AAA 기반의 인증을 이용한 HMIPv6 성능 개선 기법

(Performance Enhancement of AAA-based Authentication for HMIPv6)

김 미 영 † 문 영 성 ††
(Miyoung Kim) (Youngsong Mun)

요 약 이동시 발생하는 시그널링 메시지의 양을 줄이기 위한 방법으로 지역성을 고려한 계층적 이동성 제공 방식인 HMIPv6(Hierarchical Mobile IPv6)가 제안되었다. 이동 노드가 방문 링크로 이동하면 링크 사용을 위한 인증 절차를 먼저 수행해야한다. 이를 위해 무선 랜 및 Cellular 망을 중심으로 AAA(Authentication, Authorization and Account) 인증 서비스 도입이 진행되고 있다. 그러나 AAA 인증 서비스는 지역화 된 이동성 제공을 위한 최적화된 시그널링 교환을 제공하지 않는다. 이는 실시간 응용을 필요로 하는 세션을 가진 경우 이동 노드에 대한 서비스 지연을 초래할 수도 있다. 본 논문에서는 지역 이동시 인증 과정을 최적화 할 수 있는 인증 위임 방식을 기존의 HMIPv6 구조에 통합함으로써 인증 발생 시 시그널링의 양을 최소화 하고 서비스 지연 시간을 줄일 수 있는 방법을 제안한다. 계층적 인증 통합 모델을 제안하며 제안된 모델에 대해 이동 특성, 트래픽 특성, 도메인 크기 등에 따르는 인증 비용을 분석하고 기존의 방식과 비교하였는데 평균 33.6%의 비용 절감 효과를 얻을 수 있었다.

키워드 : Mobile IPv6, HMIPv6, AAA, DIAMETER, Authentication

Abstract *To reduce the amount of the signaling messages occurred in movement, HMIPv6 has* been introduced as the hierarchical mobility management architecture for MIPv6 by regarding the locality of movements. When approaching the visited link, the authentication procedure should be done successfully prior to any mobility support message exchanges. The AAA(Authentication, Authorization and Account) authentication service is applied gradually to the wireless LAN and Cellular networks. However, It may bring about the service latency for the sessions of requiring the real-time processing due to not providing the optimized signaling in local and frequent movements. In this paper, we propose the authentication architecture with 'delegation' scheme to reduce the amount of signaling message and latency to resume for local movements by integrating it with HMIPv6 architecture. We provide the integrated authentication model and analyze the performance and effectivity of our proposal and finally offer the analysis materials comparing to the exiting authentication scheme. It cuts down the cost to 33.6% at average measurement.

Key words : Mobile IPv6, HMIPv6, AAA, DIAMETER, Authentication

1. 서 론

IP 이동성을 제공하기 위한 프로토콜 및 이동성 바인딩을 제공하기 위한 연구가 IETF 산하 mobile ip WG에서 진행 중이며 표준화 단계에 와 있다. 이동 단말이 빈번한 이동 특성을 가지는 경우 바인딩 갱신 작업이 많이 발생하며 빈번한 인증 절차로 인해 대량의 트래픽을 유발하므로 이는 QoS 요구 사항을 만족 시킬 수 없는 위험한 요인으로 부각되고 있다. 따라서 지역 이동성에 대한 연구 및 견고한 보안 제공 방안에 관한 연구가 진행 중이다. HMIPv6는 한 도메인 안에서 빈번한 이동이 발생하는 경우 로컬에서 이동성을 처리해줌으로써 MIPv6 전체적인 시그널링 메시지의 양을 줄일 수 있는 방법이다[1].

· 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음
† 정 회 원 : 숭실대학교 정보미디어연구소 연구원
mizero31@sunny.soongsil.ac.kr
†† 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@computing.ssu.ac.kr
논문접수 : 2004년 9월 2일
심사완료 : 2005년 5월 16일

HMIPv6는 FMIPv6와 더불어 이동 발생 후 서비스 재개까지의 지연 시간을 최소화하기 위한 방법으로서 HMIPv6는 지역 이동성을 고려한 접근 방법으로써 전체적인 이동성 시그널링 메시지의 양을 줄이는 방법에 초점을 두고 있으며, FMIPv6(Fast Mobile IPv6)는 Layer2의 지원을 받아 빠른 핸드오프 처리를 통해 접속 지연을 줄이기 위한 방안에 중심을 두고 있다.

무선랜 기술을 적용한 고대역의 핫스폿 서비스가 보편화 되고, 셀룰러 망에서의 안전한 사용자 인증을 위한 보안 인프라 도입의 필요성이 증가함에 따라 DIAMETER 기반의 AAA 서비스 도입이 각 기술 분야별로 적용 및 보완되고 있는 실정이다[2].

본 논문에서는 HMIPv6와 동일한 계층적 접근 방식을 인증 기능에 추가함으로써, 지역 이동 발생 시 이동성 제공 시그널링 메시지의 최적화와 동시에 인증 메시지 최적화를 가능하도록 하였다. 이를 위해 '인증 위임' 기능을 AAA[3] 엔티티에 도입하였고, 지역 이동이 발생할 때 인증 기능을 위임 받은 AAA 엔티티가 이동노드의 홈 AAA 서비스 엔티티를 대신해서 인증 처리 및 키 재료 분배를 하도록 하였다.

2장에서는 본 논문에서 제안하는 시스템 인증 모델과 'MAP+AAAv' 엔티티를 기술하며, 3장에서는 기존 방식의 문제점 및 인증의 필요성을 기술하고 본 논문에서 제안하는 방식의 인증 절차에 대해 설명한다. 4장에서는 제안된 인증 방식에 대한 시스템 모델을 기반으로 비용 분석 및 성능을 평가하며 5장에서는 결론을 맺는다.

2. 지역 이동을 고려한 인증확장 구조

2.1 지역이동을 고려한 HMIPv6 인증의 필요성

HMIPv6의 지역 이동성 처리를 위해 반드시 인증이 선행되어야 하므로 인증 성능은 HMIPv6의 지역 이동성 서비스 및 진행 중인 세션에 대한 성능에 크게 영향을 준다. 그러나 기존의 AAA 인증 방식에서는 지역 이동과는 무관하게 방문 도메인과 홈 도메인의 AAA서버 간의 메시지 교환을 통한 인증처리를 제공하므로 HMIPv6 전체 성능의 저하를 초래한다. 따라서 이동 노드의 이동 특성을 고려한 신속한 핸드오프 처리 및 서비스 재개를 위한 인증 방법이 제공되어야 한다.

2.2 보안을 고려한 HIMPv6 인증 문제점

mobile ip 작업 그룹 내에서는 지역 이동 특성을 가지는 경우, 이동 노드의 이동 경계를 로컬 범위 내에서 별도 처리할 수 있도록 임시적인 홈 에이전트 기능을 가지는 MAP을 설치해서 로컬 도메인 내에서의 이동을 대신 처리하도록 하고 있으며 이동노드의 특성 및 MAP 도메인 크기에 대한 성능 분석 결과가 보고되고 있다[4]. 그러나 이 경우 홈 등록 시 HMIPv6 상에서 여러 가지 보안 위협이 발생할 수 있다[3].

2.2.1 MAP 발견을 위한 라우터 광고

이동 노드가 새로운 MAP 도메인으로 이동한 경우, 도메인을 관할하는 엑세스 라우터로부터 MAP 정보를 포함하고 있는 라우터 광고 메시지를 수신하고 이 메시지를 통해 MAP 리스트를 얻고 사용할 MAP을 결정하게 되는데, 만일 악의적인 사용자가 위조된 라우터 광고 메시지를 멀티캐스트 하는 경우, 이동 노드는 잘못된 MAP 정보를 얻게 되며, 이동 노드가 보내는 패킷은 가로채 질 수 있다. 이는 근본적으로 라우터와 이동 노드 간에 SA(Security Association)가 존재하지 않으므로 인해 발생하는 문제이다. 이 문제를 처리하기 위해 현재 SEND(SEcuring Neighbor Discovery) 작업 그룹에서는 라우터 발견시 IPsec(Internet Protocol Security) 및 CGA(Cryptographically Generated Address) 을 사용한 보안을 권고하고 있으나, 수동으로 키 입력 작업을 해야 하므로 노드수가 많은 링크의 경우 많은 부하가 따른다. 그러므로 동적인 SA 구성이 가능한 인프라 구조가 도입되어야 한다.

2.2.2 MAP을 통한 RCoA 구성

새로 발견한 MAP과 이전 MAP의 주소가 다른 경우, 이동 노드는 새로운 MAP 도메인으로 이동하였으므로 MAP과 홈 에이전트로 바인딩 등록을 위해 LCoA(Local Care-of Address)와 RCoA(Regional Care-of Address)를 구성해야 한다[1]. LCoA는 이동 노드가 현재 존재하는 링크 상에서 Stateless 방식으로 구성되며 RCoA는 엑세스 라우터에서 광고해준 MAP의 정보, 프리픽스 정보 및 각종 플래그 값을 통해 구성된다. 이때 악의적인 노드에 의해 광고 내용이 변경될 수 있으며 프리픽스 정보가 변경되는 경우 LCoA와 RCoA의 네트워크 주소가 위조되어 서비스 거부 공격을 받을 수 있고, MAP의 정보나 플래그 값의 변경을 통해 패킷을 가로채 위조할 수 있다. 그러므로 이를 방지하기 위해 반드시 보안 서비스가 우선적으로 제공되어야 한다.

2.2.3 로컬 바인딩 등록/응답

이동 노드가 동일한 MAP 도메인 내의 서브넷 간에 이동하는 경우 홈 등록이 필요 없고 단지 현재 속한 MAP에 로컬 바인딩 정보(LCoA)를 등록하면 된다. 그러나 이동 노드와 MAP간에 사전에 설정된 SA가 존재하지 않으므로 두 엔티티간의 메시지는 악의적인 노드에 의해 [3]에 기술된 방식에 의해 도청당할 수 있다. 이동 노드가 보내는 바인딩 등록 메시지에는 현재 구성한 LCoA 정보가 포함되어 있는데 만일 이 값이 위조된다면 상대 노드가 보내는 모든 패킷은 잘못된 주소로 터널링 되어 악의적으로 도용될 수 있다. 또한 이동 노드가 바인딩 등록 메시지를 전송한 후 반드시 응답을 수

신해야 하는데, 악의적인 노드가 응답 패킷을 가로채거나 응답 내용을 변경함으로써 이동 노느는 실패 처리된 응답을 수신하고 이 결과 MAP으로의 바인딩 등록이 실패하므로 진행 중인 연결은 모두 잃어버리게 될 수도 있다. 따라서 이동 노드와 MAP간의 바인딩 등록 및 응답 메시지의 송신자를 반드시 인증해야 한다[3].

2.3 HMIPv6 인증 확장 구조

도메인 내에서의 지역 이동성을 가질 때 이동 노드가 유지하고 있는 세션에 대한 신속한 재개를 위해 핸드오버에 따르는 지연 시간을 최소화해야 한다. 지역적인 이동성 관리 구조인 HMIPv6는 바인딩 등록 절차로 인한 패킷 손실 및 세션 지연에 대해 위의 목적을 충분히 만족시키지만, 이동 노드가 방문 링크 상에서 이동할 때 대부분의 경우 방문 링크와 홈 링크상의 보안 엔티티 간에 사전 SA를 가지지 않으므로 BST(Base Transceiver Station) 공격이나 DoS(Denial of Service)등의 공격을 방지하기 위해 방문 링크와 이동 노드는 상호 인증 절차를 우선적으로 수행해야 한다. 인증이 실패하면 Attendant에서는 802.1x에 기술된 포트 제어 기능을 통해 이동 노드의 세션 트래픽을 차단하거나 제한적으로 사용하도록 제어하게 되므로 성공적인 인증 수행 여부는 이동 노드의 핸드오버에 따른 중요한 비용으로 여겨진다. 본 논문에서는 HMIPv6와 인증 제안을 구조적으로 통합함으로써, HMIPv6엔티티인 'MAP+AAA'에서 일관된 방법으로 지역 이동성을 처리하기 위한 바인딩과 인증 절차를 수행하도록 하였다.

Random-Walk모델의 특징은 이동할 다음 위치는 현재 위치와 적절히 산포된 랜덤 집합에 있는 값에서 임의로 선택한 값을 더해서 얻을 수 있다.만일 어느 순간의 이동으로 인한 상태 천이가 이산 집합을 형성한다면 이는 이산 시간 Random-Walk로 볼 수 있다[5,6]. 본 논문에서는 이동 간격이 이산 시간 분포를 따른다고 가정하므로 이는 SMP(Semi-Markov Process)의 특수한 경우에 해당한다.

2.4 지역성을 고려한 인증 절차

이동 노드가 바인딩 등록 요청을 하기 전에 먼저 인증이 완료되어야 하고 바인딩 등록을 위한 바인딩 키를 생성해야 한다. 먼저 IPsec을 사용한 인증 및 키 교환의 경우 확장이 어렵고 암호 처리에 대한 이동 노드의 부담이 상대적으로 증가하며, SA를 새로 설정해야 하는 경우 IKE(Internet Key Exchange) 메시지 교환 절차를 수행하므로 메시지 라운드트립 횟수가 증가하게 된다. 다른 방법으로 RADIUS(Remote Access Dial-In User Service)나 DIAMETER 등의 인프라를 통한 노드 인증 방법이 있다. AAA 기반의 인증 방식은 인프라 자체의 강력한 보안 및 확장성을 제공한다. 메시지 교환 절차는 [7-9]에 나타낸 바와 같다. 그러나 빈번한 이동이 발생하는 경우 대량의 인증 및 바인딩 등록을 위한 트래픽이 발생하므로 이를 처리하기 위한 오버헤드 및 처리 지연은 실시간 응용을 요하는 이동 노드에게는 부담 요인으로 작용할 수 있다. 따라서 HMIPv6 구조에 적합하도록 인증 구조를 통합해야 하고 지역적으로 발생하는 이동에 대해서 도메인 내부에서 인증 처리를 가능하도록 하는 것이 바람직하다. 이동 노드의 이동 특성을 크게 MAP 도메인 내에서의 지역적인 이동성 및 MAP 도메인 간에 발생하는 MAP 도메인 간 이동으로 나눌 수 있으며 전자의 경우 도메인 내부에서 인증 및 바인딩 처리를 가능하게 해야 하고 후자의 경우는 이동 노드의 홈 도메인을 포함한 인증 엔티티들의 상호 작용을 통해 인증 및 바인딩 처리가 제공되어야 한다. 여러 개의 서브넷으로 구성된 하나의 MAP 도메인을 가정할 때 단위 시간당 이동 노드가 이동하는 횟수와 속성에 대해 확률적으로 MAP간 이동 발생보다 MAP 도메인 내부에서 이동이 발생할 확률이 높다. 따라서 MAP 내부에서 발생하는 이동의 경우 내부에서 인증 처리를 해준다면 인증 메시지 오버헤드 및 라운드트립을 크게 줄임으로써 전체적인 성능 향상을 이룰 수 있다. 본 논문에서 제안하는 '위임' 기능은 홈 도메인의 보안 엔티티에서 처리해야 할 인증 능력 및 권한을 이동 노드가 현재 방문하고 있는 도메인의 보안 엔티티에게 주어진 시간 동안 위임하고, 지역 이동성이 발생하는 경우 방문 도메인의 보안 엔티티가 인증 및 바인딩 키 생성/처리를 대신하도록 함으로써 HMIPv6와 구조상 통합이 가능하도록 하였다.

2.4.1 지역 이동성을 고려한 인증 절차 - MAP간 이동 발생시

MAP 도메인 경계를 벗어나 이동 노드가 다른 MAP 영역으로 이동한 경우 RCoA와 LCoA가 새롭게 구성되고 이전 'MAP+AAA' 엔티티에서 저장하고 있었던 위임 정보 및 보안 파라미터는 무효화 되므로 방문 링크

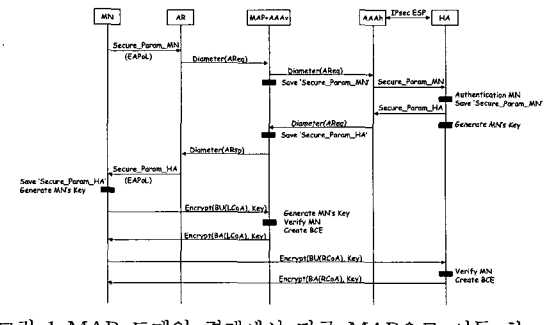

그림 1 MAP 도메인 경계에서 다른 MAP으로 이동 한 경우 인증 및 바인딩 처리 절차

와 홈 링크의 AAA 엔티티간의 전체 인증 과정이 수행되어야 하고, HMIPv6 동작에 의해 홈 에이전트와 상대 노드로의 RCoA 등록 및 'MAP+AAA'엔티티로의 LCoA 등록 절차가 수행된다.

단계별 처리 메시지 및 파라메터는 다음과 같다.

단계 1	Attendant 검색 (Attendant → 이동 노드): 멀티캐스트	
	쿠키(Cookie)	이동 노드와 Attendant간의 최소한의 링크 보호를 위한 값

단계 2	인증 요청(이동 노드 → Attendant): 유니캐스트(EAPoL)	
	<Secure_Param_MN 구성 및 전달>	
	NAI	이동노드의 홈 도메인 식별 값
	넌스 인덱스	인증 요청 메시지에 대한 재실행 공격 방지
	HoA	이동노드의 홈 주소
	CoA	이동노드의 현재 임대 주소
	SPI	이동노드와 홈 에이전트간에 미리 설정된 보안 협약에 대한 인덱스
	Authenticator	메시지 송신자 인증 및 무결성 검증을 위한 인증자 정보
	Delegation	위임 인증 요청 플래그

EAPoL 메시지를 수신하면 Attendant는 이 정보를 DIAMETER 메시지(AReq) 포맷으로 변환해서 방문 링크의 AAA 인증 서버로 전송한다.

단계 3	AAA 인증 요청(Attendant → MAP+AAAv): AReq(DIAMETER)	
	Security AVP	NAI 옵션, Nonce_Index 옵션, SPI 옵션, Signature 옵션
	Address AVP	홈 주소 옵션, CoA 옵션
	Action AVP	인증 위임(Delegation) 옵션

AReq 메시지를 수신하면 'MAP+AAA' 엔티티는 옵션에 포함된 Secure_Param_MN 정보를 임시적으로 안전한 로컬 저장소에 저장하고 NAI(Network Access Identifier) 옵션을 통해 얻은 이동 노드의 홈 도메인 AAA 서버로 AReq 메시지를 포워딩한다.

단계 4	DIAMETER 인증 메시지 포워딩(MAP+AAAv → AAAh): AReq(DIAMETER)	
	<수신된 Secure_Param_MN 정보를 로컬 저장소에 저장>	
	<수신된 NAI로부터 이동 노드의 홈 도메인 검색 후 메시지 전송>	
	Security AVP	NAI 옵션, Nonce_Index 옵션, SPI 옵션, Signature 옵션
	Address AVP	홈 주소 옵션, CoA 옵션
	Action AVP	인증 위임(Delegation) 옵션

홈 망의 AAA 서버가 이 메시지를 수신하면 이동 노드를 인증하고 바인딩 키를 얻기 위해 홈 에이전트로 메시지를 전송하는데 홈 에이전트와 홈 AAA 서버 간에는 사전에 설정된 IPsec ESP에 의해 보호된다.

단계 5	홈 에이전트로 인증 요청 정보 포워딩(AAAh → 홈 에이전트):
	<단계 4의 파라메터를 홈 에이전트 처리를 위한 메시지로 변환한 후 포워딩 함)

단계 6	이동노드 인증 및 응답(HA → AAAh)	
	<수신된 Secure_Param_MN을 저장>	
	<Secure_Param_HA 구성 및 전달>	
	넌스 인덱스	인증 응답 메시지에 대한 재실행 방지
	HA 주소	홈 에이전트의 주소
	SPI	홈 에이전트와 이동노드간에 사전에 구성한 보안 파라메터 인덱스
	인증자	메시지 송신자 인증 및 무결성 보장을 위한 인증자 정보
	처리 결과	인증 처리의 성공/실패여부 기술. 위임이 설정된 경우 위임 처리결과 포함

단계 7	인증 응답 정보 포워딩(AAAh → MAP+AAA): ARsp(DIAMETER)	
	<DIAMETER 응답 메시지 포맷으로 변환 한 후 응답 메시지 포워딩>	
	Security AVP	넌스 인덱스, 보안 파라메터 인덱스, 인증자,
	Address AVP	홈 에이전트 주소
	Action AVP	처리 결과

단계 8	인증 응답 메시지 처리 및 포워딩(MAP+AAAv → Attendant): ARsp(DIAMETER)
	<메시지 처리 결과 및 인증 설정 여부 확인>
	<인증 설정 시 Secure_Param_HA를 로컬 저장소에 저장>
	<단계 7에서와 동일한 AVP 정보를 Attendant로 전송>

ARsp 메시지는 Attendant에서 EAPoL(Extended Authentication Protocol over LAN) 메시지 형태로 변환해서 최종적으로 이동 노드로 전송된다. 이동 노드는 결과 메시지로부터 'Secure_Param_HA'를 얻게 되며 '인증 위임' 가능 여부를 확인하게 된다. 위임이 성공적으로 처리되면 'MAP+AAA' 엔티티는 지정된 바인딩 키의 라이프 타임 동안 이동 노드에 대한 인증을 대신 처리하게 된다.

2.4.2 지역 이동성을 고려한 인증 절차 - MAP 도메인 내에서의 이동 발생시

MAP 도메인 내에서 이동이 발생한 경우 위임 기능이 설정되어 있다면 인증 절차는 다음과 같이 간소화될 수 있다.

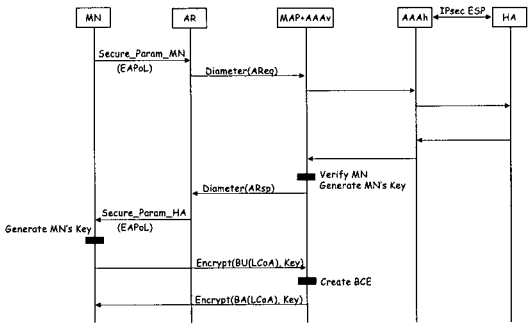

그림 2 지역 이동 발생 시 위임 기능을 통한 최적화된 인증 절차

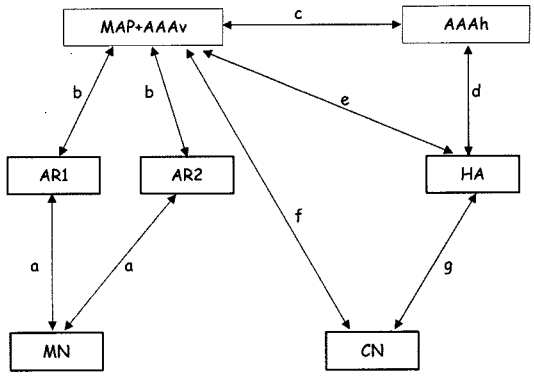

그림 3 바인딩 등록 및 인증 비용 분석 모델

이동 노드가 MAP 도메인 내부에서 이동하는 경우 다음과 같은 인증 및 바인딩 절차가 수행된다. 방문 링크 상에 존재하는 Attendant를 검색한 후 이동 노드는 인증 처리 요청을 위한 EAPoL 메시지를 전송하며 이 경우 2.6.1절에 기술된 것과 동일한 파라미터를 가진다. 이때 '위임' 기능을 사용하기 위해 플래그 값을 설정할 수 있다. Attendant는 수신된 메시지를 DIAMETER로 변환한 후 'MAP+AAA'로 전달한다. 만일 메시지에 '위임' 옵션이 설정된 경우 이동 노드에 대한 기존의 바인딩 정보를 검색하고, 이전의 인증 절차에서 미리 저장해 둔 Secure_Param_HA 내용을 DIAMETER 메시지로 전송한다. 이동 노드는 수신된 Secure_Param_HA를 사용해서 바인딩 키를 생성하고 MAP으로 로컬 바인딩 수행한다. 만일 보안 정책에 의해 또는 주기적인 키 갱신을 위해 이동 노드가 위임 기능을 설정하지 않고 인증 요청을 시작하면 'MAP+AAA'엔티티는 2.4.1절에 기술한 흐름을 따라 인증을 처리한다.

3. 성능평가

3.1 비용 분석 모델

성능평가 기준은 HMIPv6 환경 하에서 제안된 'MAP+AAA'엔티티를 경유한 인증 및 홈 등록 과정에 대한 비용 산출을 기반으로 하며, 이때 노드간의 거리와 각 노드에서의 처리 시간 및 처리 지연으로 인해 발생하는 시간 동안 지연 또는 분실되는 데 CN은 λ 비율로 MN에게 패킷을 전송하고 MN은 μ 비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정한다. 본 논문에서는 패킷을 각각 제어 패킷과 데이터 패킷으로 구분하는데 제어 패킷의 평균 길이를 l_c라하고, 데이터 패킷의 평균 길이를 l_d라고 정의하며, 비율은 $l=l_d/l_c$라고 정의한다. 즉, 제어 패킷을 전송하는 비용은 송신자와 수신자의 거리에 의해 주어지며 데이터 패킷의 전송 비용은 제어 패킷에 비해 평균 l배 크다고 가정한다. 그리고 한 호스트에서 제어 패킷을 처리하는 비용은 r이라고 가정한다.

이동 노드가 새로운 서브넷으로 이동 했을 때 먼저 해당 서브넷에 존재하는 Attendant에 접속을 하고 CoA를 구성한 후 자신의 홈 에이전트로 바인딩 등록을 해야 한다[6]. HMIPv6에서는 빈번한 로컬 이동 특성을 가지는 이동 노드에 대해서 로컬 도메인 내에서 바인딩을 등록함으로써 홈 에이전트로의 바인딩 횟수 및 지연시간을 줄일 수 있도록 하는 구조를 제시하고 있다. 그러나 바인딩 등록을 위해서 반드시 노드 및 방문 망에 대한 상호 인증이 선행되어야 한다[3]. 'MAP+AAA'엔티티는 이러한 목적을 위해 기존의 MAP 엔티티에 AAA 인증 엔티티를 추가한 것으로서, 이동 발생 시 노드는 Attendant(AP 또는 Access Router)에 대한 Layer2 접속을 완료하고 HMIPv6에서 정의한 방식에 따라 방문 도메인의 MAP 엔티티를 검색한다. 이동 상황에 따라 크게 두 가지 관점으로 살펴볼 수 있는데, 새로운 방문 도메인으로 이동한 경우와 현재 방문 도메인 내에서 다른 서브넷으로 이동한 경우로 구분할 수 있다. 새로운 방문 도메인으로 이동한 경우 이동 노드의 서비스 지연에 따른 비용은 MAP 검색 비용, LCoA에 대한 로컬 바인딩 비용, RCoA 등록을 위한 홈 바인딩 및 노드와 방문 링크의 상호 인증 비용의 합으로 구해질 수 있다. 로컬 도메인에서 이동한 경우는 MAP 검색 비용, LCoA 등록비용 및 인증 위임을 통한 로컬 인증 비용의 합으로 구해진다. 본 논문에서는 이동 노드의 보행 및 차량 이동 속도를 가지는 이동 특성 및 PMR 값에 따른 패킷 손실 및 서비스 지연 비용을 산출하고 기존의 인증 구조에 대한 비용 효율을 제시한다. 그림 4에 나타낸 바와 같이 하나의 MAP 도메인 영역은 'MAP+AAA'정보를 광고하는 엑세스 라우터(AR)의 개수에 의해 결정된다. AR의 수가 많으면 MAP 도메인 영역은 넓어지지만 각 AR이 담당하는 서브넷에 존재하는 이동 노드의 개

수도 증가하며 MAP에서 각 이동 노드에 대해 LCoA와 RCoA의 바인딩 정보 관리를 위한 테이블의 양 및 처리 시간이 증가하고 홈 에이전트나 상대 노드로부터 수신되는 트래픽을 터널링해서 이동 노드로 전송해 주는 데이터 처리 비용이 증가하게 된다. 다음은 'MAP+AAA' 엔티티가 관리하는 MAP 도메인을 보여 준다.

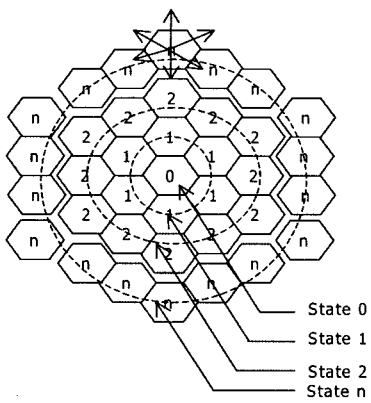

그림 4 MAP 도메인 영역 및 상태 정의

여기서 State 0은 MAP 도메인의 가장 안쪽에 존재하는 AR(Access Router)을 의미하며 외부로 나갈수록 상태가 증가하게 된다. 만일 MAP 도메인의 크기를 n으로 설정하였다면 State n은 MAP 간의 경계 부분에 존재하는 AR들의 집합으로 나타낼 수 있다. 여기서 이동 노드의 초기 상태와는 무관하게 임의의 랜덤 타임 후 이동 노드가 특정 상태에 존재하게 되는 확률을 다음과 같이 나타낼 수 있다[5,6].

$$\pi^{(n)} = \pi^{(n-1)}P = \pi^{(0)}P^n,\ n = 1,2,.... \quad (1)$$

본 논문에서 적용하는 Random-Walk 모델에 의해 각 상태를 마코프 체인으로 표시하면 다음과 같다. 여기서 $\pi_i^{(n)}$은 타임 n 후에 이동 노드가 상태 i에서 발견될 확률 값 즉, 한 상태에서 머물게 되는 long-term Steady-State 확률로서 $\sum_i \pi_i = 1$이 된다[5,6].

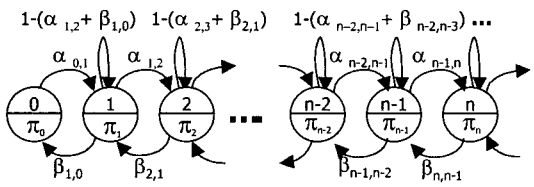

그림 5 Random-Walk 이동 모델에 대한 상태 천이도

Steady-State 확률은 다음 수식을 통해 구할 수 있다. 천이 행렬 P가 주어졌을 때 I를 항등 행렬로 정의하고 $Q=P-I$로 정의한다. 이때 e는 모두 1 크기를 가지는 n-벡터이고 b는 (n+1)위치에 1 크기를 가지고 나머지 위치는 모두 0인 단위벡터이다[10].

$$(Q|e)^T\pi = b \quad (2)$$

$\alpha_{r,r+1}$은 State 0와 가까운 임의의 AR에서 MAP 도메인 외부로 향하는 상태에 대한 천이 확률을 의미하며 $\beta_{r,r-1}$은 MAP도메인의 경계부분과 가까운 AR에서 MAP 도메인 내부로 이동하는 상태에 대한 천이 확률을 의미한다. 각 상태별로 천이 확률을 확률 매트릭스 P로 표시하면 다음과 같다.

$$P=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & . & 0 & 0 & 0 \\ 1/6 & 1/3 & 1/2 & 0 & 0 & . & 0 & 0 & 0 \\ 0 & 1/4 & 1/3 & 5/12 & 0 & . & 0 & 0 & 0 \\ 0 & 0 & 5/18 & 1/3 & 7/18 & . & 0 & 0 & 0 \\ 0 & 0 & 0 & 7/24 & 1/3 & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & . & 1/3 & \frac{(n-1)/3-1/6}{n-2} & 0 \\ 0 & 0 & 0 & 0 & 0 & . & \frac{(n-2)/3+1/6}{n-1} & 1/3 & \frac{(n)/3-1/6}{n-1} \\ 0 & 0 & 0 & 0 & 0 & . & 0 & \frac{(n-1)/3+1/6}{n} & 1/3 \end{bmatrix}$$

그림 6 상태 천이 확률 매트릭스

여기서 이동 노드의 이동 발생 확률을 q 라고 가정하고 천이 행렬을 일반화했을 때 천이 확률 α와 β는 다음과 같이 나타낼 수 있다.

$$\alpha_{i,i+1} = \begin{cases} \sigma & \text{if } i = 0 \\ \sigma\left(\dfrac{(i+1)/3-1/6}{i}\right) & \text{if } 1 \le i \le n \end{cases} \quad (3)$$

$$\beta_{i,i-1} = \sigma\left(\frac{(i-1)/3+1/6}{i}\right) \quad \text{if } 1 \le i \le n \quad (4)$$

또한 다음과 같은 관계가 성립한다.

$$\alpha_{i,i+1} + \beta_{i,i-1} = \frac{2}{3}, 1 \le i \le n \quad (5)$$

3.2 HMIPv6 상에서 이동 노드의 인증 및 바인딩 비용 분석

이 절에서는 HMIPv6상에서 기존인증 적용방식과 본 연구에서 제안된 방식을 평가하기 위한 비용 분석을 제시한다. 전체 비용은 식 (6)에 의해서 C_{All}로 정의하며, 인증비용(C_{AUTH})과 HMIPv6 구조상에서의 LCoA 및 RCoA 등록 비용 및 상대 노드가 보내는 패킷 처리 비용(C_{HMIP})의 합으로 다음과 같이 정의할 수 있다.

$$C_{All} = C_{AUTH} + C_{HMIP} \quad (6)$$

이동이 발생하면 인증 과정이 수행 되어야 하며, 분석을 위해 C_{AUTH}를 방문 도메인과 홈 도메인간의 DIAMETER 메시지 교환을 통한 인증 비용인 $C_{AUTH\text{-}g}$와 방문 도메인 내에서의 인증 처리 비용인 $C_{AUTH\text{-}l}$로 나눈다. 기존의 인증 방식에서는 방문 링크의 AAA 서버와 홈 링크의 AAA 서버간의 메시지 교환을 통한 인증 과정($C_{diameter(visit,\ home)}$)이 수행된다. 제안하는 인증 위임 방식에서는 방문 도메인 내의 AAA 서버를 통한

인증 과정($C_{diameter(visit)}$)이 수행된다. 또한, 기존의 방법에서는 이동 방향에 상관없이 매번 이동 발생 시마다 C_{AUTH-g}를 수행한다. 식 (7)에서 T는 이동 노드가 한 서브넷에 존재하는 시간, $E(T)$는 이동 노드가 서브넷에 머문 평균 시간, σ는 이동 노드의 이동 발생 확률, π_i는 이동 노드가 상태 i에 존재할 확률로 정의했을 때, 단위 시간 당 발생하는 인증 비용은 다음과 같다. 이때 이동 노드에 대한 인증 및 키 재료 분배는 성공적으로 완료된다고 가정한다.

$$C_{AUTH-g} = \frac{\pi_i \cdot \sigma \cdot C_{diameter(visit,home)}}{E(T)}, 1 \le i \le n \quad (7)$$

본 논문에서 제안하는 인증 위임 기능을 사용하는 경우 인증 과정은 방문 도메인 내의 MAP+AAA 엔티티에 의해 처리되며 이때 비용은 다음과 같다.

$$C_{AUTH-l} = \frac{\pi_i \cdot \sigma \cdot C_{diameter(visit)}}{E(T)}, 1 \le i \le n \quad (8)$$

위임 기능을 사용하는 경우 이동 노드가 처음 새로운 MAP 도메인으로 이동했을 때, 위임 설정을 위한 정보 교환이 완료되기 위해 처음 한 번은 홈 링크와 방문 링크의 AAA간에 메시지 교환을 거쳐야 하고 그 후에 MAP 도메인 안에서 이동할 때에는 인증 위임 기능을 통해 방문 링크의 AAA 서버에 의해서 이동 노드 인증 및 키 재료 분배가 이뤄지게 된다. 따라서 C_{AUTH}를 정리하면 다음 수식과 같다.

$$C_{AUTH} = \frac{\pi_n \cdot \alpha_{n,n+1} \cdot C_{diameter(visit,home)} + {}_n \cdot (1-\alpha_{n,n+1}) \cdot C_{diameter(visit)}}{E(T)} \quad (9)$$

여기서 $C_{diameter(visit,home)}$은 MAP 경계에서 다른 MAP 도메인으로 이동한 경우 발생하는 인증 절차로서 여기에는 방문 도메인과 홈 도메인에 존재하는 AAA 엔티티간의 메시지 교환이 발생한다. 각 엔티티에서의 메시지 처리 비용은 r로 정의하며 방문 링크와 홈 링크에 존재하는 AAA 서버 간에는 일정한 전송지연 값인 T_c를 가진다고 가정할 때 인증 비용은 다음 수식과 같다.

$$C_{diameter(visit,home)} = 2\psi(\log(N(AR)) + T_c) + 9r, where\ \psi\ is\ the\ weight\ factor \quad (10)$$

$C_{diameter(visit)}$는 MAP 안에서 이동이 발생한 경우에 대한 인증 절차로서 인증 위임 기능에 의해 MAP+AAA 엔티티에서 이동 노드에 대한 인증을 처리하며 인증 요청을 수신하면 인증 위임 리스트에서 MN을 검색한 후 SecureParam_HA를 이동 노드로 전송하므로 위임이 설정된 경우 인증 비용은 다음 수식과 같다.

$$C_{diameter(visit)} = \omega N(MN) + 2\psi\log(N(AR)) + 5r, where\ \omega\ and\ \psi\ are\ weight\ factors \quad (11)$$

여기서 $N(MN)$은 MAP 도메인 내에 존재하는 MN의 개수로서 각 AR 영역 내에 존재하는 이동 노드(방문 도메인에 속하는 이동 노드는 제외)의 평균 개수를 X라고 가정할 때 $N(MN)=N(AR)\times X$로 얻을 수 있다. 본 논문에서는 이동 노드와 AR간의 전송 비용은 고려하지 않는데 이는 매우 작은 상수 값을 가지기 때문이다($\simeq 0$).

C_{HMIP}는 MAP 등록(C_{BU-CoA}) 및 패킷 전송 비용(C_{packet})으로 구성되며 등록 시 MAP 도메인 경계 AR에서 외부로 향하는 경우 RCoA를 홈 에이전트에 등록해야 하고, MAP 내부에서 이동시 MAP에만 LCoA를 갱신하면 된다. 따라서 MAP 등록비용은 다음 수식과 같다.

$$C_{BU-CoA} = \frac{\pi_n \cdot \alpha_{n,n+1} \cdot C_{RCoA} + \pi_n \cdot (1-\alpha_{n,n+1}) \cdot C_{LCoA}}{E(T)} \quad (12)$$

인증이 완료되고 RCoA가 홈 에이전트 및 상대 노드로 등록되기 전까지 상대 노드가 보내는 패킷은 홈 에이전트를 통해 터널링 되어 MAP으로 전달되고 MAP을 통해 이동 노드로 전달되고 경로 최적화가 완료되면 상대 노드에서 홈 에이전트를 거치지 않고 직접 전송하게 된다. 따라서 패킷 전송 비용은 다음과 같다.

$$C_{packet} = C_{CN} + C_{MAP} \quad (13)$$

상대 노드로부터 이동 노드로의 거리는 홉 수로 계산되며 상대 노드와 이동 노드 간에 진행 중인 세션을 통해 발생하는 트래픽을 λ로 정의할 때 C_{CN}은 다음과 같다.

$$C_{CN} = \lambda_d \cdot t_{MAP} \cdot l_d((g+e)+3r) \quad (14)$$

λ_d는 이동 노드가 상대 노드로부터 수신하는 데이터 패킷의 수신율로서 이는 트래픽의 특성에 따라 달라진다. t_{AUTH}와 t_{MAP}은 각각 인증 및 MAP 등록을 완료하는데 걸리는 시간이며 l_d는 데이터 패킷의 평균 길이를 나타낸다. MAP에서 패킷을 수신하면 RCoA와 LCoA의 바인딩 테이블을 검색하고 해당 AR을 찾아서 패킷을 라우팅 하므로 C_{MAP}은 다음 식과 같다.

$$C_{MAP} = \lambda_d \cdot (\psi N(MN) + l_d \cdot \omega\log(N(AR))), where\ \psi\ and\ \omega\ are\ weight\ factors \quad (15)$$

3.3 결과 분석

이 절에서는 결과 분석을 위해 제안된 모델 및 산출된 수식을 기반으로 이동 노드의 이동 특성(보행, 차량), 상대 노드와의 트래픽 특성, MAP 도메인의 크기, MAP 도메인에 존재하는 방문 이동 노드의 개수에 대한 인증 비용 변화를 분석한다. 분석을 위해 상수 및 시스템 파라미터를 다음과 같이 정의한다.

표 1 시스템 파라미터

X	ψ	ω	T_c	r	C_{RCoA}	C_{LCoA}	t_{MAP}	t_{AUTH}	l_d
12	0.1	0.001	80	0.00083	100	20	2	2	0.1
a	b	c	d	e	f	g			
2	2	6	2	6	6	6			

결과 분석을 위해 한 AR 영역 내에 존재하는 이동 노드의 평균 개수를 12로 가정하며, 도메인과 도메인 간의 트래픽 지연은 80의 고정된 값으로 정의한다. 이때 a,b,c,d,e,f,g는 각각 링크 가중치로서 도메인 내부 엔티티간 링크에 대해서는 2값을 외부 엔티티와의 링크에 대해서는 6을 가정한다. l_d는 데이터 트래픽의 평균 길이로서 수신되는 하나의 데이터 패킷의 길이를 의미한다. Ψ와 ω는 각각 무선 및 유선 구간에 대한 처리 지연 값으로서 이동 노드의 무선 접속 능력은 1Mbps로 가정하고 도메인 내부의 유선 구간은 100Mbps를 가진다고 가정한다. C_{RCoA}, C_{LCoA}, t_{MAP}와 t_{AUTH}은 각각 100, 20, 2, 2로 정의하며[4], r은 수신 패킷에 대한 각 프로토콜 계층별 처리 시간의 합을 의미한다[11]. 또한 MAP 도메인의 크기를 4(n=4)로 가정하면 이때 상태 천이 행렬 P는 수식 (3), (4)에 의해 다음과 같이 계산되며, long-term Steady-State 확률 값인 π는 수식(2)에 의해 아래와 같이 얻을 수 있다.

$$P=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{3} & \frac{5}{12} & 0 \\ 0 & 0 & \frac{5}{18} & \frac{1}{3} & \frac{7}{18} \\ 0 & 0 & 0 & \frac{7}{24} & \frac{1}{3} \end{bmatrix}, \quad \pi=\begin{bmatrix} 0.0521571900 \\ 0.2123392733 \\ 0.2937039845 \\ 0.2729282637 \\ 0.1688969723 \end{bmatrix}$$

그림 7 MAP 도메인 크기가 4인 경우(n=4) 상태 천이 확률 및 Steady-State 확률

여기서 수식(5)에 의해 현재 MAP 도메인을 벗어나 다른 MAP으로 천이확률($\alpha_{4,5}$)은 $\frac{3}{8}$이 된다.

3.4 인증 방식 비용의 효율성 비교

기존에 제안된 인증 방식으로는 Dupont과 Perkins의 제안 방식이 있다[8,9]. Perkins 방식은 인증 메시지 처리 시 바인딩 갱신을 동시에 처리하도록 내장옵션을 사용함으로써 메시지 교환의 횟수를 줄인 방법이며 Dupont 방식의 경우 인증 및 바인딩 처리를 별도의 메시지로 처리하게 한 방식이다. 그러므로 Dupont 방식이 Perkins 방식에 비해 처리되어야 할 메시지 교환 횟수가 더 많지만, Perkins 방식에서 드러난 보안 허점이 존재한다. 이는 아직 SA가 설정되기 전에 이동 노드의 바인딩 정보를 내장함으로써 보안 위협이 존재하기 때문이다. 따라서 본 논문에서 일반적인 인증 방식은 Dupont의 제안 방식으로서 이동 특성과 무관하게 총 12 단계에 걸친 메시지 교환을 통해 인증 및 바인딩 등록을 완료한다[8]. 이동 노드가 이동했을 때 Micro 이동성에 관계없이 무조건 홈 도메인과 방문 도메인의 AAA 엔티티 간 메시지 교환을 통한 노드 인증 절차를 실행하므로 수식 (9)는 다음과 같이 변경될 수 있다.

$$C_{AUTH}=\frac{\pi_n \cdot \alpha_{n,n+1} \cdot C_{diameter(visit,\,home)}+\pi_n \cdot (1-\alpha_{n,n+1}) \cdot C_{diameter(visit,\,home)}}{E(T)} \quad (16)$$

즉, MAP 도메인 외부로 이동하는 경우와 내부에서 이동하는 경우 모두에 대해 $C_{diameter(visit,\,home)}$ 인증 비용이 적용된다. 이 절에서는 이동 노드의 이동 특성과 트래픽 특성에 따른 제안 방식과 일반 방식간의 비용 효율성을 비교하며, MAP 도메인의 크기 변화에 따른 인증 비용을 비교한다.

3.4.1 이동 성질에 대한 효율성 비교

전체적인 인증 비용 비교를 위해 고려되어야 할 사항으로는 이동 노드 이동 특성 및 MAP 도메인의 크기가 있다. 이동 특성은 노드의 이동 특성 및 이동 확률로 표시되며 MAP 도메인의 크기는 도메인에 존재하는 평균 이동 노드의 개수로 정의할 수 있다. 본 논문에서는 MAP 도메인의 크기는 4로 정의하였고 이동 노드는 보행 이동 속도로 움직인다고 가정하였다. 그림 8은 제안된 방식과 기존 방식간의 인증 비용을 보여 준다.

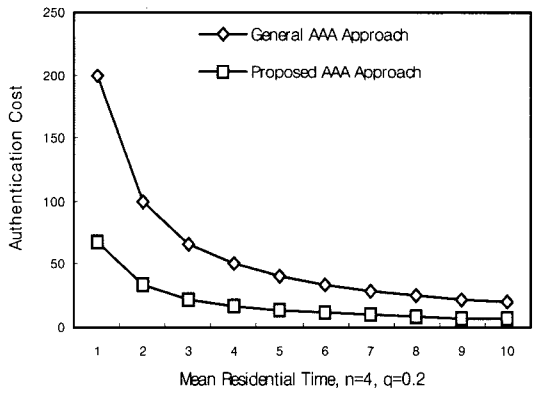

그림 8 기존 인증 방식과 제안 인증 방식의 비용 비교

한 서브넷에 머무는 시간이 길수록 이동 발생이 적어지므로 인증 비용이 감소한다. 이는 일반적인 인증 방식과 제안 방식 모두 적용되는 비용 변화 특성이지만, 일반 방식의 경우 도메인 내에서의 이동에 관한 비용 최적화 고려가 없으므로 도메인 내부 이동시에도 도메인 외부로의 이동 인증 비용이 적용된다. 일반적인 인증 방식을 적용한 경우 MAP 도메인 내부에서 이동한 경우에도 $C_{diameter(visit,\,home)}$ 인증 비용이 적용 되므로 인증 및 바인딩 등록을 위한 시그널링 비용이 크며 이는 이동 노드의 이동이 빈번하게 발생하는 경우 급격히 증가하게 된다. 반면, 제안된 인증 방식의 경우, MAP 도메인 내부에서 이동하는 경우 $C_{diameter(visit)}$ 인증 비용이 적용되

므로 도메인 외부와 교환되는 시그널링 메시지 양이 크게 줄어듦으로 인증 비용이 적다. 따라서 이동 횟수가 많을수록 제안 방식과 일반 방식간의 인증 비용 차는 급격히 증가한다.

3.4.2 트래픽 성질에 따른 효율성 비교

이동 노드가 상대 노드와 세션을 유지한 채 이동하는 경우 인증이 완료되기 까지 세션을 통해 수신되는 트래픽은 지연 또는 폐기된다. 그림 9는 상대 노드로부터 이동 노드로 수신되는 패킷의 도착율에 따른 패킷 분실 비용의 변화량을 나타낸 것이다.

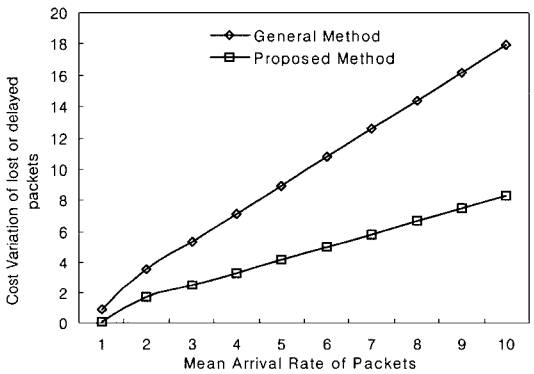

그림 9 수신 트래픽 양에 따른 패킷 분실 비용 비교

수신 트래픽이 적은 경우 분실 패킷 비용은 일반적인 경우와 제안 경우에 있어서 큰 차이를 보이지 않으나 트래픽이 증가할수록 분실 패킷 비용이 급격히 증가한다. 이는 동일한 수신 조건을 가정할 때 일반적인 방식의 경우 보다 많은 인증 지연이 발생하므로 이 기간 동안 수신되는 트래픽은 분실 또는 지연된다. 따라서 제안 방식이 동일한 이동 특성 및 도메인 조건을 가정할 때 트래픽 양이 많은 경우 더 나은 성능을 제공한다.

4. 결 론

HMIPv6는 계층적인 이동성 관리 구조를 제공함으로써 이동 노드가 일정한 경계 내에서 이동할 경우 방문 도메인에 존재하는 MAP 엔티티를 통해 이동성을 제공받을 수 있도록 하는 구조로서 이는 실시간 응용 적용 시 서비스 지연 및 빈번한 이동으로 인해 발생하는 시그널링 오버헤드를 최소화하는 데 적합하다. 그러나 대부분의 이동 서비스에서 이동성 제공을 위해 반드시 이동 노드와 방문 링크 상호간에 인증 절차를 실행해야 하는데 이는 [3]에 기술된 보안 위협으로부터 안전을 확보하기 위해 필수적인 것이다. 현재 무선 랜과 셀룰러 망에서 AAA 기반의 인증 방식의 도입이 이루어지고 있다.

AAA는 인증, 권한 제어 및 과금 서비스를 제공하는 신뢰성과 확장성 기반의 전용 서비스로서 대표적인 프로토콜인 RADIUS와 DIAMETER가 사용된다. 본 논문에서는 보다 안전하고 확장성을 제공하며 메시지 교환 횟수가 적인 DIAMETER를 기반으로 한다.

이동 발생 후 서비스 재개를 위한 전체 과정은 이동 노드와 방문 링크 상호 인증, 바인딩 키 생성 및 바인딩 등록 부분으로 구성된다. 즉 신속한 서비스 재개를 위해서는 이들 과정에 대한 지연을 최소화해야한다. 바인딩 등록 부분은 HMIPv6 구조상에서 지역 이동성 제공을 통해 서비스 지연을 최소화 할 수 있으나, AAA 서비스 인프라는 지역 이동성을 고려하지 않고 메시지 교환이 발생하므로 이는 심각한 지연 요인이 될 수 있고 전체적인 서비스 재개에 영향을 주게 된다.

본 논문에서는 HMIPv6와 동일한 구조를 갖으며, 지역 이동성을 고려한 인증 서비스가 가능하도록 MAP+AAA 엔티티를 도입하고 위임 기능을 정의함으로써, 지역에서 이동 발생 시 해당 도메인에 존재하는 AAA 엔티티가 인증 및 바인딩 키 재료 분배를 가능하도록 하였다.

제안된 방법은 이동 노드의 성질 등에 따른 비용 분석 및 기존 방식과의 비용 분석을 통해 이동 발생 확률이 높은 경우 기존 방식에 비해 비용이 절감됨을 알 수 있고, 트래픽 양이 많은 경우 패킷 손실 및 지연 비용이 낮아짐을 알 수 있으며, 일반적인 인증 방식과 비교한 결과 평균 33.6%의 비용 절감 효과를 얻을 수 있었다.

본 연구에서 제안된 방법은 향후 이동 실시간 응용을 요구하는 QoS(Quality of Service) 보장형 서비스에 적합한 인증 구조로서 무선 랜과 셀룰러 망에 도입 시 서비스 제공 및 보안성 향상에 기여할 것이다.

참 고 문 헌

[1] H. Soliman, C. Castelluccia, "Hierarchical Mobile IPv6 mobility management(HMIPv6)," IETF Internet Draft, Mobile IP Working Group, Jun. 2003.

[2] Pat. R. Calhoun, Erik Guttman, Jari Arkko, "DIAMETER Base Protocol," draft-ietf-aaa-diameter-12.txt, Internet Draft, IETF, July. 2002.

[3] A. Mankin, B.Patil, D. Harkins, E. Nordmark, P. Nikander, P. Roberts, T. Narten, "Threat Model introduced by Mobile IPv6," draft-ietf-mobileip-ipv6-scrty-reqts-02.txt, Internet Draft, IETF, May. 2001.

[4] S. Pack, Y. Choi, "Performance Analysis of Hierarchical Mobile IPv6 in IP-based Cellular Networks," IEEE PIMRC '2003, Beijing, Sep. 7-10, 2003.

[5] L. Kleinrock, "Queueing Systems, Volume 1: Theory," ISBN-0471491101, John Wiley & Sons, Jan. 1975.

[6] K. Chiang, N. Shenoy, "A Random Walk Mobility Model for Location Management in Wireless

Network," IEEE PIMRC '2001, San Diego, Sep. 30 - Oct. 3, 2001.
[7] M. Kim, Y. Mun, J. Nah, S. Sohn, "Localized Key Management for AAA in Mobile IPv6," IETF Internet Draft, Mobile IP Working Group, Oct. 2002.
[8] F. Dupont, J.Bournelle, "AAA for Mobile IPv6," draft-dupont-mipv6-aaa-01.txt, Internet Draft, IETF, Nov. 2001.
[9] F, Le, B. Patile, Charles E. Perkins,"Diameter Mobile IPv6 Application," draft-le-aaa-diameter-mobileipv6=01.txt, Internet Draft, IETF, Nov. 2001.
[10] www.mapleapps.com, "Computing the Steady-State Vector of Markov Chain," Waterloo Maple, 2001.
[11] A.Hess, G.Schafer, "Performance Evaluation of AAA / Mobile IP Authentication," Proc. of 2nd Polish-German Teletfaffic Symposium(PGTS'02), Gdansk, Poland, Sept. 2002.

김 미 영

1992년 전주우석대학교 전산학과 졸업(학사). 1995년 광운대학교 대학원 전산학과 졸업(석사). 1995년~1997년 (주)필컴 시스템 개발부 근무. 2000년~2005년 숭실대학교 대학원 컴퓨터학과 졸업(박사). 2005년 2월~현재 숭실대학교 정보미디어 연구소 전임연구원. 관심분야는 Mobile IP, AAA, Network Security

문 영 성

정보과학회논문지 : 정보통신
제 32 권 제 1 호 참조