이동 시 높은 이동성 시그널링 오버헤드가 발생된다. MIPv6는 적어도 두 개의 주소에 의해 MN의 이동성을 지원하며, HoA(Home of Address)는 HA(Home Agent)에 의해 고정된 주소를 제공하고 CoA (Care-of Address)는 MN이 새로운 서브넷으로 이동할 때 외부 액세스 네트워크의 변경 정도를 얻는다. MIPv6에서의 위치 업데이트와 패킷 전달 절차는 다음과 같다. MIPv6의 위치 업데이트는 MN이 홈 도메인에 머무를 때 패킷들을 정해진 HoA로부터 받고 일반적인 IP 라우팅 메커니즘에 의해 전달된다. MN이 현재 네트워크를 지나 다른 AR(Access Router)로 접근할 때 접근한 새로운 접속점의 CoA를 획득하여 이동 탐지가 이루어 진다. 새로운 CoA 설정을 위해 MN은 HA에 BU(binding update) 메시지를 보내어 새로운 위치를 등록한다. MIPv6 패킷 전달은 MN이 홈 네트워크로부터 멀어질 때 HA는 바인딩 업데이트를 수행하며 MN들의 프록시 객체에서 이루어 진다. 이것은 HA가 MN으로의 모든 NS(neighbor solicitation)에 응답하기 때문에 HA에서 MN의 패킷 주소가 만료되는 것을 의미한다. HA가 가로챈 패킷을 가지며 그 패킷을




(그림 1) MIPv6와 PMIPv6 네트워크 구조

터널 내에서 압축하고 MN들의 현재 CoA에게 전달한다. 터널 헤더는 HA들의 주소를 시작 주소로 가지고 MN들의 CoA를 목적지 주소로 가진다. MN은 CN(Corresponding Node)에서 직접 MN에게 보낸 패킷을 압축 해제하여 원본 패킷으로 만든다. MN이 CN과의 연결이 이루어지지 않았을 때는 HA를 이용한 역 터널링 절차를 통하여 CN으로 패킷을 보낼 수 있다.

## 2.2 PMIPv6

PMIPv6는 네트워크 기반의 이동성 관리를 사용하여 시그널링 오버헤드를 줄이고 MN의 호스트 기반 이동성 스택이 불필요하게 된다. PMIPv6는 로컬 이동성 관리 도메인만 지원한다.

PMIPv6에서의 위치 업데이트와 패킷 전달 절차는 다음과 같다. PMIPv6의 위치 업데이트는 MN이 LMD(Local Mobility Domain)로 이동할 때 MAG과 LMA 사이의 터널 연결을 위해 MAG은 PBU(Proxy Binding Update) 메시지를 LMA로 보낸다. 이 터널은 MN으로 들어오거나 나가는 패킷의 경로 선택에 사용된다. MAG로부터 PBU 메시지를 받으면 LMA는 MN이 현재 MAG 아래에 있는 것을 인식하고 MN의 세션과 경로 정보를 관리하는 BCE(binding cache entry)를 사용할 수 있다. 그리고 MN은 LMA에 의해 할당된 HNP(Home Network Prefix)가 포함된 RA(Router Advertisement) 메시지를 MAG로부터 받는다. MN은 Prefix 정보를 기반으로 주소를 생성한다. 만약 MN이 MAG1에서 MAG2로 이동하면 MAG2 역시 PBU 메시지를 LMA에게 보내고 MAG2와 LMA간에 터널을 연결한다. 그 이유는 MAG2 역시 동일한 HNP를 MN에게 보내고 MN은 IP 레벨 이동성을 따르지 않으며 MN의 IP 주소는 바뀌지 않기 때문이다. 그래서 MN은 LMD에서 이동성 관련 시그널에 관계없이 이동할 수 있다. PMIPv6의 패킷 전달은 CN으로부터 패킷이 전송되면 라우팅 프로토콜에 따라 LMA로 전달된다. LMA의 BCE를 기반으로 MN과 터널 연결을 하는 MAG에게 패킷이 전달된다. 터널의 끝은 각각 LMA와 MAG의 주소이다. 마지막으로 MAG는 MN에게 패킷을 전송한다. 모든 역방향 패킷들은 MAG에서 LMA로 연결되어 있다. 터널 헤더가 제거된 후에는 내부 패킷의 헤더에 의해 LMA가 목적지로 전송한다. MIPv6은 MN이 글로벌 이동할 때 도달 가능성 유지를 허용하지만 이는 세 가지 문제점을 가진다.

(1) 바인딩 업데이트 지연: 만약 HA가 MN들 액세스 네트워크로부터 멀리 있다면 총 시간 중 글로벌 이동성 업데이트에 대한 고려가 필요하다. 이 과정 동안 패킷은 예전 주소의 경로 설정이 계속되어 기본적으로 버려진다.
(2) 시그널링 오버헤드: MN이 하나의 last-hop 링크에서 다른 쪽으로 이동할 때 상당히 큰 시그널이 요구된다. 새로운 링크에서의 IP 주소 설정과 영구적인 HoA와 CoA의 매핑을 바꾸기 위한 네트워크 내부로의 글로벌 이동성 프로토콜 시그널링 요구를 포함한다. 시그널링의 량은 무선 대역폭 사용과 실시간 서비스 성능에 부정적인 영향을 미친다.
(3) 위치 보호: MN의 CN들을 위한 토폴로지 위치 이동과 잠재적인 도청자를 위해 CoA를 바꾼다. 공격자는 MN의 액세스 네트워크 내 서브넷을 고정하고 MN의 지리적인 위치를 정확히 알아내어 조합할 수 있다.

반면, PMIPv6는 MN의 LMD내에서의 지역적인 이동만 핸들링 할 수 있는 네트워크 기반의 방법이다. PMIPv6는 per-MN-prefix 모델을 사용한다. 그래서 유일한 HNP는 각 MN에 부여되며 다른 MN과 공유되지 않는다. MN이 PMIPv6 도메인에서 이동하는 동안 고정되어 있어 처음으로 PMIPv6 도메인에 접근할 경우를 제외하면 네트워크 계층 이동 탐지와 주소 설정 과정이 필요하지 않다. 그래서 이동 지연과 시그널링 오버헤드를 줄일 수 있다. PMIPv6에서는 각 MN이 아닌 LMA와 MAG간 터널이 연결된다. 그 이유는 MN은 이동 관련 시그널을 포함하지 않기 때문이다. 이로 인해 MN의 위치 보호가 보장될 수

있다[9].

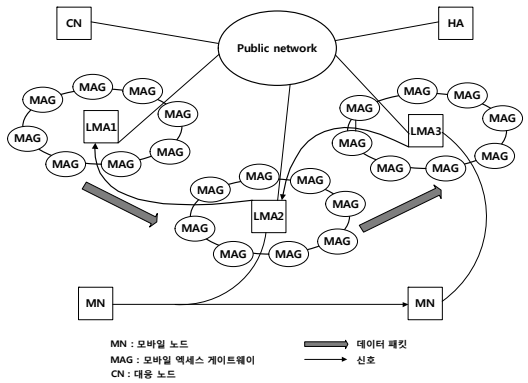
본 논문에서 제안한 PMIPv6 기반의 Proxy-AAA 기법은 PMIPv6의 도메인 내 인증과 도메인 간의 인증 정책, 프로토콜 선택 과정의 전체 오버 헤드의 계산 및 바인딩 업데이트 비용 등으로 성능 평가 지표를 표시한다. 본 논문에서 제시한 기법의 성능 평가를 위하여, PMIPv6 기반의 Proxy-AAA 기법에서 전체 시스템의 오버헤드는 두 가지 구성한다. 첫째는 시그널링 제어 오버헤드와 둘째는 데이터 전송 오버헤드이다. 시그널링 제어 오버헤드는 인증 시그널링 제어 오버헤드와 등록 시그널링 제어 오버헤드가 포함된다. 이는 앞서 제시한 MIPv6와 PMIPv6 사이의 공존 관계가 성립되는 상황에서의 결과보다 다른 성능 평가 결과를 보여준다. 이것은 AAA 서버 기반의 세션 키를 재사용함으로써 LMA들간 직접 전송하도록 유도하여 전체 시스템의 시그널링 오버헤드를 줄일 수 있기 때문이다. 본 논문의 4장에서는 차량과 보행자의 이동의 경우에 대하여 성능 평가를 수행한다. 이는 4장에서 보다 자세히 다룬다.

## 3. 제안 기법

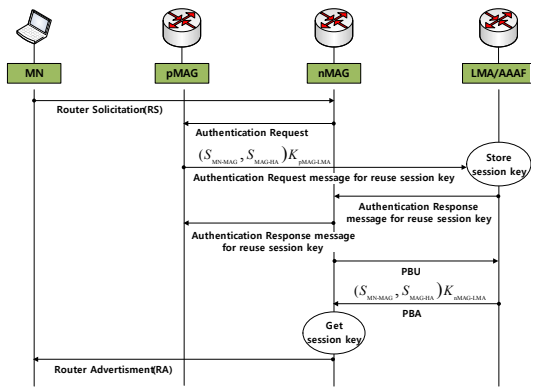
모바일 IP 환경 내 MN의 이동 시 인증은 초기화되기 시작하여, 이러한 시작점을 시작으로 과도한 비용을 발생한다는 전제하에 현재까지 연구 성과에서는 특정 상황에서의 비용 발생의 요구사항을 해결하지 못하였다. 본 장에서는 이러한 해결책으로 PMIPv6 기반의 Proxy-MIPv6 AAA 인증기법을 제안한다.

### 3.1 Proxy-AAA 기법

제안 기법은 계층적 AAA로부터 발전되어 빠른 인증과 Diameter 프로토콜 기반의 모바일 IP를 지원한다. AAA 서버는 LMA에 배치될 것이며 짧고 간단한 빠른 이동 인증과 계층적 인증을 통해 도메인 내 인증에서의 비용을 줄여줄 것이다. 제안하는 Proxy-AAA 기법은 기존 인증기법들과 바인딩 업데이트 방법들을 개선하였으며 도메인 내 이동과 인증뿐만 아니라 도메인 간에서도 적용된다. 도메인 내에서의 Proxy-AAA는 계층적 모바일 IPv6의 이동과 인증 과정에서 LMA 기반의 세션 키를 재사용한다. 도메인 간의 Proxy-AAA는 이동과 인증 과정에서 AAA 서버 기반의 세션 키를 재사용하며 LMA들간 직접 전송하도록 유도한다. 연결되어 있는 LMA들은 직접 정보를 전송하고 게다가 HA까지 연결되어 (그림 2)에서



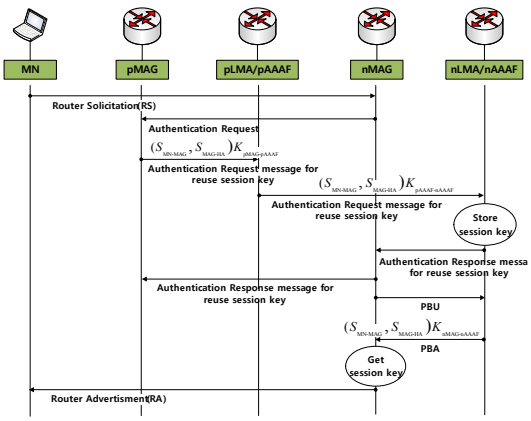

(그림 2) 다른 LMA간 전달 기법




(그림 3) 도메인 내의 이동 흐름

처럼 전체 시스템의 시그널링 오버헤드를 상당히 줄여줄 수 있다. MN이 네트워크 영역의 왼쪽에서 오른쪽으로 이동할 때 LMA1, LMA2를 거쳐 LMA3까지 이동한다. MN이 LMA2 영역에 도착할 때 BU 메시지를 LMA2로 보내고 LMA2는 LMA1에게 전달한다. LMA1이 메시지를 받으면 저장된 LMA 리스트와 비교하고 이 MN에 적절한 정보를 조사하여 현재 LMA 주소의 MN으로 업데이트한다. LMA1은 HA를 거치지 않고 LMA2로 패킷 데이터를 직접 전달한다.

(그림 3)은 도메인 내 이동과정에서의 메시지의 흐름을 보여준다. MN이 nMAG로부터 통지를 받으면 MN은 세션키를 재사용하기 위해 pMAG로 인증요청 메시지를 보낸다. 요청을 받으면 pMAG은 $K_{\mathrm{pMAG-LMA}}$를 이용하여 세션키 $S_{\mathrm{MN-MAG}}$와 $S_{\mathrm{MAG-HA}}$를 암호화하고 이를 LMA에게 보낸다. LMA는 암호화된 세션키를 저장하고 재사용 응답 메시지를 nMAG을 거치지 않고 MN에게 보




(그림 4) 도메인 간의 이동 흐름

낸다. MN은 응답을 받으면 등록 요청 메시지를 nMAG을 통하여 LMA에게 보낸다. LMA은 요청을 받으면 세션키 $S_{\mathrm{MN-MAG}}$와 $S_{\mathrm{MAG-HA}}$를 암호화하기 위해 $K_{\mathrm{nMAG-LMA}}$를 사용하고 그 키를 MN에게 전달한다. 그러면 MN과 LMA 사이에 신뢰된 바인딩 업데이트 채널이 생성된다.

(그림 4)는 도메인 간의 이동에서 메시지 흐름을 보여준다. 다른 도메인 간의 업데이트 절차는 (그림 3)의 도메인 내의 흐름과 유사하나, pLMA이 다른 도메인의 nLMA/ AAAF로 전달하는 과정이 추가되며, 이는 외부에서 메시지를 받아 전달되도록 하는 과정으로 바인드 업데이트가 유지되도록 한다.

### 3.2 프로토콜 선택

네트워크와 MN들에게 가장 적합한 이동성 관리 프로토콜을 선택하기 위해 인증과정 동안 MAG는 MN들의 프로필로부터 MN의 선호도를 찾는다. MN들이 액세스 네트워크에서 선호하는 프로토콜을 비교하고 선택한다. 반면, MN들의 선호도는 높은 우선권을 갖는다. 만약 MN이 선호도를 가지고 있지 않다면 기본 MIPv6와 Proxy-AAA 기법의 성능을 평가하여 적절한 프로토콜을 선택한다. 기본 MIPv6와 Proxy-AAA 기법의 성능 평가를 위해 MAG에 의한 탐색으로 경로 반응시간을 확인한다. 경로가 탐색되는 동안 MAG는 두 개의 탐색 메시지를 LMA에게 보낸다. 하나는 nLMA를 지나 pLMA로 전달되고 이 RTT(Round-Trip Time)를 $RTT_{\mathrm{Proxy-AAA}}$로 표시한다. 다른 탐색 메시지는 pLMA로 직접 보내지고 이 RTT를 $RTT_{\mathrm{mip}}$로 표시한다. $n$시간 동안의 경로 탐색 후 MIPv6 경로의 평균 RTT($\overline{z}_n$)는 다음과 같이 계산될 수 있다.

$$\overline{z}_n = \alpha RTT_{mip}(n) + (1-\alpha)\overline{z}_{n-1} \quad (1)$$

매개변수 $\alpha$는 평균 계산에서 지난 이벤트들의 가중치을 나타낸다. 예를 들어 우리가 $\alpha$를 0.8로 설정하면 가장 최근 값 $z_{n-1}$은 $z_n$ 값의 20% 가중으로 계산된다. 만약 $\alpha$ 값을 신중히 선택한다면 이력 현상을 피할 수 있다[10]. 가변적인 $z$는 다음과 같이 초기화할 수 있다.

$$\overline{z}_0 = RTT_{mip}(0) \quad (2)$$

비슷한 방법으로 Proxy-AAA 기법의 평균 RTT를 계산할 수 있으며 이를 $\overline{t}_n$으로 표시한다. 기본 MIPv6의 경로 반응시간이 우리의 Proxy-AAA보다 작고 MN의 이동 빈도가 낮을 때는 기본 MIPv6의 성능이 좋다. 반면 기본 MIPv6의 반응시간이 우리의 Proxy-AAA 기법보다 작지 않고 MN의 이동 빈도가 높을 땐 Proxy-AAA기법의 성능이 좋다. 다음과 같은 프로토콜 선택 기준은 네트워크의 상태와 이동성 매개변수 값들에 따라 보다 나은 프로토콜을 선택하도록 한다.

$$\frac{\overline{t}_n - \overline{z}_n}{N_{\mathrm{h}}} < H_{\mathrm{t}}, \text{ Proxy-AAA기법 선택}$$
$$\frac{\overline{t}_n - \overline{z}_n}{N_{\mathrm{h}}} \geq H_{\mathrm{t}}, \text{ 기본 MIPv6 선택} \quad (3)$$

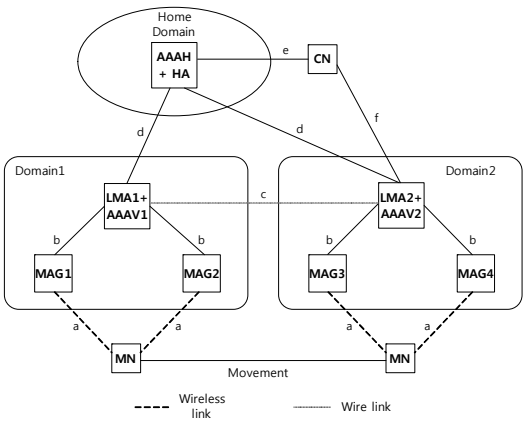
이 $N_{\mathrm{h}}$는 이동 빈도이고 $\frac{\overline{t}_n - \overline{z}_n}{N_{\mathrm{h}}}$는 보다 나은 성능의 프로토콜을 판단하는 지표가 되며 $H_{\mathrm{t}}$는 프로토콜을 결정하기 위한 한계점이다.

## 4. 성능 평가

본 장에서는 성능평가의 모델링과 수학적 접근을 통하여 시스템을 분석하고 결과를 도출한다.

### 4.1 모델링

관리 영역 내에서 방문 도메인의 LMA에 AAA 서버(AAAV)를 배치하고 AAA 서버는 모든 MAG들의 LMA




(그림 5) Proxy-AAA의 비용 분석 모델

영역 내에서의 계정, 인증과 권한을 책임진다. Proxy-AAA 기법에서 전체 시스템의 오버헤드는 두 가지 구성되며 시그널링 제어 오버헤드 $C_{\text{signal}}$과 데이터 전송 오버헤드 $C_{\text{packet}}$이다. 시그널링 제어 오버헤드는 인증 시그널링 제어 오버헤드 $C_{\text{auth}}$와 등록 시그널링 제어 오버헤드 $C_{\text{reg}}$가 포함된다. $C_{\text{packet}}$은 CN에서 MN($C_{\text{CN-MN}}$)으로의 데이터 전송 오버헤드로 구성된다. Proxy-AAA 네트워크 토폴로지의 시스템 오버헤드 분석은 (그림 5)와 같다.

$$C_{\text{total}} = C_{\text{signal}} + C_{\text{packet}} = \beta(C_{\text{reg}} + C_{\text{auth}}) + \alpha C_{\text{CN-MN}} \quad (1)$$

이$\alpha$는 CN에서 MN으로 패킷 데이터를 전송하는 평균 속도(패킷 데이터의 평균 도착율)이고 $\beta$는 MN이 한 서브넷에서 다른 쪽으로 이동할 때 평균 변환 시간을 나타낸다[11]. 이 시간 동안 CN에서 MN으로 전송되는 평균 패킷 수는 같다고 가정하고 MN이 받은 이동성을 위한 패킷 비율(PMR)은 $p = \alpha/\beta$로 표현된다. 이는 MN이 이동 때마다 CN으로부터 받은 평균 패킷 수이다.

PMR은 패킷 도착율과 이동성 비율의 비율을 나타내며 이 논문의 중요한 지표다. PMR 값이 크면 패킷 도착율이 이동성 비율보다 큰 것이고 데이터 전송 비용 역시 크다는 의미다. PMR 값이 작으면 패킷 도착율이 이동성 비율보다 작은 것이고 바인딩 업데이트의 시간 비용이 크다는 의미다. 추가로 데이터 패킷의 평균 길이와 시그널링 패킷은 $l_{\text{d}}$와 $l_{\text{s}}$로 표현된다. 비율은 $l$=$l_{\text{d}}$/$l_{\text{s}}$로 가정한다. Proxy-AAA의 비용 계산이 가능하기 위해 [12]에서 제공된 $l_{\text{d}}$=1024B, $l_{\text{s}}$=100B값을 사용한다. 전송 시그널링 패킷의 오버헤드는 독립체 간의 거리와 관련되고 하나의 데이터 패킷 전송의 오버헤드는 하나의 시그널링 패킷을 위한 $l$시간이다.

$$C_{\text{total}} = \beta(C_{\text{reg}} + C_{\text{auth}}) + \alpha l_{\text{d}} L_{\text{CN-MN}} = \beta l_{\text{s}}(L_{\text{reg}} + L_{\text{auth}}) + \alpha l_{\text{d}} L_{\text{CN-MN}} \quad (2)$$

본 논문은 유무선 네트워크 기반의 시뮬레이션 환경을 구축하여 수행하였다. 유선 네트워크의 경우, 10 Mbit/s의 이더넷 LAN 환경으로, 무선 네트워크 경우, 2 Mbit/s 단일 홉의 WLAN 환경으로 구성한다. 본 논문에서는 실증적인 공식을 바탕으로 계산한 유선과 무선 링크들의 지연시간을 $T_{\text{rt}}(h,k)$와 $W_{\text{rt}}(k)$로 표현한다.

$$T_{\pi}(h,k) = 3.63k + 3.21(h-1)$$
$$W_{\pi}(k) = 17.1k \quad (3)$$

이$k$는 패킷의 길이이고 KB(kilobytes) 단위이며 $h$는 라우팅 홉 수이다. 여기서 몇 가지를 가정하여 사용한다. $\eta$은 유선 전송에서 거리단위 당 시그널링 패킷 비용을 나타낸다. 무선 전송에서의 비용은 10$\eta$이다. 추가적으로 $\sigma$은 유선 전송에서 거리단위 당 데이터 패킷 비용을 나타낸다. 무선 전송에서의 비용은 5$\sigma$이다.

$$C_{\text{packet}} = \alpha C_{\text{CN-MN}} = \alpha l_{\text{d}} \left[\sigma(l_{\text{CN-HA}} + l_{\text{HA-LMA}} + l_{\text{LMA-MAG}}) + 5\sigma l_{\text{MAG-MN}})\right] \quad (4)$$

MN의 이동성은 fluid 모델에 의해 설명된다. LMA의 영역은 사각형 150m X 150m로 가정한다. 만약 보행자의 속도가 3mph(miles / hour)이면 $\beta$=0.01이고 차량의 속도가 60mph이면 $\beta$=0.2이다.

$$C_{\text{packet}} = \beta p l_{\text{d}} \left[\sigma(l_{\text{CN-HA}} + l_{\text{HA-LMA}} + l_{\text{LMA-MAG}}) + 5\sigma l_{\text{MAG-MN}})\right] \quad (5)$$

Proxy-AAA 제안기법의 목적은 인증과 등록으로 인한 시그널링 오버헤드를 줄이는 것이다. 그래서 Proxy-AAA 기법과 기존 AAA 기법을 비교할 것이다. 기존 AAA는 AAA와 HMIPv6의 간단한 조합이다. 적절한 성능평가 매개변수 값과 정의는 (표 1)과 같다 [1-4].

(표 1) 성능평가 매개변수

| 매개변수 | 설 명 |
|---|---|
| $C_{\text{MN-MAG}}$ | MN과 MAG사이의 시그널 전송 비용 |
| $C_{\text{MAG-LMA}}$ | MN과 MAG사이의 시그널 전송 비용 |
| $C_{\text{HA-LMA}}$ | MN과 MAG사이의 시그널 전송 비용 |
| $C_{\text{LMA-LMA}}$ | MN과 MAG사이의 시그널 전송 비용 |
| $C_{\text{AAAV-AAAH}}$ | MN과 MAG사이의 시그널 전송 비용 |
| $P_{\text{MAG}}$ | MAG의 시그널 처리 비용 |
| $P_{\text{HA}}$ | MAG의 시그널 처리 비용 |
| $P_{\text{LMA}}$ | MAG의 시그널 처리 비용 |
| $P_{\text{AAA}}$ | MAG의 시그널 처리 비용 |

특정 시간 동안 MN이 LMA영역을 $m$횟수만큼 벗어나면 인증은 $m$횟수만큼 수행될 것이다. $m$-1이전까지는 도메인 내 인증이고 마지막은 도메인 간 인증이다. MN의 이동 결과에 따른 인증 프로세스는 매개변수 값 $\lambda$와 함께 포아송 분포와 연관지을 수 있다.

$$p(n)=\int_{t=0}^{\infty}p(n,t)f(t)\mathrm{d}t=\int_{t=0}^{\infty}\frac{(\lambda t)^n}{n!}\mathrm{e}^{-\lambda t}f(t)\mathrm{d}t$$
$$=(-1)^n\frac{\lambda^n}{n!}\frac{\mathrm{d}^nF(s)}{\mathrm{d}s^n}\bigg|_{s=\lambda} \quad (6)$$

LMA 영역 내에서의 MN 시간은 감마분포와 함께 추정해볼 수 있고 예상과 변화량의 밀도 함수 $f(t)$는 $1/\mu$와 $\nu$로 표현된다. 그리고 Laplace 변환하면 다음과 같이 표현된다.

$$F(s)=(1+\mu\nu s)^{-1/\mu^2\nu} \quad (7)$$

$$\frac{\mathrm{d}^nF(s)}{\mathrm{d}s^n}=(-\mu\nu)^n\left[\prod_{j=0}^{n-1}\left(\frac{1}{\mu^2\nu}+\mathrm{j}\right)\right](1+\mu\nu s)^{-\left(\frac{1}{\mu^2\nu}+n\right)} \quad (8)$$

그러나, $\mu 2\nu$=1일 때 $f(t)$는 지수분포가 될 수 있다. 이 경우 인증 시간의 예상 $E(m)$은 다음과 같이 표현된다.

$$E(m)=\sum_{n=1}^{\infty}nP(n)=\sum_{n=1}^{\infty}n\frac{\mu\lambda^n}{(\lambda+\mu)^{n+1}}=\frac{\lambda}{\mu} \quad (9)$$

HMIPv6의 비용 모델에 의해 분석하면 PMIPv6에서 도메인 내와 도메인 간의 바인딩 업데이트에 대한 시그널링 오버헤드를 다음과 같이 표현할 수 있다.

$$\mathrm{BU}_{\text{intra}}^{\text{PMIPv6}}=2C_{\text{MN-MAG}}+2C_{\text{MAG-LMA}}+2P_{\text{MAG}}+P_{\text{LMA}} \quad (10)$$

$$\mathrm{BU}_{\text{inter}}^{\text{PMIPv6}}=2C_{\text{MN-MAG}}+2C_{\text{MAG-LMA}}+$$
$$2C_{\text{LMA-HA}}+2P_{\text{MAG}}+2P_{\text{LMA}}+P_{\text{HA}} \quad (11)$$

추가적으로 기존 AAA 기법을 사용할 때의 인증 지연은 다음과 같이 표현된다.

$$A^{\text{traditional}}=2C_{\text{MN-MAG}}+2C_{\text{MAG-LMA}}+$$
$$2C_{\text{LMA-AAA}}+2C_{\text{AAAV-AAAH}}+2C_{\text{LMA-HA}}+$$
$$P_{\text{AAA}}+2P_{\text{MAG}}+4P_{\text{LMA}}+P_{\text{HA}} \quad (12)$$

기존 AAA 기법을 사용한 LMA영역에서의 전체 시그널링 오버헤드는 다음과 같이 표현된다.

$$C_{\text{signal-traditional}}=\mathrm{BU}_{\text{total}}+A^{\text{traditional}}E(m)$$
$$=\mathrm{BU}_{\text{intra}}^{\text{PMIPv6}}(E(m)-1)+\mathrm{BU}_{\text{inter}}^{\text{PMIPv6}}+$$
$$A^{\text{traditional}}E(m) \quad (13)$$

제안한 Proxy-AAA 기법을 사용한 LMA 영역에서의 전체 시그널링 오버헤드는 다음과 같이 표현된다.

$$C_{\text{signal-proposed}}=\mathrm{BU}_{\text{LMA}}+A_{\text{intra}}^{\text{Proxy-AAA}}(E(m)-1)+A_{\text{inter}}^{\text{Proxy-AAA}}$$
$$=\mathrm{BU}_{\text{intra}}^{\text{PMIPv6}}(E(m)-1)+\mathrm{BU}^{\text{Proxy-AAA}}+$$
$$A_{\text{intra}}^{\text{Proxy-AAA}}(E(m)-1)+A_{\text{inter}}^{\text{Proxy-AAA}} \quad (14)$$

제안한 Proxy-AAA 기법에서는 MN의 다른 LMA 도메인 사이의 이동을 위한 바인딩 업데이트 비용을 다음과 같이 표현한다.

$$\mathrm{BU}^{\text{Proxy-AAA}}=2C_{\text{MN-MAG}}+2C_{\text{MAG-LMA}}+2C_{\text{LMA-LMA}}+2P_{\text{MAG}}+3P_{\text{LMA}} \quad (15)$$

Proxy-AAA 기법을 사용할 때 LMA과 AAAV를 함께 배치하고 $l_{\text{LMA-AAA}}$=0으로 가정하면 도메인 내와 도메인 간에서의 인증 시그널링 오버헤드는 다음과 같이 표현된다.

$$A_{\text{intra}}^{\text{Proxy-AAA}} = 2C_{\text{MN-MAG}} + 2C_{\text{MAG-MAG}} + 2C_{\text{MAG-LMA}} + 4P_{\text{MAG}} + P_{\text{LMA}}$$
$$A_{\text{inter}}^{\text{Proxy-AAA}} = 2C_{\text{MN-MAG}} + 2C_{\text{MAG-MAG}} + 2C_{\text{MAG-LMA}} + C_{\text{LMA-LMA}}$$
$$+2C_{\text{AAAV-AAAH}} + 4P_{\text{MAG}} + 2P_{\text{LMA}} + P_{\text{AAA}} \quad (16)$$

$$C_{\text{MN-MAG}} = 10\eta l_{\text{MN-MAG}} l_s$$
$$C_{\text{MAG-MAG}} = \eta l_{\text{MAG-MAG}} l_s$$
$$C_{\text{MAG-LMA}} = \eta l_{\text{MAG-LMA}} l_s$$
$$C_{\text{LMA-HA}} = \eta l_{\text{LMA-HA}} l_s$$
$$C_{\text{LMA-LMA}} = \eta l_{\text{LMA-LMA}} l_s$$
$$C_{\text{LMA-AAA}} = \eta l_{\text{LMA-AAA}} l_s$$
$$C_{\text{AAAV-AAAH}} = \eta l_{\text{AAAV-AAAH}} l_s \quad (17)$$

$$A_{\text{intra}}^{\text{Proxy-AAA}} = (20\eta l_{\text{MN-MAG}} + 2\eta l_{\text{MAG-MAG}} + 2\eta l_{\text{MAG-LMA}}) l_s + 4P_{\text{MAG}} + P_{\text{LMA}}$$
$$A_{\text{inter}}^{\text{Proxy-AAA}} = (20\eta l_{\text{MN-MAG}} + 2\eta l_{\text{MAG-MAG}} + 2\eta l_{\text{MAG-LMA}} +$$
$$\eta l_{\text{LMA-LMA}} + 2\eta l_{\text{AAAV-AAAH}}) l_s + 4P_{\text{MAG}} + 2P_{\text{LMA}} + P_{\text{AAA}} \quad (18)$$

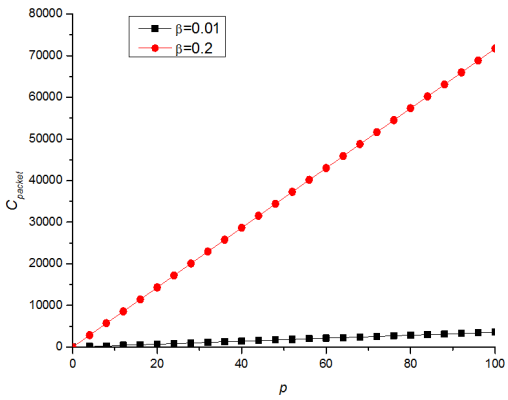
이 $R$ 은 Proxy-AAA와 기존 AAA 기법의 시그널링 오버헤드 비율이라고 가정하면 $R = C_{\text{signal-proposed}} / C_{\text{signal-traditional}}$으로 표현된다. LMA 영역에서의 시그널링 오버헤드 계산 공식으로 분석하면 시그널링에 대한 평균 오버헤드는 $C_{\text{signal-a}} = T_a / C_{\text{signal-proposed}}$로 표현되고 $T_a$는 해당 LMA 영역 내에서의 평균 상주 시간을 나타낸다. 실제 네트워크 환경에서 이 값은 반드시 0.3보다 작다.

## 4.2 성능 분석

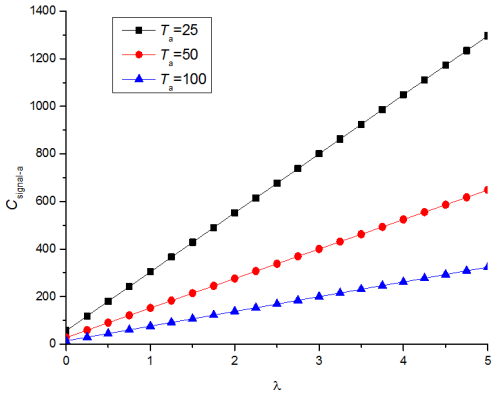
이 절에서는 기존 인증 기법과 Proxy-AAA 인증 기법의 시스템 오버헤드를 비교하여 설명한다. 매개변수 값들은 (표 2)에서 볼 수 있다 [1-4].

(표 2) 매개변수 값

| 매개변수 | 값 | 매개변수 | 값 |
|---|---|---|---|
| $l_{\text{MAG-LMA}}$ | 5 | $l_{\text{MN-MAG}}$ | 1 |
| $P_{\text{MAG}}$ | 4 | $l_{\text{HA-LMA}}$ | 10 |
| $l_{\text{LMA-LMA}}$ | 10 | $l_{\text{LMA-AAA}}$ | 10 |
| $\sigma$ | 0.05 | $\eta$ | 0.1 |
| $P_{\text{LMA}}$ | 3 | $P_{\text{HA}}$ | 4 |
| $P_{\text{AAA}}$ | 3 | $l_{\text{CN-HA}}$ | 50 |
| $l_{\text{MAG-MAG}}$ | 1 | - | - |



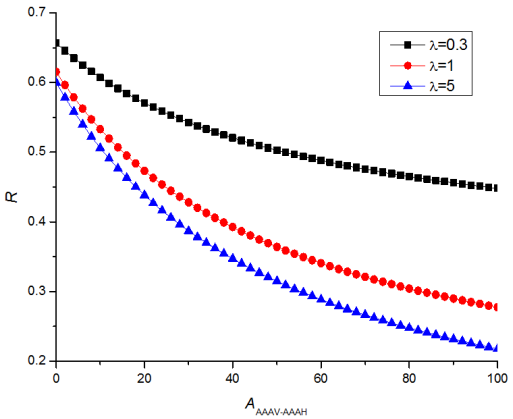

(그림 6) 패킷 데이터 전송 오버헤드($\mu$=0.1)



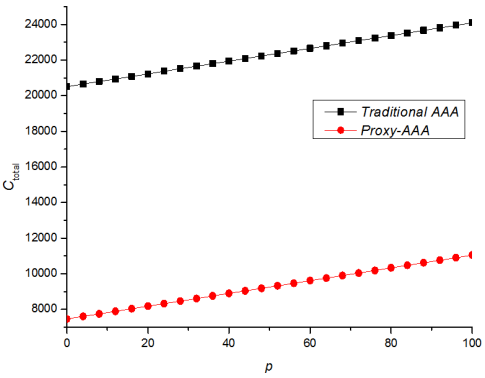

(그림 7) 시그널링 오버헤드($l_{\text{AAAV-AAAH}}$ =50)

우선 MN은 보행자와 차량이 있으며 각각의 다른 데이터 패킷 전송 오버헤드를 분석한다. (그림 6)은 보행자($\beta$=0.01)와 차량($\beta$=0.2)의 데이터 패킷 전송 오버헤드를 보여준다. 분석 결과, PMR $p$증가에 따른 데이터 패킷 전송 오버헤드 $C_{\text{packet}}$ 증가를 볼 수 있다. 추가적으로 $p$값이 고정되면 $\beta$가 클수록 CN에서 MN으로 보내는 데이터 패킷의 평균 도착율 $\alpha$가 커지고 $C_{\text{packet}}$이 커진다. 그리고 $\beta$값이 고정되면 $\alpha$가 커지면 $C_{\text{packet}}$이 커진다.

(그림 7)은 Proxy-AAA의 평균 시그널링 오버헤드의 분석이다. 인증 이벤트 $\lambda$의 도착율이 증가하면 시그널링 오버헤드 $C_{\text{signal}}$이 증가한다. 즉, LMA영역에서 MN의 잦은 도착으로 인한 인증 이벤트들의 도착율 증가를 가져오며 도메인간 인증과 등록의 시그널링 오버헤드는 커질 수 밖에 없다. 그래프에서 특정 포인트를 보면 $\lambda$가



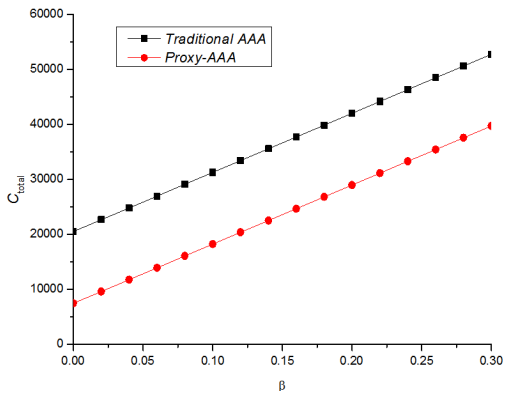

(그림 8) 시그널링 오버헤드 비율(Proxy-AAA/기존 AAA)




(그림 9) 전체 오버헤드($\beta$=0.01, $\lambda$=1)

1.5일때 $T_a$가 100이면 $C_{signal}$은 17이다. $\lambda$가 1.5일때 $T_a$가 50이면 $C_{signal}$은 26이다. $\lambda$가 1.5일때 $T_a$가 25이면 $C_{signal}$은 52 이다. 이는 상주 시간 $T_a$가 증가할수록 시그널링 오버헤드 $C_{signal}$은 작아지는 것을 설명한다. 즉, MN의 동일 LMA 도메인에서 상주시간이 길어지면 도메인간 교환과 인증이 적고 전체 시스템에서의 시그널링 오버헤드도 낮다.

(그림 9)는 기존 AAA 기법과 Proxy-AAA 기법간의 시그널링 오버헤드율 $R$의 분석이다. 여기서 $R$은 항상 1보다 작다. 즉, MN이 LMA영역이나 도메인간 이동에 상관없이 제안하는 Proxy-AAA 기법의 시그널링 오버헤드가 기존 AAA기법보다 항상 작다. 그래프를 보면 $l_{AAAV-AAAH}$가 증가할수록 R은 감소한다. 다시 말해 MN이 홈 도메인으로부터 멀어질 때 Proxy-AAA의 효율성이 나타난다. $l_{AAAV-AAAH}$ 값이 40으로 고정되고 $\lambda$가 0.3이면 $R$은 0.5이다. 그리고 $\lambda$가 1이면 R은 0.39이고 $\lambda$가 5이면 $R$은 0.35이다. 이는 MN의 도착율 $\lambda$가 크면 $R$은 작으며 Proxy-AAA의 시그널링 오버헤드가 뛰어난 효율성을 나타낸다.




(그림 10) 전체 오버헤드($p$=30, $\lambda$=1)

(그림 9)는 PMR $p$증가에 따른 전체 오버헤드에 대한 분석이다. 보행자($\beta$=0.01)이동 시 $p$증가에 따른 전체 오버헤드 $C_{total}$ 증가를 볼 수 있다.

(그림 10)은 이동성 $\beta$증가에 따른 전체 오버헤드에 대한 분석이다. 고정된 PMR에서 $\beta$증가에 따른 전체 오버헤드 $C_{total}$ 증가를 볼 수 있다. 그래프를 통해 기존 AAA 기법에 비해 Proxy-AAA기법이 보다 효율적임을 알 수 있다.

## 5. 결 론

본 논문에서는 AAA와 PMIPv6의 결합을 통하여 기존의 긴 지연시간과 추가적인 오버헤드를 줄이는 방안을 제시하였다. 이로서, 여러 LMA들 간에 빠른 이동 모드와 포워딩 모드가 지원가능함을 확인할 수 있었다. 뿐만 아니라 전체 오버헤드 역시 제안 기법이 기존 AAA기법 보다 항상 적은 수치를 보임으로서. 로컬 이동성을 지원하는 PMIPv6에 포워딩 모드의 AAA인증기법이 보다 효율적으로 도메인간 이동이 가능하다는 것을 보여주었다. 또한, LMA 도메인간 이동이 발생할 때 RAAAS(Root AAA Server)와 홈 도메인 간의 거리가 더 멀어질수록 성능효율이 높아진다는 것은 본 연구에서 추구한 목적과 적합한 방법으로 향후 이동성 프로토콜의 응용 서비스에

서 요구하는 보안성과 QoS(Quality of Service)를 만족시킬 수 있을 것으로 예상할 수 있다. 본 연구에서 제안된 AAA의 기술과 PMIPv6의 결합은 차세대 네트워크 환경에서 적합한 인증 체계로서 보안성 향상에 기여할 것이다.

## 참 고 문 헌


[1] C. de Laat, G. Gross, L. Gommans, L. Gommans, D. Spence, "Generic AAA Architecture," RFC 2903, August 2000.

[2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol," RFC 3588, September 2003.

[3] A. Mankin, B. Patil, D. Harkins, et al, "Threat Model introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6," draft-ietf-mobileip-ipv6-scrty-reqts-02.txt, Internet Draft, May 2001.

[4] Le F, Patil B, Perkins C, et al, "Diameter mobile IPv6 application," Internet Draft, 2004.

[5] Lee S Y, Huh E N, Kim S B, et al, "An efficient performance enhancement scheme for fast mobility service in MIPv6," Proceedings of the International Conference on Computational Science and its Applications(ICCSA'05), pp. 628-637, May 2005

[6] Kim M, Kim M, Mun Y, "A hierarchical authentication scheme for MIPv6 node with local movement property," Proceedings of the International Conference on Computational Science and its Applications(ICCSA'05), pp. 550-558, May 2005.

[7] Song Mei, Wang Li, Song Jun-de, "A secure fast handover scheme based on AAA protocol in mobile IPv6 networks," The Journal of China Universities of Posts and Telecommunications, 15(Sup1), pp. 14-18, 2008.

[8] G. Giaretta, "Interactions between PMIPv6 and MIPv6: scenarios and related issues," draft-ietf-netlmm-mip-interactions-04, June 2009.

[9] J. -F. Guan, et al, "Implementation and analysis of proxy MIPv6," WCM, September 2009.

[10] D. -G. Anderson, "Improving end-to-end availability using overlay networks," Massachusetts Institute of Technology, February 2005.

[11] Jain R, Raleigh T, Graff C, et al, "Mobile Internet access and QoS guarantees using mobile IP and RSVP with location registers," Proceedings of International Conference on Communications(ICC'98), Vol 3, pp. 1690-1695, June 1998.

[12] Lee K, Mun Y, "An efficient macro mobility scheme supporting fast handover in hierarchical mobile IPv6," Proceedings of the International Conference on Computational Science and its Applications (ICCSA'05), pp. 408-417, May 2005.

## ◐ 저 자 소 개 ◑


**이 승 현**

2004년 한신대학교 정보통신학과 졸업(학사)
2006년 성균관대학교 일반대학원 컴퓨터학과 졸업(석사)
2008년 성균관대학교 일반대학원 전기전자컴퓨터공학과 박사수료
관심분야 : 유비쿼터스 컴퓨팅 미들웨어, 통신시스템, 모바일 통신, 차세대이동통신 등
E-mail : lshyun0@ece.skku.ac.kr

**신 동 렬**

1980년 성균관대학교 전기 및 전자공학과 졸업(학사)
1982년 한국과학기술원 전기 및 전자공학과 졸업(석사)
1992년 Georgia Tech. 전기 및 전자공학과 졸업(박사)
1994년~현재 성균관대학교 정보통신공학부 교수
관심분야 : 유비쿼터스 컴퓨팅,통신 시스템, 유무선 네트워크,센서 네트워크, 미들웨어 등
E-mail : drshin@ece.skku.ac.kr

**정 종 필**

1997년 성균관대학교(공학사)
2003년 성균관대학교 정보통신공학부 졸업(석사)
2008년 성균관대학교 정보통신공학부 졸업(공학박사)
관심분야 : 모바일컴퓨팅, 센서 이동성, 차량 모바일 네트워크, 스마트기기 보안, 네트워크 보안 등
E-mail : jpjeong@skku.edu