http://dx.doi.org/10.7236/JIWIT.2012.12.3.99
JIWIT 2012-3-14

프록시 모바일 IPv6 네트워크에서 3S를 고려한 도메인간 이동성관리 기법

3S: Scalable, Secure and Seamless Inter-Domain Mobility Management Scheme in Proxy Mobile IPv6 Networks

강 민*, 정종필**

Min Kang, Jongpil Jeong

요 약 PMIPv6(Proxy Mobile IPv6)는 MN(Mobile Node)의 적극적인 참가를 요구하지 않는 네트워크 기반의 이동성 관리 방법으로 통신 및 인터넷 커뮤니티 사이에서 상당한 주목을 받고 있다. 그것은 낮은 핸드오버 지연을 유지하면서 다수의 MN를 지원할 수 있는 확장성 있는 PMIPv6 도메인의 구축방안은 여전히 연구가 진행 중에 있다. 본 논문에서는 확장성과 안전성 그리고 끊김없는 PMIPv6 도메인을 구축하기 위한 3S 접근 방식을 제안한다. 제안기법에서 모든 MAG(Mobility Access Gateway)는 LMA(Local Mobility Anchor)와 같은 역할을 하고 다른 MAG와 가상 링을 구성한다. 일관된 해싱은 각 MN과 모든 MAG의 MN의 LMA간 효율적인 분산 매핑에 사용된다. MAG와 MN은 대칭키를 이용하여 인증한다. 수학적 분석을 통하여 3S의 안전성, 확장성 그리고 끊김없는 서비스를 검증한다. 또한 3S의 핸드오버 절차를 제안하고 이전의 기법에 비해 낮은 핸드오버 지연이 발생함을 보여 준다.

Abstract Proxy Mobile IPv6 (PMIPv6) has received considerable attention between telecommunications and the Internet communities and does not require active participation of the Mobile Node (MN) by way of network-based mobility management. The PMIPv6 domain is studying establishment in progress to support extensively a number of MN by using a low handover latency. In this research, we are propose a novel 3S scheme for building Scalable and Secure and Seamless PMIPv6 domains. In the proposed scheme, all of Mobility Access Gateway (MAG) are acting as the Local Mobility Anchor (LMA) and composing a virtual ring with another MAG. General hashing is used in the efficient distribution-mapping between each MN and the MN's LMA of all MAGs. And, MAG and MN are authenticated using the symmetric key. Through mathematical analysis, we verifies the safety, scalability, and seamless service for 3S. Also, we're propose a handover procedure of 3S and show better than the existing schemes in terms of handover latency.

Key Words : PMIPv6, Handover, 3S, SARP, Mobility Management, Chord

Ⅰ. 서 론

모바일 무선 네트워크의 급속한 성장은 모바일 가입자와 모바일 기기의 무선 엑세스에 대한 수요증가가 이끌었다. 다양한 무선 접속 네트워크 기술은 매우 낮은 핸드오버 지연시간의 기술을 지원하기 위한 구체적인 방법

*성균관대학교 정보통신대학원 컴퓨터공학과 석사과정
**성균관대학교 정보통신공학부 교수
접수일자 2012.5.22, 수정완료 2012.6.7,
게재확정일자 2012년 6월 8일

Received: 22 May, 2012, Revised: 7 June, 2012, Accepted: 8 June, 2012
*Corresponding Author : kang.min@hanmail.net
Computer Enfineering, Graduate School of Information and Communication, Sungkyunkwan University, Korea

을 사용한다. 이처럼 다양한 무선 엑세스 네트워크가 보편적인 IP(Internet Protocol) 지원 제품군과 그 핵심 인프라 안에서 IP 이용조건을 수렴하므로, 그것은 모든 IP 기반의 서비스를 과도하게 즐기면서 여러 기술에 대한 액세스 기능이 있는 MN(Mobile Node)이 원활하게 이 기종 네트워크를 통해 로밍할 수 있게하는 것이 중요한 일이다[1, 3].

PMIPv6(Proxy Mobile IPv6)[2]는 IETF(Internet Engineering Task Force)의 NETLMM(Network-base Localized Mobility Management) 작업그룹에 표준화된 네트워크 기반 이동성관리 기법이다. PMIPv6를 통해 수정되지 않은 IP노드는 관리상 주어진 IP도메인 내에서 하나의 인터페이스에서 IP주소를 변경하지 않고도 AR(Access Router)를 변경할 수 있다. 그리고 IP기반의 도메인은 회사 / 캠퍼스 네트워크처럼 다양한 크기로 사용자를 커버할 수 있다. 따라서 작은 핸드오버 지연시간을 유지하면서, 넓은 지역에 걸쳐 다수의 MN에 서비스를 제공할 수 있는 확장성 있는 PMIPv6 도메인 구축 문제를 해결하기 위해 매우 중요하다. PMIPV6 연구에서 최근 몇 년 동안 많은 연구가 있었고, 위의 문제는 여전히 진행 중에 있다[4].

본 논문에서는 이 문제를 해결할 새로운 기법을 제시한다. 첫째, 확장성과 안정성 그리고 끊김없는 PMIPv6 도메인을 구축하기 위한 3S(Scalable, Secure and Seamless) 접근방법을 제안한다. 3S는 네 가지 주요 장점이 있다. 1) 확장성 이다. 모든 MAG(Mobile Access Gateway)가 MAG / LMA 처럼 되는 것을 제안 한다. 2) PMIPv6도메인의 보안 강화를 위한 메커니즘을 제공한다. 3) 빠른 핸드오버 절차를 사용하여, 매우 낮은 핸드오버 지연을 유지한다. 4) 보다 쉽게 로드 균형 조정을 실현한다. 둘째, 3S의 깊은 성능을 분석하고 단일 PMIPv6 도메인이 대부분의 큰 도시의 인구보다 훨씬 많은 10^8개 이상의 MN을 지원할 수 있다는 것을 보여준다.

논문의 구성은 다음과 같다. 2장에서 PMIPv6, Chord 및 SARP의 기본 개념에 대하여 설명하고, 3장에서 3S 기법을 제안하고 4장에서 그 평가 결과를 설명한다. 5장에서 본 논문의 결론을 언급한다.

II. 관련 연구

1. Proxy Mobile IPv6의 개요

PMIPv6[2]는 이동성 관련 시그널링의 참여를 요구하지 않고 MN의 IP이동성을 가능하게 한다. 대신, 두 개의 네트워크 엔티티 즉 MAG와 LMA는 PMIPv6 도메인에 MN을 대신하여 IP 이동성을 관리하기 위해 사용된다. 각 MN은 도메인 내의 미리 구성된 LMA에 의해 제공된다. MAG는 MN의 움직임을 감지하고 MN의 HoA (Home of Address)로 경로를 업데이트할 MN의 LMA와 시그널링을 시작한다, 액세스 링크에서 MN의 홈 링크를 변경하지 않고, MN의 LMA와의 사이에 터널을 설정하여 서로 통신할 수 있다. [3]에 정의된 HA(Home Agent)처럼 LMA는 PBU(Proxy Binding Update)와 PBA (Proxy-Binding Acknowledgement)메시지를 처리한다. LMA도 MN이 처리하고 제공하는 도중에 패킷을 가로채고 적절한 MAG의 터널에서 패킷을 가로챈다. 그리고 PMIPv6에서 요구하는 추가 기능을 제공한다.

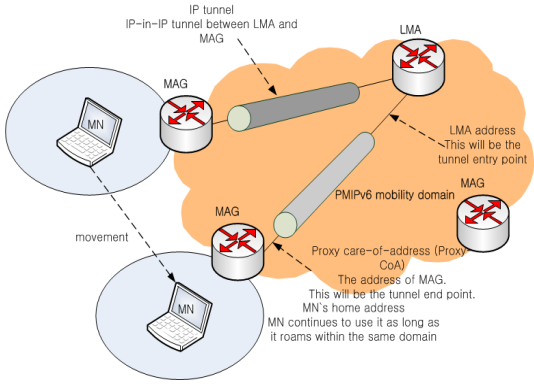

그림 1. PMIPv6의 개요
Fig. 1. Overview of PMIPv6

그림 1은 PMIPv6 도메인 내의 이동성 지원을 보여준다. 특히, PMIPv6 도메인은 MN의 HoA와 MN이 PMIPv6 도메인 내의 어디를 이동하든 개념적으로 따라오는 홈 네트워크에 해당하는 구역을 할당하는 것을 학습한다. MAG는 MN의 접속을 감지할 때마다, 액세스 링크 앞에서 MN의 홈 네트워크를 제공한다. 따라서 MN의 관점에서, 전체 PMIPv6 도메인은 홈 네트워크로 나타나고 MN은 PMIPv6 도메인 내에서 이동할 때 COA(Care-of-Address)를 구성할 필요가 없다. MN이 PMIPv6 도메인의 이전 MAG(pMAG)에서 새 MAG (nMAG)로 이동할 때, 그림 2에 설명된 절차로 핸드오버가 실행된다.

1 단계) MN이 nMAG에 연결될 때 접속 인증 절차는 MN의 ID (예: MN-identifier)를 사용하여 수행된다. 성공적인 접속 인증 시, nMAG은 MN의 ID를 알 수 있다.

2 단계) nMAG은 MN의 구성 프로파일을 얻을 수 있는 정책 저장소 (예 : 인증, 권한 부여 및 계정(AAA) 서버)에 쿼리 메시지를 보낸다.

3 단계) 정책 저장소는 MN의 MN-ID, LMA 주소 및 nMAG에 지원되는 주소를 구성 모드에 포함하여 MN의 프로필을 보낸다.

4 단계) nMAG은 MN대신 MN의 LMA에 MN-ID를 포함하여 PBU 메시지를 보낸다.

5 단계) LMA가 PBU 메시지를 받으면 보낸 사람이 PBU 메시지를 보낼 수 있는 권한이 있는지 확인하기 위해 정책 저장소를 확인한다.

6 단계) 정책 저장소는 보낸 사람이 권한이 있는지 여부를 확인하기 위해 LMA에 회신을 보낸다.

7 단계) 보낸 사람이 권한이 있는 경우, LMA는 MN의 HNP(Home Network Prefix) 옵션을 포함하여 PBA 메시지를 전송하고, nMAG에 터널을 통해 MN의 HNP에 대한 경로를 설정한다. 두 터널의 끝단은 그림 1에 설명된 LMA 주소와 nMAG의 주소를 포함한다. 또한 LMA는 바인딩 캐시를 업데이트해야 한다.

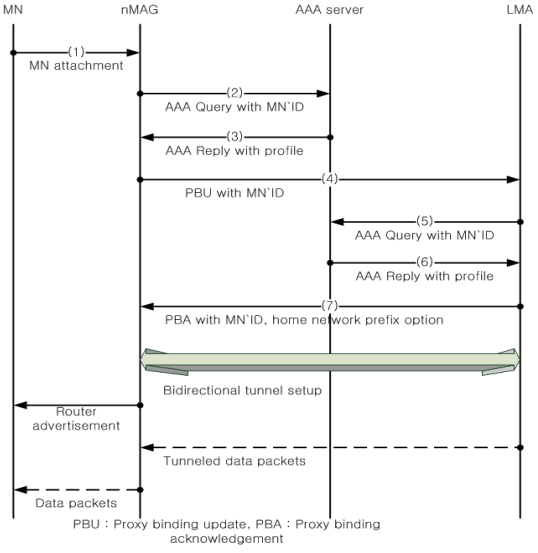

그림 2. PMIPv6의 핸드오버 절차
Fig. 2. Handover procedures of PMIPv6

nMAG이 PBA 메시지를 받게 되면, 그것은 접속 네트워크에서 MN의 홈 네트워크를 변경하지 않고 모든 필요한 정보를 획득한다. 그런 다음 MN은 MN의 HNP를 포함하는 RA(Router Advertisement) 메시지를 보내고 LMA에 터널을 설정한다. LMA에 터널을 설정한 이후 패킷은 nMAG의 모든 해당 노드에서 MN에게 전달받는다.

본 논문에서 3S도메인을 구축하기 위한 접근 방법을 제안한다. 우리의 접근법은 IETF NETLMM 작업 그룹에서 개발된 제안과 충돌하지 않는 것을 확인할 수 있다. 반면에, 그것은 자연스럽게 그 제안을 보완한다.

2. Chord 시스템

Chord[5]는 키를 기반으로 노드를 찾기 위해 사용되는 확장 가능한 분산 프로토콜 방식이다. N-노드 Chord 시스템에서, 각 노드는 다른 노드에 대한 정보를 유지하기 위해 O(logN)이 필요하고, 다른 노드에 O(logN) 메시지를 통해 모든 조회를 해결한다. 또한, N-노드 Chord 시스템의 평균 조회 시간은 (1/2) logN이다. 이 목적을 위해 Chord는 SHA-1[6]을 사용하여 모든 노드와 키에 m-비트의 식별자를 할당하고 일관성 있는 해싱으로 노드에 키를 할당한다[7]. 특히, 노드의 식별자는 노드의 IP 주소와 노드의 키를 해싱하여 얻을 수 있다. 개연성 있는 두 개의 노드 또는 비슷한 ID의 해싱 키를 만들기 위하여, 식별자 길이 m은 충분히 커야 한다.

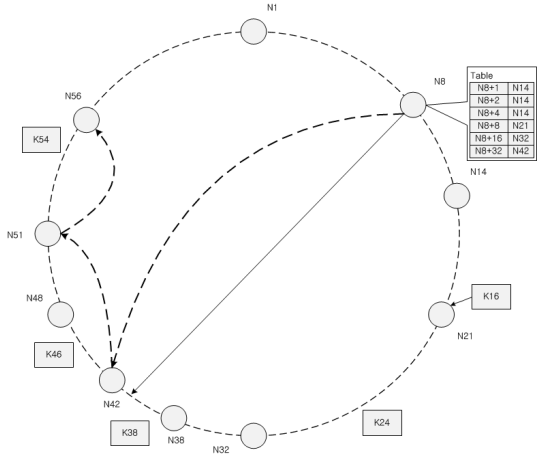

그림 3. Chord 시스템
Fig. 3. Illustration for Chord System

그림 3에서 식별자는 Chord 서클 모듈로 2^m에 정렬된다. 계승자(K)는 키 K의 계승자를 나타낸다. 따라서 계승

자(K)는 식별자를 0에서 2^m-1의 숫자 서클로 표현하는 경우 K부터 시계방향으로 첫 번째 노드이다. 키 K로 주어질 때, 그것은 계승자(K)에 할당된다.

Chord에서, 노드는 최소한의 간섭으로 네트워크를 들어가고 떠날 수 있다. 특히, 노드 n은 네트워크를 결합했을 때, 이전 n의 계승자에 할당된 일부 키는 N에 할당된다. 한편, 노드 n은 네트워크를 빠져나오면, 그 할당된 키는 모두 n의 계승자로 할당될 수 있다. 또한, 다른 노드에 키의 할당을 변경할 필요는 없다.

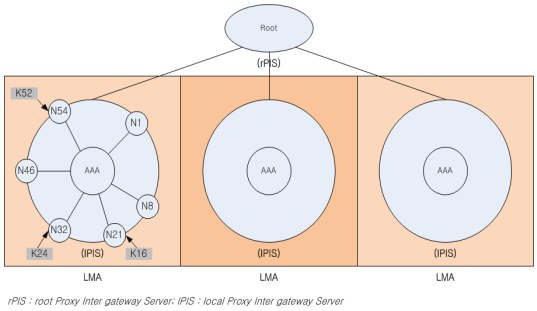

그림 4. rPIS – IPIS
Fig. 4. Root Proxy Inter-Gateway Server (rPIS) – local PIS (IPIS)

Ⅲ. 3S 이동성관리 기법

1. 시스템 아키텍처

3S의 목표는 확장성과 안전성 그리고 끊김없는 강력한 PMIPv6를 제공하는 것이다. 이런 목적을 위해, PMIPv6 도메인의 모든 MAG가 [8]에서 지정한 MN-ID와 유사한 MAG 식별자가 많은 MAG에 있다는 것을 가정한다. 게다가, PMIPv6 도메인의 모든 MAG는 MAG 식별자를 통해 일관성 있는 해싱을 사용하여 Chord 서클에 구성된다. 가장 중요한 것은, 모두 같은 LMA에서 3S 기능의 모든 MAG의 MN과, 일부 액세스 링크를 통해 MAG에 연결된 MN에 미리 구성되어 제공된다. MN에 주어진, 도메인의 네트워크 관리자 또는 알고리즘에 의해 구성된 PMIPv6 도메인의 LMA는 MN이 PMIPv6 도메인 내에 이동하는 동안 변경되지 않는다. 실제로, 대부분은 하루 동안 사무실에서 약 8 시간 매일 일하고 저녁에 집에 돌아갈 때까지 종종 MN은 특정 지역에 위치해 있다. 즉, MN은 자신의 집 또는 직장의 MAG 커버링 지역에 소속되어 있다. 우리가 높은 확률로 MN를 위한 LMA와 같은 MAG를 선택하면 LMA / MAG 직접 다른 MAG로 터널링 없이 MN에게 패킷을 보낼 수 있다. 즉, MN의 LMA는 MN의 LMA에 첨부되지 않은 경우에만 다른 MAG에 터널 패킷에 필요하다. 반대로 MN으로의 패킷전송은 전형적인 PMIPv6 도메인에서 MN이 거의 MAG에서 멀리 이동하지 않더라도 어느 방향의 터널에서 MN에 첨부되는 MAG의 패킷은 MN에 제공하는 LMA에 의해 항상 가로챈다. 그 결과, 우리의 접근 방식은 가장 많이 MN을 다루는 MAG로 LMA를 배치하여 터널링 간접비가 감소한 후 자원의 효율성을 크게 향상시킨다.

위에서 명시된 바와 같이 MN의 LMA는 잘 알려지지 않은 네트워크 관리자로부터 구성되어져 있다. 그 결과, MAG는 MN의 접속을 감지했을 때, 어떤 MAG가 MN의 LMA인지 알 수 없다. 이 문제를 해결하기 위해서는 간단한 해시 메커니즘을 통해 MAG의 (key, value)조합을 저장한다. 여기서 key는 MN-ID의 해시 값이며 value는 해당 MN를 제공하는 LMA의 IPv6 주소이다. 주어진 MN-ID는 LMA의 IPv6 주소로 MN의 경우 MN-ID의 후속 MAG에 저장해야 한다. 그림 4에서, key 24와 MN-ID가 일치하는 MN의 경우 MN의(key, value)조합은 노드 N32에 해당하는 MAG에 저장된 것이다. 다른 MAG에서 MN의 접속을 감지한 LMA의 MN을 찾기 위한 쿼리 메시지를 보내서 QServer에 저장된 MAG의 MN에 대한 (key, value)조합을 보여준다. 이 방식으로 그림 4에서 QServer의 key 24의 노드는 N32이다. 즉, QServer(24) = 32 이다.

새로운 MAG가 MN의 접속을 감지할 때마다, 그것을 MN의 LMA가 알지 못할 수도 있다. 이 경우, MN의 LMA를 찾을 수 있도록 Chord 시스템에 쿼리 메시지를 보낸다. 쿼리 메시지는 MN-ID, 새로운 MAG의 식별자와 IPv6 주소를 포함해야 한다. Chord 노드 앞에서 쿼리 메시지로 QServer(MN)에서 뽑아낸다. 효율적인 전달을 위해 위에서 명시된 바와 같이 모든 MAG는 MN-ID의 IPv6주소로 (key, value)조합의 해시값을 갖는 테이블을 유지한다. MN의 QServer 역할의 MAG는 쿼리 메시지를 받으면 LMA는 새 MAG의 MN에게 IPv6 주소를 보낸다. 새로운 MAG는 MN이 속한 LMA의 IPv6 주소를 받으면, 그것을 로컬 LMA에 IPv6 주소를 저장한다. 이러한 목적으로, 새로운 MAG는 각 접속된 MN을 제공하

는 LMA의 IPv6 주소를 테이블에 기록하여 유지하는 것이 필요하다.

쿼리 메시지가 오랜 조회 지연으로 앞의 Chord 링에 다중 홉을 통해 전달 될 수 있다. 이러한 관점에서, 그것은 한 홉 D1HT(Distributed One Hop Hash Table)[9]에 MAG를 구성하는 것이 좋다. 그러나 목표는 확장 가능한 대형 PMIPv6 도메인에 구축되어 있기 때문에, 대형 PMIPv6 도메인 네트워크 관리 및 문제 해결을 단순화하기 위해 여러 라우팅 도메인으로 분할할 수 있다. 그 경우, PMIPv6 도메인에 MAG는 PMIPv6 도메인 및 DHT이 적용되지 않을 수 있고, 한 홉의 다른 MAG의 경로를 알 수 없다.

2. 3S 기법의 보안성

같은 Chord가 D1HT 기반 프로토콜을 사용하는 중요한 이슈는 한 노드가 다른 노드를 신뢰하지 않을 수 있다는 것이다. 다행스럽게도, 위에 설명된 Chord 시스템에서 MAG는 보통 하나의 네트워크 제공자가 관리하는 공통 PMIPv6 도메인에 위치하고 있다. 따라서 다른 MAG의 공격으로부터 MAG를 보호할 필요가 없다. 그러나 그것은 모바일 호스트에 의해 속지 않도록(spoof) MAG을 보호하기 위해 필요하다.

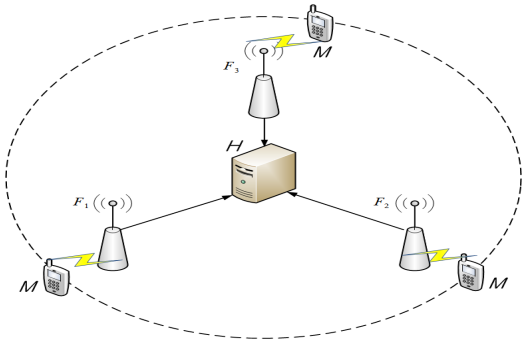

그림 5. 익명의 로밍 서비스를 위한 로밍 경로
Fig. 5. Roaming path with anonymity for roaming service

이런 목적을 위해, 로밍 서비스를 위해 PKI서버를 사용한 공개키 기반의 인증방식을 사용하지 않고 [10]에서 제안한 대칭키를 사용하여 사용자 익명성을 위한 로밍서비스의 효율적인 무선인증 프로토콜을 사용하여 인증을 수행한다.

대칭키를 시용한 Chang[11]의 프로토콜 약점을 보완한 [10]의 프로토콜을 사용하여 인증을 수행한다. Chang[11]의 프로토콜 약점은 사용자 식별 ID_M과 SID사이에 구속력이 있었다는 사실에 기초를 둔다. 이 결함은 내부의 상대자가 동일한 HA에 등록된 다른 사용자의 신원을 밝힐 수 있다. 이러한 문제를 해결하기 위해, 무선 환경에서 로밍 서비스에 대한 익명성을 가진 새로운 상호 인증 프로토콜을 사용한 [10]의 프로토콜을 소개 하였다. 이 프로토콜은 사용자 비밀 번호 및 스마트카드를 사용하지만, 신원의 익명성을 보존하고 세션 키 기밀성을 제공할 수 있다. 이 프로토콜은 그림 6에 설명된 두 단계로 동작한다.

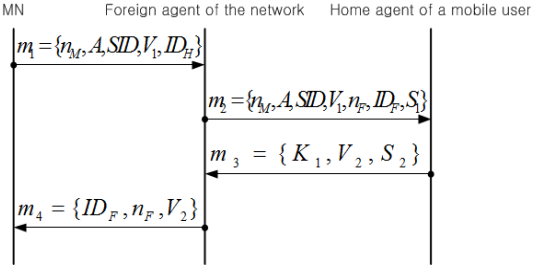

그림 6. 인증 메커니즘의 작동절차
Fig. 6. Operation Process of Authentication Mechanism

(가) 1 단계 : 등록

초기화하기 위해, H 는 큰 소수 p, q와 q순서의 배수 그룹에서 생성한 q를 선택한다. H는 또한 비밀 키 $b \in Z_q^*$와 적절한 단방향 해시 함수 $h(0)=\{0,1\}^* \rightarrow Z_q^*$를 선택한다. 이 방식은 다음 단계로 진행된다.

(1) M은 식별자 ID_M과 선택된 패스워드 PW_M을 H에 등록하기 위해 제출한다.

(2) H는 $B=g^b \bmod p$ 와 $u=h(ID_M \| b) \oplus pw_M$ 을 계산한다. H의 쟁점은 스마트카드에 들어갈 $\{p,q,B,h(\sigma),u\}$를 보안 채널을 통해 M에게 제공하는 것이다.

(나) 2 단계 : M(Mobile Node)과 F(Foreign Network) 사이의 상호 인증

그림 6에 명시된 바와 같이 이 단계에서 사용자 M 및 F는 상호 인증을 수행하고 세션 키에 동의한다.

(1) M이 F가 관리하는 외부 네트워크에 들어갔을 때, 스마트카드의 식별자 ID_M 과 패스워드 PW_M을

입력하면 된다. 그러면 적당한 방법으로 임의의 두 개의 숫자 a와 n_M을 선택한다. $A = g^a \bmod p$, $D = B^a \bmod p$, $C = u \oplus PW_M^*$, $SID = ID_M \oplus h(d \| n_M)$, $V_1 = h(C \| D)$을 계산한다. 이 방법은 M을 대신하여 $m_1 = \{n_M, A, SID, V_1, ID_H\}$ 메시지를 F에게 보낼 수 있다. 실제로 A와 D는 오프라인에서 미리 계산될 수 있다.

(2) m_1을 접수하는 즉시 F는 무작위로 n_F를 선택한다. $S_1 = h(K_{FH} \| n_M \| A \| SID \| V_1 \| n_F \| ID_F)$을 계산하고, $m_1 = \{n_M, A, SID, V_1, n_F, ID_F, S_1\}$ 메시지를 H에게 보낸다, K_{FH}는 F와 H사이에 미리 공유된 대칭키이다.

(3) m_2을 접수하는 즉시 H 는
$S_1^* = h(K_{FH} \| n_M \| A \| SID \| V_1 \| n_F \| ID_F)$
를 계산하고 $S_1^* = S_1$인지 체크한다. 그 다음에 H는 ID_M^*가 합법적인 식별자인지, $V_1^* = V_1$공식이 성립하는지 체크 한다. 두 조건이 충족되는 경우 H는 계속해서
$SK = h(D^* \| ID_M^* \| n_M \| ID_F \| n_F)$,
$K_1 = SK \oplus h(K_{FH} \| n_F)$,
$V_2 = h(D^* \| n_M \| ID_F)$,
$S_2 = h(K_{FH} \| n_F \| K_1 \| V_2)$를 계산하고, 메시지 $m_3 = \{K_1, V_2, S_2\}$를 F에게 보낸다.

(4) m_3을 접수하는 즉시 F는 $S_2^* = h(K_{FH} \| n_F \| K_1 \| V_1)$, $SK = K_1 \oplus h(K_{FH} \| n_F)$를 계산하고 $S_2^* = S_2$가 동일시하고 있는지 체크한다. 만일 그렇다면, 그것은 M은 인증된 사용자 이고 M에게 $m_4 = \{ID_F, n_F, V_2\}$ 메시지를 전달해 준다고 생각한다.

(5) m_4을 접수하는 즉시 M은 $V_2^* = h(D \| n_M \| ID_F)$를 계산하고 $V_2^* = V_2$가 동일시하고 있는지 체크한다. 만일 그렇다면, M은 F가 인증되었고 동의 세션 키 $SK = h(D \| ID_M \| n_M \| ID_F \| n_F)$가 계산된다.

제안 기법은 상호 인증을 구현한다. 합법적인 사용자 M으로 가장하여 상대자 A가 되는 것은 불가능하다. H부터 M이 V_1을 따라서 $V_1 = h(C \| D)$, $C = u \oplus PW_M$, $D = B^a \bmod p$에서 문제가 없음을 증명한다. 그러나 이 공격 모델은 M의 스마트카드 또는 그의 비밀번호 둘 중에 하나를 취득한 A를 허락한다. 따라서 A는 M의 자격을 받은 u 또는 M의 패스워드 PW_M 둘 중에 하나를 보지 못한다. 또한, 상대방 A는 F 또는 M 둘 중 하나를 속여 H로 가장할 수 없다. 이것은 이 메시지에 해당되기 때문이다. K_{FH}로 보호되고 n_F로 확인된 F를 위해 S_2가 만들어 지고 D로 보호되고 n_M으로 확인된 M을 위해 V_2가 만들어 진다.

3. 3S의 이동성 구조

MN이 nMAG로 이동하기위해 CN과 통신할 때 nMAG는 CN과 통신을 유지하기 위해서 핸드오버 절차를 시작한다. 이 절 에서는 먼저 기본적인 핸드오버 절차를 그림 7에 설명된 다음과 같은 단계로 구성하여 제안한다.

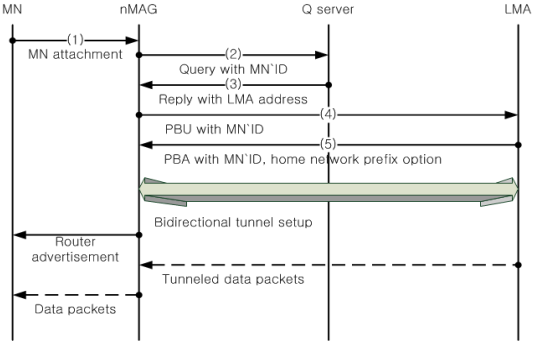

그림 7. 3S에서 기본 핸드오버 절차
Fig. 7. Basic handover procedure in 3S

1 단계) MN이 nMAG에 연결하면 액세스 인증 절차는 MN의 ID를 사용하여 수행된다. 성공적으로 인증되어 액세스되면 MN의 ID는 nMAG을 알 수 있다.

2 단계) nMAG는 MN이 속한 LMA의 IPv6 주소를 얻기 위해 Chord 시스템에 쿼리 메시지를 보낸다. 그것은 MN의 QServer에 도달할 때까지 쿼리 메시지는 Chord 노드로 라우팅된다. 위에서 언급한 바와 같이, 쿼리 메시지는 개인키를 사용하여 nMAG에 의해 서명되어야 한다.

3 단계) MN의 QServer는 nMAG에 MN이 속한 LMA의 IPv6 주소를 보낸다. 보안을 위해, QServer도 nMAG가 보낸 그 메시지에 서명을 해야 한다.

4 단계) nMAG는 MN을 대신하여 MN의 LMA에 MN의 ID를 포함하여 PBU 메시지를 보낸다. 다시 말하지만, MN의 LMA는 진위를 확인할 수 있도록 nMAG은 PBU 메시지에 서명을 해야 한다.

5 단계) LMA는 PBU 메시지를 받으면 nMAG의 공개키를 사용하여 PBU 메시지의 진위를 확인한다. nMAG가 인증된 경우, LMA 서명과 MN의 ID를 포함하여 반환하는 PBA 메시지, MN의 지원 주소 설정 모드, nMAG에 MN의 HNP옵션도 있다. 또한 nMAG에 터널을 통해 MN의 HNP에 대한 경로를 설정한다.

일단 nMAG가 PBA메시지를 받으면, 다음 단계로 표준 PMIPv6에서 지정한 기능을 수행 한다. 위의 절차에서 한 가지 큰 차이점은 nMAG하고 MN의 LMA는 AAA 서버에 쿼리 하는 것이 필요하지 않다는 것을 알 수 있다. 한편, nMAG이 먼저 MN의 LMA의 IPv6 주소를 얻기 위해 Chord 시스템에 메시지를 보내야 한다. 또한, 모든 메시지들은 보낸 사람의 개인키를 사용하여 서명되어 있다. 그 결과, 메시지들의 신뢰성은 보장된다. 따라서 표준 PMIPv6와는 달리, MN의 프로파일은 LMA에 저장되어 있기 때문에 3S가 AAA서버에 쿼리 하는 것은 필요하지 않다.

그러나 위의 핸드오버 절차에서 제시한 것은 nMAG이 보낸 쿼리 메시지가 여러 홉의 Chord 시스템에 전달될 수 있기 때문에 긴 핸드오버 지연을 발생할 수 있다. 이 문제를 해결하기 위해서 PMIPv6의 빠른 핸드오버 사용을 제안한다. 불행이도, nMAG이 어떤 MAG서버의 MN의 LMA인지 알지 못하기 때문에 3S에서 F-PMIPv6를 직접 사용하지 못하고 수정할 수 없다.

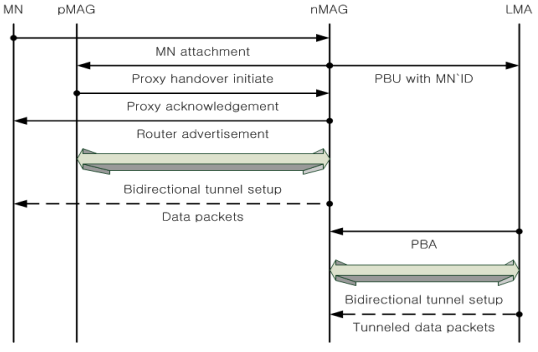

그림 8. PMIPv6에서 빠른 핸드오버 절차
Fig. 8. Handover message flows in fast PMIPv6

그림 8은 PMIPv6에서 수정된 빠른 핸드오버 절차를 보여 준다, 이것은 다음의 단계로 구성되어 있다.

1 단계) MN이 nMAG에 연결하면 액세스 인증 절차는 MN의 ID를 사용하여 수행된다. 성공적으로 액세스 인증되면 nMAG는 MN의 신원을 안다. 이 단계는 기본 핸드오버 절차 1 단계와 같다.

2 단계) 새로운 MAG는 MN의 이전 MAG(pMAG)에게 PHI(Proxy Handover Initiate) 메시지를 보낸다. PHI 메시지는 MN-ID를 포함 해야 한다.

3 단계) PHI메시지를 수신하면, pMAG는 nMAG에게 PAck메시지와 함께 응답한다. 그 메시지는 MN의 LMA IPv6주소와 MN ID로 MN 프로파일을 포함한다, MN의 주소 설정모드를 지원하고, MN의 HNP 옵션도 있다.

4 단계) nMAG가 MN의 프로필을 받으면, MN에게 RA(Router Advertisement) 메시지를 보낸다. 동시에, 그것은 MN의 LMA에 PBU 메시지를 보낸다.

5 단계) 데이터 패킷은 nMAG와 pMAG 사이의 터널을 통해 직접 전달하실 수 있다. nMAG이 pMAG에서 패킷을 받으면, 그것은 MN에게 보낸다.

6 단계) MN의 LMA는 nMAG에서 PBU 메시지를 받은 후 그것은 그 BCE(Binding Cache Entry)에서 MN의 위치를 업데이트한다. 그리고 nMAG에 PBA 메시지를 보낸다. 또한, 그것은 nMAG에 터널을 설정한다. 후속 패킷은 nMAG에 MN의 LMA에서 직접 전달된다.

7 단계) nMAG는 MN의 LMA에서 PBA 메시지를 받으면 그것은 MN의 LMA에 터널을 통해 MN의 HNP에 대한 경로를 설정한다. 또한, nMAG은 pMAG을 향해 터널을 설정한다.

보안을 위해, 모든 메시지는 자신의 개인키를 사용하여 보낸 사람에 의해 서명되어야 한다. 또한, nMAG는 [12]에서와 같이 PAR에 RtSolPr(Router Sends a Router Solicitation for Proxy)를 보내는 방법과 비슷한 방법으로 PHI 메시지를 보낼 수 있다. 다음 절에서와 같이 3S의 기본 핸드오버보다 3S의 빠른 핸드오버 방식이 핸드오버 지연이 훨씬 적다.

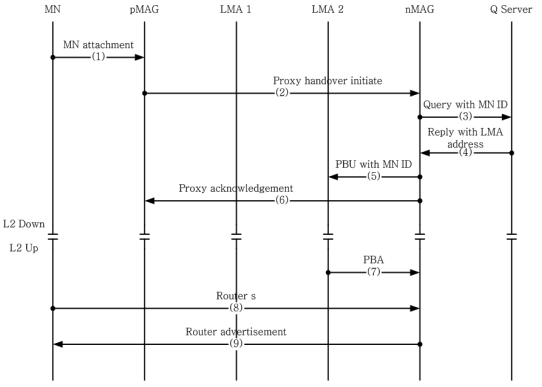

그림 9. 3S에서 빠른 핸드오버에 대한 메시지 흐름
Fig. 9. Handover message flows for fast handover in 3S

그림 9에서 3S에서 빠른 핸드오버 메시지 흐름을 보여준다. 그림 8과 그림 9를 비교하면 PMIPv6의 빠른 핸드오버와 3S의 빠른 핸드오버에서 명확한 하나의 차이점을 알 수 있다. 빠른 PMIPv6를 위한 핸드오버에서 nMAG는 pMAG에 PHI 메시지를 보내는 동시에 LMA에 PBU 메시지를 보낸다. 한편, 그것이 pMAG에서 PA 메시지를 받은 후 빠른 3S에 대한 핸드오버에 nMAG가 LMA에 PBU 메시지를 보낸다. 이것이 있기 때문에 3S의 빠른 핸드오버에서 nMAG는 MN의 LMA가 어느 MAG서버인지 알 수 없다. 따라서 그것은 PBU메시지를 보낸 위치를 알 수 없다. 반대로, PMIPv6의 빠른 핸드오버에서는 nMAG의 MN의 LMA를 알 수 있다. 그 결과 MN의 LMA에 직접 PBU메시지를 보낼 수 있다. 이 차이는 3S에서의 빠른 핸드오버와 PMIPv6에서의 빠른 핸드오버의 차이로 이어지는 것을 확인할 수 있다. 3S의 빠른 핸드오버에서 이 차이의 부작용은 많은 패킷이 pMAG을 통해 nMAG에 보내진다는 것이다. 3S의 빠른 핸드오버에서 nMAG는 PMIPv6의 빠른 핸드오버 이후에 PBU 메시지를 보낼 수 있기 때문이다. 그림 8과 그림 9를 비교하면, pMAG과 nMAG사이의 왕복 시간이 지연과 동일하다는 것을 알 수 있다. PMIPv6 도메인에서 pMAG와 nMAG가 비슷할 때 그들 사이의 왕복 시간은 일반적으로 몇 초에서 수만 밀리초의 범위를 갖는다. MAG의 커버 영역에서 MN이 상주하는 시간과 비교하면, 지연은 상주 시간에 비해 상당히 적다는 것을 다음 장에서 보여준다.

Ⅳ. 성능 평가

1. 3S 시스템 모델링

각각 M과 N을 PMIPv6 도메인의 MAG와 MN의 숫자로 한다. 더 나아가서 MAG의 요청 처리 수용력을 C, 하나의 MN이 초당 처리하는 MAG의 핸드오버 평균값을 p로 한다. 스토리지 요구사항과 처리능력에서 3S의 가능성을 분석할 수 있다.

1) 스토리지 요구사항 : MAG는 네 개의 테이블을 유지하기 위해 다음이 필요하다
- MN에 속한 모든 바인딩 업데이트 항목과 정책 개요를 저장하는 테이블
- MAG의 LMA의 각각의 MN에 대한 바인딩 캐시 항목을 기록하는 테이블
- MAG의 LMA의 각각의 MN의 개요를 저장하는 테이블
- Chord 시스템의 효율적인 검색을 위한 테이블

MN에 연결된 모든 것 들과 MAG는 바인딩 업데이트 항목과 이에 대한 정책 테이블을 저장해야 한다. 바인딩 업데이트 항목은 MN-ID를 포함한다(최대 128비트), MN의 연결 인터페이스의 링크계층 식별자(16비트), MN의 연결 인터페이스에 앞에 할당된 IPv6 홈 네트워크 목록(각각 128비트 필요), MN과 공유 엑세스 링크의 MAG 링크 로컬 주소(128비트), MN의 LMA의 IPv6주소(128비트), MAG와 MN 사이의 링크 인터페이스(대부분에서 128 비트), MN의 LMA와 MAG 사이의 양방향 터널의 터널 인터페이스 식별자(최대 128 비트), MN-ID를 포함한 정책 프로파일(대부분 128비트), MN의 LMA의 IPv6주소(128비트), 기타 옵션 필드(대부분 200비트). 모든 필드의 합계는 약(1,600 + 128 * S) 비트 MAG에서 MN의 바인딩 업데이트 항목 및 정책 프로파일을 저장할 저장 공간을 수반, 여기서 s는 MN의 연결 인터페이스에 할당된 숫자이다. 대략적으로 MAG가 MN의 바인딩 업데이트 항목 및 정책 프로필을 저장하는 데 약 3,000 비트의 저장 공간을 필요로 한다고 가정한다.

마찬가지로, MAG가 그 LMA 바인딩 업데이트 항목의 필드 및 바인딩 캐시 항목에 해당이 있기 때문에, MAG의 각 MN을 위한 MN의 바인딩 캐시 항목 및 정책 프로필을 저장하는 데 약 3,000 비트의 저장 공간을 필요하다고 가정한다.

테이블에서 모든 항목은 키(128 비트)와 다음 홉의 IPv6 주소(128 비트)를 포함한다. 따라서 테이블의 항목이 256 비트의 저장 공간을 가짐을 알 수 있다. 그러나 테이블 항목의 수가 MN보다 훨씬 적고, MN의 바인딩 캐시 항목을 저장하는데 필요한 저장 공간은 테이블 항목을 저장하는데 필요한 공간보다 훨씬 크기 때문에 테이블 저장 공간의 요구사항은 중요하지 않다.

따라서 MN는 약 6,000 비트의 저장 공간이 필요하다. 현재의 기술로, 하나의 DRAM은 2 기가비트의 저장 공간을 제공할 수 있다. 따라서 MAG는 300,000개 이상의 MN 대한 정보를 저장할 수 있다.

2) 처리 능력 : 3S의 성능을 제한하는 또 다른 요소는 MAG의 처리 능력이다. MN이 새로운 MAG에 연결할 때마다, 새로운 MAG는 MN이 속한 LMA의 IPv6 주소를 받아볼 수 있도록 Chord 시스템에 쿼리 메시지를 보낼 것이다. N-node의 코드 시스템에서 평균 라우터 쿼리 메시지의 경로는 $\log N/2$이다. 즉, 쿼리 메시지가 Chord 시스템에 의해 평균 $\log N/2$회 처리된다. MN의 QServer가 쿼리 메시지를 받으면, 그것은 MN이 속한 LMA의 IPv6 주소를 찾기 위해 캐시를 확인할 것이다. MN의 LMA가 MN의 새 MAG를 발견했을 때, 그것은 MN의 MAG에게 PBA메시지를 보내고, MN의 LMA에게 PBU메시지를 보낼 것이다. Chord 시스템의 MAG의 처리과정에서 MN의 핸드오버 비용은$(\log N/2+4)$이다. MN 이 MAG에서 초당 p의 핸드오버를 수행하는 경우, 초당 핸드오버의 총 개수는 M_p이다. 위 두 숫자의 곱, Chord 시스템의 초당 $(\log N/2+4)M_p$의 메시지 처리과정이 필요하다. 대부분 손실없이, 이 메시지가 동일한 처리 능력을 가진 모든 MAG에 의해 처리된다고 가정한다. 따라서 하나의 MAG에서 메시지를 처리하는 데 $(\log N/2+4)M_p/N$ 필요하다. 그러나 MAG의 처리능력은 C의 한계가 있다. 그것은 $(\log N/2+4)M_p/N \le C$ 이필요하다. $N=2^s$를 주어 M의 값을 다시 작성할 수 있다.

$$M \le \frac{C\times 2^{s+1}}{p\times(s+8)} \qquad (1)$$

위의 두 가지 측면에서 3S도메인에서 지원되는 MN의 총 숫자는 다음과 같다.

$$M \le \min\left(\frac{C\times 2^{s+1}}{p\times(s+8)}, 300{,}000\times 2^s\right) \qquad (2)$$

많은 메시지는 자신의 개인키를 사용하여 MAG에 의해 서명되기 때문에, MAG에 서명을 만들고 확인하는 것이 필요하다. 그것은 3 GHz의 프로세서 각각, ESIGN같은 빠른 암호 시스템을 사용하여 100~150 마이크로초에 2048비트의 서명을 작성하고 확인할 수 있다. 이것은 3 GHz의 프로세서가 각각 초당 6,600개의 서명을 만들어 확인하고, 10,000개의 서명을 할 수 있음을 의미한다. 또한 멀티코어 기술의 빠른 발전과 함께 미래의 MAG는 초당 10,000개의 메시지를 처리한다고 예상할 수 있다(즉, C = 10,000).

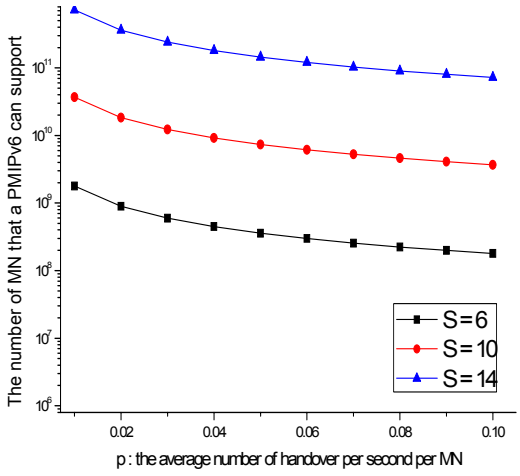

그림 10. SARP도메인이 p, s에 따라 처리할 수 있는 MN의 수

Fig. 10. The Number of MN that a SARP domain can support when p and s vary

그림 10은 p와 s가 다를 때 3S도메인에서 지원되는 MN의 개수를 보여준다. p는 그림 10에서 큰 값으로 중간으로 설정하고 나중에 이 절에서 설명한다. 이 그림에서, 하나는 분명 3S도메인이 10^7개의 MN에 대한 지원을 할 수 있다고 볼 수 있다면 P = 0.01 및 S = 6 이다(64 MAG에 해당하는). S를 유지하여 바꾸지 않고 p를 증가시키면, 3S도메인이 지원되는 MN의 숫자를 줄일 수 있다. p가 0.1증가하면, MN의 숫자는 약 10^6으로 줄일 수 있다. s가 10일때(1024 MAG에 해당하는), 3S도메인이 지원할 수 있는 범위의 MN의 숫자는 10^7(p가0.1)이다. 이 값은 3S도메인이 1024개의 MAG으로 구성되어 있다면 p=0.1일 때 10^7개의 MN을 지원할 수 있다는 것을 의미한다.

위 고려 사항으로 그림 11에서와 같이 단일 3S도메인은 N=16,384(즉, s=14)이면서 p=0.1일때 지원할 수 있는 값이 10^8MN개 이다. 단일 3S도메인에서 MN의 수를 더 늘리면 도메인 안에 더 많은 MAG를 배치하여 지원할 수 있다.

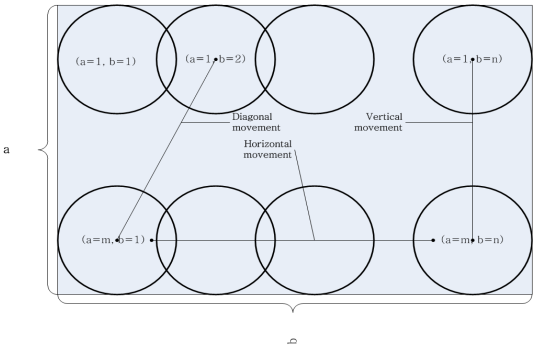

그림 11. 직사각형 네트워크 구성
Fig. 11. Rectangular network topology

3) p의 추정 : P의 범위를 0.01에서 0.1을 주어 보다 많은 3S의 가능성을 분석해본다. 이 절에서, 이 선택에 대한 이유를 제시한다. p는 MAG에 MN이 초당 수반되는 평균 핸드오버다. 이것은 일반적으로 APs이후 많은 APs에 연결 하려는 MAG과 APs에 연결한 비슷한 MAG에 PBU, PA 및 쿼리 메시지에 연결되지 못한 핸드오버 사이의 핸드오버 비율에 비해 낮은 핸드오버 비율이다. 이러한 목적으로, 각 MAG의 커버리지 영역 내에 MN의 평균 체류 시간을 분석한다. 특히, 임의의 좌표 이동성 모델[14]을 고려한다, 이것은 모바일 네트워크 연구에서 가장 자주 사용되는 모델이다. 이 모델에서, MN 무작위로 균일한 분포에 따라 관심의 영역에서 대상 지점(좌표)를 선택하고 이 지점에 직선에서 일정한 속도로 이동한다. 여기 일정한 속도는 ($V_{\min}$, $V_{\max}$) 사이에서 선택된다. 일정 시간 대기 후 새로운 대상과 이 대상에서 일정한 속도로 이동하는 속도 등을 선택 한다. 이 방법에서, 이동은 전이라 하고, 전환 기간 동안 경과 시간과 이동 거리는 각각, T와 L로 표시되고 전이 길이와 전환 시간이라고 표시한다. 이것을 기준으로 MN은 이 문서에서 0으로 간주되는 시간의 기간동안 고정되어 유지된다. 그 후, 새로운 전환이 시작된다.

평균 전이시간(E[T]로 표시됨)과 전환하는 동안 MAG의 커버리지 영역 사이의 횡단의 평균 개수(E [C] 로 표시됨) 의 계산이 필요하다.

$$p = E[C]/E[T] \tag{3}$$

그림 11에서 E[C]와 E[T]를 계산하기 위해 단일 SARP도메인이 커버할 수 있는 길이 b미터 폭 a미터의 직사각형 면적이 있다고 가정한다. 뿐만 아니라, 직사각형 영역은 m행과 n열의 MAG를 커버하고 커버리지 영역은 반경 R의 원으로 덮여져 있다고 가정한다. 임의의 좌표 모델에서 평균 전이 길이 E[L]은 [14]에 의해 주어진다.

$$E[L] = \frac{1}{15}\left[\frac{a^3}{b^2} + \frac{b^3}{a^2} + \sqrt{a^2+b^2}\left(3 - \frac{b^2}{a^2} - \frac{a^2}{b^2}\right)\right] + \frac{1}{6}\left[\frac{b^2}{a}\Phi\left(\frac{\sqrt{a^2+b^2}}{b}\right) + \frac{a^2}{b}\Phi\left(\frac{\sqrt{a^2+b^2}}{a}\right)\right] \tag{4}$$

$$\Phi(x) = \ln\left(x + \sqrt{x^2-1}\right).$$

전환 길이 L과 운동 속도 V는 임의의 좌표 모델에 독립적이므로 평균 전이 시간 E[T]는 다음 같이 계산할 수 있다.

$$E[T] = E[L/v] = E(L)E(1/v) \tag{5}$$

뿐만 아니라, 이동 속도 v는 ($V_{\min}$, $V_{\max}$)사이에서 균일하게 분포한다. 다음 식을 얻을 수 있다.

$$E(1/v) = \int_{V_{\min}}^{V_{\max}} \frac{1}{v} \times \frac{1}{V_{\max} - V_{\min}} dv = \frac{\ln(V_{\max}/V_{\min})}{V_{\max} - V_{\min}} \tag{6}$$

따라서 평균 전이시간 E[T] 5번 수식의 E[L]과 E[1/v]를 각각 4번 수식과 6번 수식으로 대체하여 얻을 수 있다. E[C]를 계산하기 위해서, 그림 11에 표시된 가로, 세로, 사선 세 종류의 움직임을 고려해야 한다. MAG(αi, βi)커버리지 영역에서 다른 MAG(αj, βj)으로의 이동성은 MAG의 횡단 숫자 c(αi, βi , α j , β j)는 MN과 MAG사이에서 주어진다[15].

$$c(\alpha_i, \beta_i, \alpha_j, \beta_j) = |\alpha_i - \alpha_j| + |\beta_i - \beta_j| \tag{7}$$

뿐만 아니라, MAG의 횡단 평균 개수 E[C]는 모든 가능한 MAG쌍 이상의 c(αi, βi, αj, βj) 평균으로 계산된다.

$$E[C]=\frac{1}{m^2n^2}\sum_{\alpha_i=1}^{m}\sum_{\beta_i}^{n}\sum_{\alpha_j=1}^{m}\sum_{\beta_j=1}^{n}c(\alpha_i,\beta_i,\alpha_j,\beta_j) \quad (8)$$

7번 수식을 이용하여c(αi, βi , α j , β j)를 대체하면 다음을 얻을 수 있다.

$$E[C]=\frac{1}{m^2n^2}\sum_{\alpha_i=1}^{m}\sum_{\beta_i}^{n}\sum_{\alpha_j=1}^{m}\sum_{\beta_j=1}^{n}(|\alpha_i-\alpha_j|+|\beta_i-\beta_j|) \quad (9)$$

a, b, R이 주어지면 다음을 구할 수 있다.

$$m=(a-L_0)/(2R-L_0), n=(b-L_0)/(2R-L_0) \quad (10)$$

여기서 L_0은 두 인접한 MAG의 커버리지 영역 간의 중복되는 거리이다. (3), (5), (9), (10)에서, P를 얻을 수 있다.

그림 12에서, $V_{\min}$=1, L_0=20미터, a=80000미터, b=60000미터인 $V_{\max}$ 변화에 의한 다른 R값의 평균값 p로 구성한다. 그림 11에서, 분명히 하나는 볼 수 있다. p가 0.094임에도 불구하고 R이 100미터이고 $V_{\max}$가 50미터/초로 매우 높은 속도라는 것이다. 뿐만 아니라, 그림 10에서 MAG이 커버할 수 있는 영역의 반경이 증가한다면 p가 크게 줄어든다. 예를 들어, R이 200m에서최대 속도가 50m/s인 경우 p는 약 0.045로 감소된다. 또한, R이 200m보다 크고 $V_{\max}$가 30m/s보다 작을 때 P는 0.03 이하이다.

그림 13에서, $V_{\min}$=1, L_0=20미터, a=30000미터, b=10000미터인 $V_{\max}$ 변화에 의한 다른 R값의 평균값 p에 대해 구체적으로 구성한다. 이 그림에서, 그림 13에서 비슷한 결과를 얻는다. 다른 값에 대한 곡선은 그림 12와 그림 13에 표시된 것과 매우 유사하며, 공간을 제한하기 위해 그들로 인해 표시되지 않는 것을 확인할 수 있다. 이러한 결과는 우리가 3S의 타당성을 분석했을 때 0.01에서 0.1에 이르기까지 P을 설정하는 합리적인 것을 나타낸다. 또한, 이러한 결과는 MN이 MAG의 적용 지역에 머무는 평균 체류 시간은 적어도 10 초인 것을 보여준다.

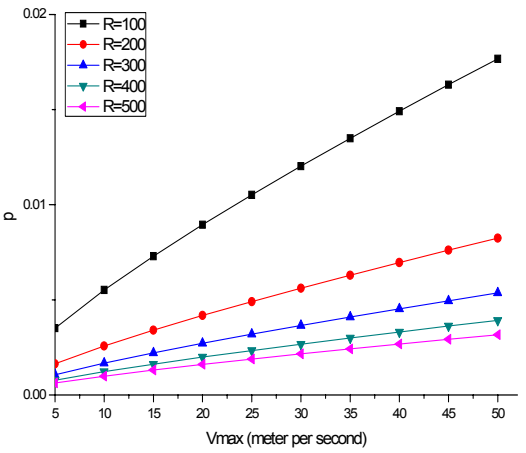

그림 12. R의 값에 따른 P의 평균값 ($V_{\min}$=1, L_0=20 meters, a=80,000 meters, b=60,000 meters)

Fig. 12. The Average Value of p for Different R when $V_{\min}$=1, L_0=20 meters, a=80,000 meters, b=60,000 meters

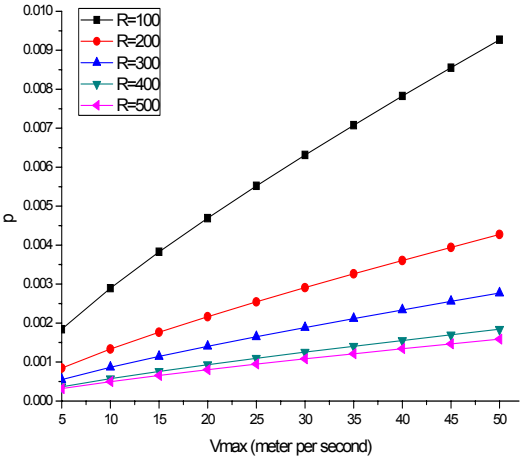

그림 13. R의 값에 따른 P의 평균값 ($V_{\min}$=1, L_0=20 meters, a=80,000 meters, b=60,000 meters)

Fig. 13. The Average Value of p for Different R when $V_{\min}$=1, L_0=20 meters, a=80,000 meters, b=60,000 meters

2. 핸드오버 지연시간 분석

이 절에서, 3S의 핸드오버와 SARP의 핸드오버, SARP의 빠른 핸드오버로 제안된 핸드오버 절차를 비교하여 도메인 내에서, 도메인 간의 핸드오버 지연시간을

분석한다.

핸드오버 지연시간은 많은 요인에 의해 영향을 받을 것이므로 모델화하는 것이 어렵다. [13]에서 사용되는 것과 같은 방식을 사용하고 [14]를 분석한 모델을 그림 14에 보여준다.

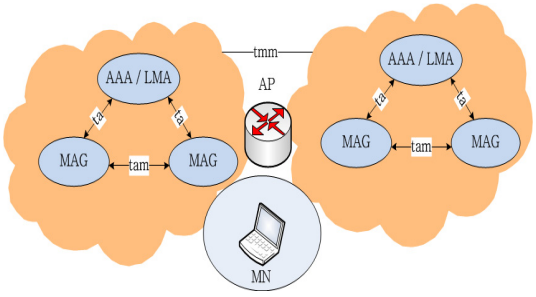

그림 14. 핸드오버 지연시간 분석을 위한 분석모델
Fig. 14. An analytical model for handover latency analysis

MN과 MAG사이의 평균지연과 MAG와 MAG사이의 평균지연은 t_{mm}이다. 이것은 MN와 MAG사이, MAG와 MAG사이의 패킷 전송에 필요한 시간이다. MAG와 LMA간의 평균 지연은 t_{am}이다. 대부분의 손실없이 PMIPv6 도메인에서 두 MAG 간의 지연도 t_{am}이라고 가정한다. MAG와 AAA 간의 평균 지연은 t_a이다.

3S의 핸드오버를 [14]의 분석방법으로 평균 핸드오버 지연은 다음과 같다.

$$D_{3S}^{Intra} = t_{mm} \tag{11}$$

$$D_{3S}^{Inter} = D_{3S}^{Intra} \tag{12}$$

SARP의 기본 핸드오버에서 핸드오버 평균 대기시간은 다음과 같이 구성되어 있다. MAG에서 MN에 대한 평균 지연(t_{mm}), MAG에서 QServer에 쿼리 메시지를 보내기 위한 평균 지연(T_{query}), QServer와 MAG사이의 평균지연(t_{qm}), 그리고 MAG와 LMA간의 평균 왕복지연($2t_{am}$). QServer와 MAG가 직접 연결되지 않을 수도 있기 때문에, $t_{qm} = t_a$라 가정한다. 또한, T_{query}는 Chord 시스템에서 쿼리 메시지가 지나가는 홉수(h)와 Chord 시스템에서 각 홉의 평균 지연(t_{aa})에 의존적이다. t_{qm}과 마찬가지로, $t_{aa} = t_a$라고 가정한다. t_{aa}와 t_{qm}에 적합한 MAG에서 AAA서버가 직접 연결되지 않아서 발생하는 평균 지연의 t_a를 추정한다. [5]에서, h가 속한 [0, log$_2$N](즉, h ∈ [0, s])과 그것의 평균이 $\frac{s}{2}$라는 것을 알 수 있다. 결과적으로, SARP의 기본 핸드오버에서 핸드오버 평균 대기시간은 다음과 같이 주어진다.

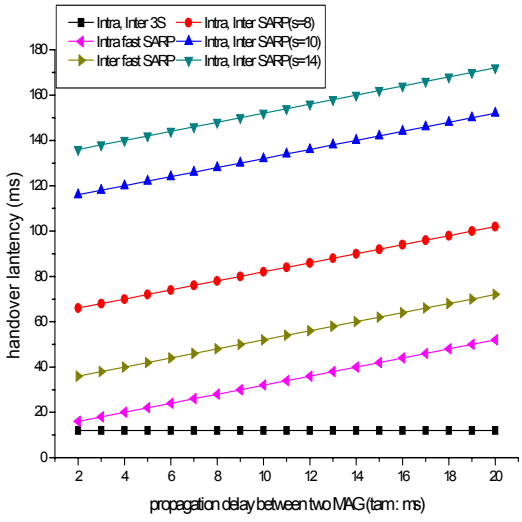

그림 15. 핸드오버 지연시간 분석(t_{mm} = 12ms, t_a = 10ms)
Fig. 15. Comparison of handover latency for the four handover approaches when t_{mm} =12ms and t_a =10ms

$$\begin{aligned} D_{SARP-basic}^{Intra} &= T_{query} + t_{qm} + 2t_{am} \\ &= h \times t_a + t_a + 2t_{am} + t_{mm} \\ &= (h+1)t_a + 2t_{am} + t_{mm} \end{aligned} \tag{13}$$

$$D_{SARP-basic}^{Inter} = D_{SARP-basic}^{Intra} \tag{14}$$

SARP의 빠른 핸드오버에서 핸드오버 평균 대기시간은 다음과 같이 구성되어 있다. MAG에서 MN으로의 평균 패킷 전송지연 (t_{mm})과 nMAG와 pMAG사이의 평균 지연 ($2t_{am}$) 이다.

$$D_{SARP-fast}^{Intra} = 2t_{am} + t_{mm} \tag{15}$$

$$D_{SARP-fast}^{Inter} = D_{SARP-fast}^{Intra} + 2t_{qm} \tag{16}$$

SARP의 빠른 핸드오버 평균 대기시간을 계산했을 때 MN의 nMAG와 MN의 LMA 간의 지연을 고려하지 않는 것을 확인할 수 있다. MN의 LMA가 MN의 pMAG에게 패킷을 보낼 수 있기 때문에 MN의 nMAG으로 가는 터널링된 패킷은 MN이 nMAG으로부터 패킷을 받을 수 있도록 한다.

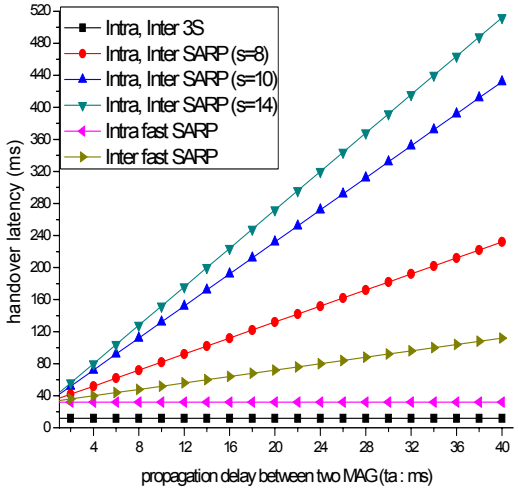

그림 16. 핸드오버 지연시간 분석(t_{mm} = 12ms, t_{am} = 10ms)
Fig. 16. Comparison of handover latency for the four handover approaches when t_{mm} =12ms and t_{am} =10ms

그림 15에서 t_{mm} = 12ms 이고 t_a = 10ms 일 때 위에서 언급한 3가지 경우에서의 변화에 대한 핸드오버 지연을 비교한다. 3S의 핸드오버에서, 평균 핸드오버 지연의 h를 다음과 같이 구성한다(h=s/2).

위 결과에서 3S의 핸드오버가 가장 낮은 평균 핸드오버 지연을 갖는다. 이는 두 인접한 MAG의 평균 왕복 지연에 의존하기 때문이다. 뿐만 아니라, 3S 핸드오버의 평균 핸드오버 대기 시간과 3S의 빠른 핸드오버의 평균 핸드오버 지연을 비교했을 때, 3S의 빠른 핸드오버의 핸드오버 대기 시간이 상당히 낮음을 알 수 있다.

그림 16에서 t_{mm} = 12ms 이고 t_{am} = 10ms일 때 위에서 언급한 3가지 경우에서의 변화에 대한 핸드오버 지연을 더 비교한다. 특히 t_a가 큰 경우(예, 40ms), SARP 핸드오버에서 핸드오버 지연은 너무 길어진다. 실시간 어플리케이션에서는 일반적으로 150ms보다 낮은 핸드오버 지연을 요구한다. 한편, 3S의 핸드오버와 SARP의 빠른 핸드오버는 매우 낮은 평균의 핸드오버지연 값을 갖는다. t_a가 2ms에서 40ms로 변할 때 3S의 핸드오버 지연과 SARP에서의 빠른 핸드오버 지연은 t_a에 의존하지 않기 때문에 낮은 핸드오버 지연시간을 갖는다. 3S의 핸드오버는 매우 낮은 핸드오버 지연 값을 갖는다.

3. 3S와 SARP의 비교

SARP와 함께 그 위에 표시되어 있고, PMIPv6 도메인이 10^8이상의 MN와 수도권을 커버할 수 있다. 따라서 MN는 같은 지역 내에서 돌아다닐 때, 하나의 PMIPv6 도메인이 같은 지역을 커버 할 수 있기 때문에 PMIPv6 도메인간의 핸드오버가 없다. 그러나 PMIPv6에 대해 먼저 PMIPv6 도메인이 같은 지역을 커버하고 MN의 같은 수를 지원하는 것이 불가능한 것을 확인할 수 있다. 따라서 우리가 같은 지역을 커버하는 많은 PMIPv6 도메인을 사용하는 것은 그의 평균적으로 지연될 평균 SARP 도메인의 지연을 핸드오버보다 훨씬 긴 PMIPv6 도메인간 핸드오버 연결을 그림 17에서 보여준다.

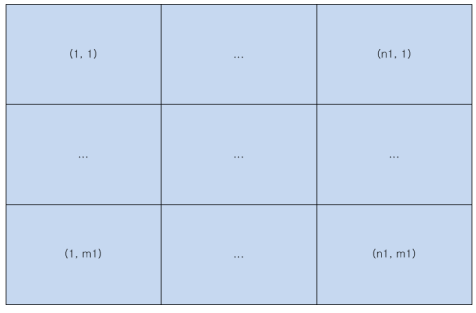

그림 17. PMIPv6도메인의 구획
Fig. 17. Layout of PMIPv6 domains

비교를 위해, SARP에 대한 위의 타당성 분석에 사용되는 임의의 좌표 모델과 직각의 서비스 지역을 고려한다. 뿐만 아니라, 표준 PMIPv6에서 LMA는 Q MN에 대한 트래픽과 km^2 마다 S MN가 있다는 것을 다룰 수 있다고 가정한다.

그러므로 길이를 A m와 너비 B m 직각의 지역을 제공하면 MN의 총 개수는 다음 식으로 계산된다.

$$M = \frac{a}{1000} \times \frac{b}{1000} \times S = 10^{-6} \times a \times b \times S \quad (17)$$

모든 PMIPv6도메인이 오직 하나의 LMA를 유지한다고 가정하면, 사각 토폴로지를 커버하는데 필요한 PMIPv6도메인의 총수는 다음으로 계산된다.

$$N_D = \frac{M}{Q} = \frac{a \times b \times S}{10^6 \times Q} \tag{18}$$

일반적인 손실없이, PMIPv6 도메인의 범위 영역이 M 및 N, 수직 및 수평 도메인이 각각 있도록 그림 17과 같이 레이아웃을 가지고 있다고 가정한다. 하나의 전환 기간 동안 PMIPv6 도메인 사이의 핸드오버 평균값은

$$E[C] = \frac{1}{3}\left(m_1 + n_1 - \frac{1}{m_1} - \frac{1}{n_1}\right) \tag{19}$$

$m_1 \times n_1 = N_D$ 이기 때문에, $m_1 = n_1 = \sqrt{N_D}$ 일 때 E[C]에서 분명히 최소값을 얻을 수 있다.

$$\begin{aligned} E[C]_{\min} &= \frac{1}{3}\left(\sqrt{N_D} + \sqrt{N_D} - \frac{1}{\sqrt{N_D}} - \frac{1}{\sqrt{N_D}}\right) \\ &= \frac{2}{3}\left(\sqrt{N_D} - \frac{1}{\sqrt{N_D}}\right) \\ &= \frac{2}{3}\left(\sqrt{\frac{a \times b \times S}{10^6 \times Q}} - \sqrt{\frac{10^6 \times Q}{a \times b \times S}}\right) \end{aligned} \tag{20}$$

그림 18은 Q=100,000에서 a, b, S가 변할 때 E[C]min을 보여준다. 이 그림에서 이동에 따른 핸드오버 수가 a=b=10km이고 S=1,000인 경우를 제외하고 0보다 큰 것을 분명하게 관찰할 수 있다. S(즉 MN의 밀도)가 증가하면 이동에 따른 핸드오버 평균값도 증가한다. 마찬가지로 네트워크 서비스 지역이 확대되면 이동에 따른 핸드오버 평균값도 증가한다.

S가 변하지 않고 유지하면 단순히 100km에서 6400km로 서비스 지역이 증가하는 경우 PMIPv6 도메인 간 핸드오버의 평균 개수는 5이상 증가한다. 마찬가지로, 서비스 지역이 변하지 않으면, PMIPv6 도메인 사이 핸드오버의 평균값은 0부터 약 3 증가한다. 비교하면, 단일 SARP도메인이 6,400km 전체 영역을 커버 할 수 있더라도 S = 20,000 이후 이 경우, MN의 총 개수는 단 1.28×10^8이다, 이것은 지금까지 단일 SARP도메인의 한계이다.

하나의 LMA는 10만 개 이상의 MN를 지원할 수 있다고 말할 수도 있지만 100만으로 S를 높이고 해당하는 E[C] min을 구상하여 그림 19에서 보여준다. 이 그림에서 S = 100,000과 비교했을 때 핸드오버 평균수는 감소하지만 PMIPv6 도메인 간의 핸드오버들의 평균수가 대부분 0보다 큰 것을 볼 수 있다.

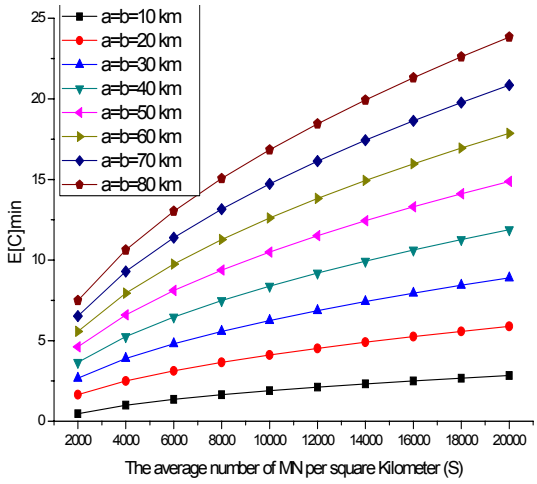

그림 18. 표준 PMIPv6의 LMA가 100,000 MN를 다룰 때, 전환당 평균 핸드오버 개수

Fig. 18. The average number of handovers per transition when a standard PMIPV6 LMA is able to deal with 100,000MN

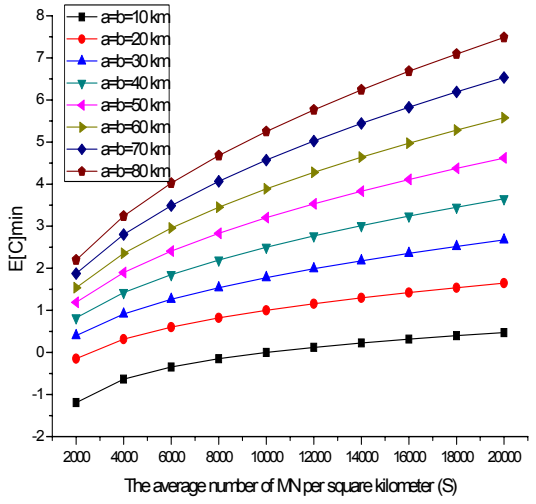

그림 19. 표준 PMIPv6의 LMA가 1,000,000 MN를 다룰 때, 전환당 평균 핸드오버 개수

Fig. 19. The average number of handovers per transition when a standard PMIPv6 LMA is able to deal with 1,000,000 MN

V. 결 론

본 논문에서 확장가능한 안전하고 끊김없는 PMIPv6 도메인 구축을 제안하는 3S기법을 제안한다. 제안된 기법에서 모든 MAG은 LMA로 동작한다. 잘 알려진 분산 해시 테이블 프로토콜인 Chord를 기반으로 3S를 고려한 도메인을 모두 MAG으로 구성한다. MN과 LMA간의 바인딩은 일관된 해싱을 사용하고 Chord 시스템을 통해 배포된다. 또한 SARP이 제안한 도메인이 PKI서버를 유지하는 것은 도메인 안의 모든 MAG에 대한 공개/개인키 쌍을 가지고 있어야 한다는 의미이다. 보안이 보장되도록 3S를 고려한 도메인의 모든 핸드오버 관련 메시지는 서명된다. 3S를 고려하여 도메인의 핸드오버 절차를 제안하고 타당성을 분석했다. 결과적으로, 3S를 고려한 도메인이 상당히 많은 MN을 지원할 수 있다는 것을 보여준다.

향후에 3S의 추가적인 성능 향상을 도모하기 위한 연구를 지속할 것이며, 지금보다 더 많은 MN을 지원하면서도 도메인 내에서 또는 도메인 간의 이동시에도 상당히 낮은 핸드오버 지연을 유지할 수 있는 방안을 연구하여 3S의 성능을 더욱 발전시켜 나갈 것이다.

참 고 문 헌

[1] Ibrahim Al-Surmi, Mohamed Othman, and Borhanuddin Mohd Ali, “Mobility management for IP-based next generation mobile networks: Review, challenge and perspective”, Journal of Network and Computer Applications, Volume 35, Issue 1, Pages 295-315, January 2012

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil,“Proxy mobile IPv6,” IETF RFC 5213, Aug. 2008.

[3] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in IPv6,” IETF RFC 3773, June 2004.

[4] Hongbin Luo, Hongke Zhang, Yajuan Qin, and Victor C. M. Leung, "An Approach for Building Scalable Proxy Mobile IPv6 Domains," IEEE Trans. Netw., Vol. 8, No. 3, September 2011.

[5] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F.Dabek, and H. Balakrishnan, “Chord: a scalable peer-to-peer lookup protocol for Internet applications,” IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 17-32, Feb. 2003.

[6] D. Eastlake and P. Jones, “US secure hash algorithm 1 (SHA1),” IETF RFC 3174, Sep. 2001.

[7] D. R. Karger, E. Lehman, F. Leighton, M. Levine, D. Lewin, and R. Panigrahy, “Consistent hashing and random trees: distributed caching protocols for relieving hot spots on theWorldWideWeb,” in Proc. 29th Annu. ACM Symp. Theory Comput., May 1997, pp. 654-663.

[8] A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury, “Mobile node identifier option for mobile IPv6 (MIPv6),” IETF RFC 4283, Nov. 2005.

[9] L. R. Monnerat and C. L. Amorim, “D1HT: a distributed one hop hash table,” in Proc. 20th IEEE International Parallel & Distributed Processing Symposium, Apr. 2006.

[10] Tao Zhou, Jing Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks"

[11] C.C. Chang, C.Y. Lee, Y.C. Chiu, Enhanced authentication scheme with anonymity for roaming service in global mobility networks, Computer Communications 32 (2009) 611 - 618.

[12] R. Koodli, “Fast handovers for mobile IPv6,” IETF RFC 4068, July 2005.

[13] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, “Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6,” IEEE Wireless Commun., vol. 15, no. 2, Apr. 2008.

[14] Q. B. Mussabbir, W. Yao, Z. Niu, and X. Fu, “Optimized FMIPv6 using IEEE 802.21 MIH services in vehicular networks,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3397-3407, Nov. 2007.

[15] C. Bettstetter, H. Hartenstein, and X. Perz-Costa, “Stochastic properties of the random waypoint mobility model,” Wireless Netw., vol. 10, no. 5, pp. 555-567, Sep. 2004.

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0027030) 교신저자 : 정종필

저자 소개

강 민(준회원)

- 2009년 한양사이버대학교 컴퓨터공학과(공학사)
- 2009년~ 현재 성균관대학교 정보통신대학원(석사과정)

<주관심분야 : Network Mobility, Network Security>

정 종 필(정회원)

- 2008년 성균관대학교 정보통신대학(공학박사)
- 2009년 성균관대학교 컨버전스연구소 연구교수
- 2010년~현재 성균관대학교 산학협력단 산학협력중점교수

<주관심분야 : 모바일컴퓨팅, 센서 이동성, 차량 모바일 네트워크, 스마트기기 보안, 네트워크 보안, IT융합, 인터랙션사이언스 등>