Mobile IPv6에서 AAA를 이용한 MN과 CN간의 상호 인증 및 경로 최적화

(Mutual Authentication and Route Optimization between MN and CN using AAA in Mobile IPv6)

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

요 약 IETF의 mobileip 작업 그룹에서는 경로 최적화를 위해 절차가 간단하고 이동 노드의 낮은 연산 처리 능력을 고려해 암호학적 연산을 대폭 줄인 보안 기능으로서 RR(Return Routability)를 제공하지만 실질적으로 제공하는 보안 강도는 매우 낮으므로 이를 개선하기 위해 현재 CGA(Cryptographically Generated Address), IPsec(Internet Protocol Security)등의 암호학적 처리 방법과 PKI(Public Key Infrastructure), AAA(Authentication, Authorization and Account)등의 기존 인프라와 통합하는 강력한 보안 서비스 방법이 연구되고 있다. 본 논문에서는 유선망 및 802.11, 3GPP(3rd Generation Partnership Project)등의 무선망에서 성공적으로 사용되고 있는 AAA 인프라 기반의 노드 인증 및 안전한 경로 최적화를 위한 키 분배 방안을 제안하고 제안된 방법에 대한 비용 분석 모델을 통해 RR과 효율성을 비교하였는데 결과적으로 최대 20 퍼센트의 성능 향상을 보였다.

키워드 : Mobile IPv6, AAA, Authentication

Abstract The mobileip working group is equipped with the RR(Return Routabilit) taking the simple procedures and small amount of cryptographic operations by considering the processing capability of the mobile node however it dose not provide security features enough. To replace with enhanced methods, mobileip WG is making an effort to find the approved solutions include CGA(Craptographically Generated Address), IPsec(Internet Protocol Security) as well as the existing infrastructure such as AAA(Authentication, Authorization and Account) and PKI(Public Key Infrastructure). In this paper, we propose the authentication and route optimization based on AAA suitable for the requested security service for its successful story in wireless network such as 802.11 and 3GPP(3rd Generation Partnership Project) as well as wired one. We analyze the effectiveness of our scheme according to the traffic and mobility properties. The result shows the cost reduction up to 20 percent comparing with RR.

Key words : Mobile IPv6, AAA, Authentication

1. 서 론

본 논문은 이동 노드가 외부 망에 진입하고 홈 등록을 완료한 후 상대 노드와의 경로 최적화 과정을 수행하기 위한 인증 및 키 분배에 관해 기술한다. 실시간 멀티미디어 전송과 같은 대량 트래픽 전송 세션을 가지는 경우 삼각 라우팅으로 인해 발생하는 라우팅 지연을 줄이기 위해 이동 노드와 상대 노드간에 직접 라우팅을 가능하게 하는 경로 최적화가 수행되어야 한다. 그러나 경로 최적화 패킷은 공격자에 의해 유출되거나 악용됨으로써 이동 노드의 모든 패킷을 공격자가 가로챌 수 있으므로 DoS(Denial of Service), DDoS(Distributed DoS), MITM(Man In The Middle) 등의 공격이 감행될 수 있다. 따라서 경로 최적화시 반드시 보안 기능이 제공되어야 한다. mobileip 작업 그룹에서 정의한 경로 최적화를 위한 인증 및 키 분배 방식으로는 RR(Return Routability)이 있다. RR은 연산 및 메시지 오버헤드를 줄이는 관점에 주안점을 둔 것으로서 비교적 간단한 방식을 취하지만 제공하는 보안강도는 매우 낮다. 이에 작

· 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음
† 비 회 원 : 숭실대학교 컴퓨터학부
mizero31@sunny.soongsil.ac.kr
†† 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@computing.ssu.ac.kr
논문접수 : 2003년 11월 6일
심사완료 : 2004년 5월 7일

업 그룹에는 암호학적 처리에 기반을 둔 CGA 방식이나 IPsec 또는 PKI, AAA등의 기존 보안 인프라를 활용해서 보안 강도를 높이기 위한 다른 대안을 모색 중이며, 다각적인 접근 방법을 통한 실험 결과가 보고되고 있다. AAA 인프라 구조를 활용한 인증 및 키 분배를 제공하기 위해서 이동 노드(MN), 홈 에이전트(HA) 등의 Mobile IP 관련 엔티티 이외에 Attendant, 방문 도메인의 AAA 서버, 홈 도메인의 AAA 서버 등의 엔티티가 사용된다. RR의 기본 동작은 홈 에이전트를 경유한 터널링 경로를 통해 바인딩 키의 절반을 수신하고 상대 노드(CN)와의 직접 경로를 통해 나머지를 수신하는 구조를 갖는다. 이때 상호 인증 과정 및 바인딩 키의 분배 경로에 위치하는 공격자에 대한 보안 기능이 취약하므로 이동 노드로 위장한 공격자에 의해 세션이 재지정되거나 트래픽이 악의적인 노드로 유출될 수 있다.

본 논문에서는 AAA를 이용한 상대 노드 인증 및 경로 최적화 방안에 관해 기술하며, 트래픽 패턴 및 이동 특성에 따른 성능 분석을 제시하고 RR과의 효율성을 비교 분석하였다. 하나의 세션에 대해서 이동 노드가 상대 노드로부터 평균 패킷 길이 비율 단위로 패킷을 수신하고 평균 이동 비율로 이동하는 특성을 가질 때 이동시 수신하게 되는 패킷의 평균 개수를 정의하기 위해 각각 제어패킷과 데이타패킷의 비율을 구분하고 PMR (Packet to Mobile Ratio)을 도입하였다. 제안된 구조는 비용 분석을 통해 효율성을 검증하였는데 결론적으로 최대 20 퍼센트의 성능 향상을 보였다.

이 논문의 2장에서는 Mobile IPv6 상에서 경로 최적화 시 AAA 인프라를 사용한 인증 모델 및 엔티티를 정의한다. 3장에서는 제안하는 인증 구조 및 바인딩 절차를 기술하고 4장에서는 제안된 기법의 인증 비용을 분석하고 성능 평가 결과를 기술한다. 마지막으로 5장에서는 결론을 짓는다.

2. AAA 인증 모델 및 엔티티

그림 1은 AAA(Diameter) 인증 구조를 사용해서 이동 노드와 Attendant 간에 세션 키를 교환하고 이동 노드의 현재 위치 정보를 홈 에이전트로 등록하기 위한 AAA 기반의 통신 모델을 나타낸다[1,2].

CN 인증 및 경로 최적화를 위한 바인딩 등록 절차를 정상적으로 수행하기 위해서[3], 인증 과정은 이동성 제공을 위한 다른 절차들보다 우선되어야 하며, 바인딩 키의 생성 및 분배는 CN의 홈 AAA나 CN의 홈 AAA 서버와 로밍 협약을 채결한 방문 망의 외부 AAA 서버에 의해서 수행될 수 있다. AAA 인증 모델에서는 이동 노드(MN), 상대 노드(CN), 홈 에이전트(HA), Attendant, V_AAA 및 H_AAA 등 6개의 엔티티를 정의하

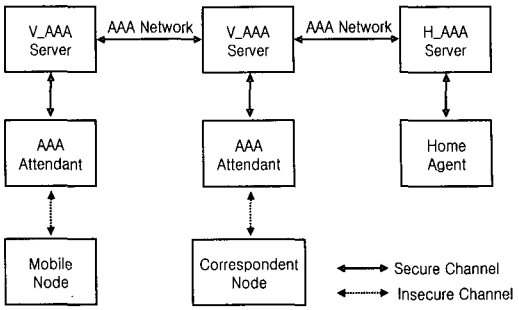

그림 1 AAA 인증 모델

고 있다. AAA 엔티티는 DIAMETER 고유의 인증 기능 및 키 분배 역할을 수행하며, 그 외의 엔티티는 이동 서비스를 위한 바인딩 등록 절차를 처리한다. 이동 노드와 홈 에이전트는 [3]에서 정의한 모든 기능을 만족한다. Attendant는 이동 노드가 외부 링크에서 가장 먼저 접속하게 되는 외부 AAA 클라이언트 엔티티로서 이동 노드가 전송하는 패킷에 대한 통과, 폐기, 보류 등의 정책을 수행할 수 있으며, AAA 서버를 통한 인증 성공시 AAA 서버로부터 이동 노드와 Attendant간의 세션을 암호화할 수 있는 세션 키를 얻을 수 있고 암호화 처리를 통해 패킷을 통과 시킬 수 있다. V_AAA는 외부 링크의 AAA(DIAMETER) 인증 서버로서 이동 노드가 외부 망으로 이동 하고 홈 등록을 마친 후 상대 노드와 진행 중인 세션을 유지하면서 경로 최적화를 수행하고자 하는 경우, 상대 노드의 주소를 통해 상대 노드의 홈 망을 식별하고 상대 노드와의 안전한 경로 최적화를 위해 상대 노드가 속한 홈 AAA로 인증 및 바인딩 키 요청 메시지를 전송한다. 이때 상대 노드는 홈 망에 고정된 노드이거나 또는 이동 노드일 수 있는데, 만일 상대 노드가 이동 노드로서 다른 망으로 이동한 경우라면 상대 노드의 홈 AAA 서버나 홈 에이전트를 통해 상대 노드의 현재 위치를 파악한 후 상대 노드가 방문한 외부 AAA 서버로 메시지를 전달한다. 이때 상대 노드의 외부 AAA 서버는 이동 노드의 AAA 서버 및 홈 AAA 서버와 이동성 로밍 계약을 채결하였다고 가정한다. H_AAA는 이동 노드나 상대 노드가 속한 홈 도메인의 AAA 인증 서버로서, H_AAA는 이동 노드의 인증에 필요한 인증 정보들로 구성된 프로 파일을 관리하고 있으며 라이프 타임이 만료될 때 까지 인증 및 키 생성, 분배 역할을 위임받을 수 있다. 이동 노드가 보내온 인증 정보(이동노드의 NAI[4], 노드 인증자(Authenticator, 이동 노드의 홈 주소, 상대 노드의 주소 등)를 기반으로 이동 노드에 대한 인증 처리 과정을 진행하고 결과를 V_AAA로 전송한다. 만일 홈 망이 재구성된 경우(Network Renumbering) 동적인 홈 에이전트 발견

절차를 수행할 수도 있다[3,5].

3. 경로 최적화를 위한 MIPv6 인증 구조

이동 노드가 경로 최적화를 수행하는 경우, 바인딩 메시지를 보호하기 위한 안전한 보안 방법이 제공되어야 한다. RR은 mobileip 작업 그룹에서 정의한 인증 및 바인딩 키 분배 방식으로 간단한 메시지 절차를 제공하지만, 제공하는 보안 강도는 매우 낮다. 따라서 RR의 HoTI(Home Test Init)/HoT(Home Test)나 CoTI (Care-of Test Init)/CoT(Care-of Test) 메시지 전달 경로 상에 위치하는 공격자에 의해 바인딩 키가 노출될 위험이 존재한다. 이 장에서는 AAA 인프라구조를 활용해서 안전하게 상호 인증 및 바인딩 키 분배를 수행하기 위한 절차를 기술한다.

3.1 배경

이동 노드가 홈 등록을 마친 후 상대 노드와의 세션 트래픽 특성을 고려해서 효과적인 라우팅을 통해 패킷 전달 지연을 줄일 수 있도록 경로 최적화를 수행할 수 있다. 특히 실시간 멀티미디어 세션의 경우 반드시 경로 최적화를 수행해야 한다. IETF의 mobileip 작업 그룹에서는 이동 노드의 암호 처리 연산 부하를 줄이고 보안을 제공하기 위해 RR을 사용하도록 권하고 있지만, RR의 낮은 보안 강도로 인해 연산 부하가 높아지더라도 보다 강력한 보안을 제공할 수 있는 대안이 모색 중이며, 이는 IPsec, CGA등의 방법이나, 기존의 보안 인프라인 AAA, PKI 등의 도입을 의미한다. RR을 통해 송수신되는 패킷은 암호학적인 연산이 없는 패킷이므로 해당 경로 상에 공격자가 위치한다면 쉽게 패킷의 내용을 알 수 있다[6]. 따라서 암호학적 연산을 추가하고 확장성 있고 안전하게 인증 및 키 분배를 수행하기 위한 인프라 구조와의 통합된 보안 방식이 제공되어야 한다.

3.2 관련 연구

3.2.1 무선랜 802.11에서의 인증 구조

무선 랜에서 802.1x를 사용하는 AAA 기반의 인증 구조를 나타내면 그림 2와 같다. 이동 노드가 외부망의 AP(Access Point)에 접속(Association)하게 되면 외부망 액세스를 위한 인증 과정을 수행하고 무선 구간의 사용 허가 및 세션 키를 얻어야 한다[7]. 만일 인증 과정이 실패하면 이동 노드는 외부 망의 액세스가 차단되거나 필터링 되므로 진행 중인 세션을 잃게 된다. 그림 2는 802.1x 상에서 이동 노드 인증 과정을 보여 준다. 먼저 이동 노드는 802.11 프로토콜을 통해 AP 검색, 채널 할당 및 BSS(Basic Service Set) 접속을 수행한 후 인증 및 무선 구간의 세션 키를 할당 받기 위해 802.1x 인증 절차를 시작한다. 이때 세션 키가 할당되기 전의 무선 구간은 EAPoL(EAP over LAN) 프로토콜을 사용

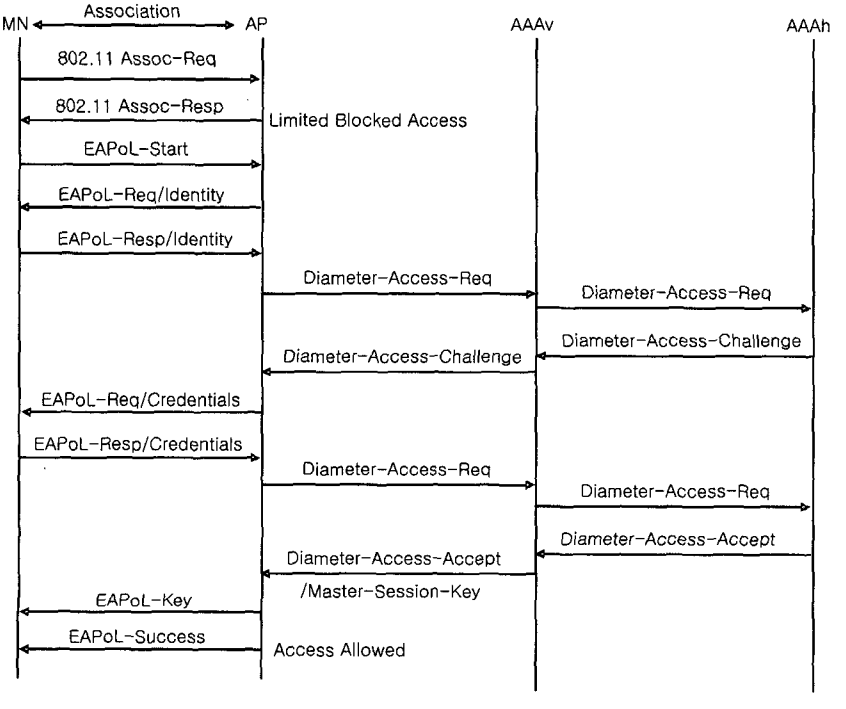

그림 2 무선 랜에서 802.1x를 통한 인증 과정[7]

해서 기본적인 보안을 제공한다. EAPoL에 캡슐화된 인증 정보는 RADIUS나 DIAMETER 메시지로 변환된 후 방문 도메인 및 홈 도메인의 AAA 서버로 전송된다. 802.1x 절차가 완료되면 이동 노드의 외부 망 사용이 허용되고 이동 노드와 AP 간의 무선 구간을 보호하기 위한 세션 키가 설정된다.

3.2.2 Mobile IP에서의 RR 기반의 인증 구조

이동 노드와 상대 노드는 사전에 협의된 보안협약(SA)를 가지지 않는다. 따라서 RR을 사용하는 경우 이들 간에 암호학적 연산을 통해 패킷을 암호화할 수 없다[3]. RR의 기본 동작을 보면 그림 3과 같다. 먼저 이동 노드는 HoTI(Home Test Init) 메시지를 통해 RR 절차를 시작한다. 이 메시지는 이동 노드의 홈 에이전트를 경유해 상대 노드로 전달되며, 메시지 수신 시 상대 노드는 바인딩 키를 생성하고 HoTI 메시지에 대한 응답으로 HoT(Home Test) 메시지를 이동 노드로 전송한다. 이때 메시지는 홈 에이전트를 통해 터널링 되며 상대 노드가 생성한 바인딩 키의 절반이 포함된다. HoT를 수신한 후 이동 노드는 직접 경로를 통해 상대 노드로 CoTI(Care-of Test Init) 메시지를 전송하며 이에 대한 응답으로 CoT(Care-of Test) 메시지를 수신하는데 메시지에는 상대 노드가 생성한 바인딩 키(키 재료)의 나머지 절반에 해당하는 정보가 포함된다. CoT 메시지를 수신하면 이동 노드는 HoT 메시지에서 수신한 정보와 함께 바인딩 키(키 재료)를 유도하고 상대 노드로 바인딩 갱신 메시지를 전송하고 응답을 수신하게 된다. 바인딩 정보는 유도된 바인딩 키에 의해서 보호된다. 무선 랜 환경에서 802.1x를 통해 인증을 처리하는 경우 이동 노드는 새로운 망에 접속했을 때 먼저 AP와의 Association 절차를 수행하고 해당 망에서의 인증 작업을 성공적으로 마쳐야 한다. 따라서 RR 절차를 시작하기 전에 반드시 외부 망 엔티티를 통한 인증 및 세션 키 분배 과정을 수행해야 한다[7].

3.3 제안하는 인증 및 경로 최적화를 제공하는 AAA 구조

AAA를 통한 인증 및 경로 최적화를 위해 6개의 메시지가 정의된다. AReq 메시지는 이동 노드에 의해 발생하는 메시지로서 Attendant와의 세션 설정 및 사용을 위한 키 요청, 홈 등록을 위한 바인딩 키 재료 요청 및 경로 최적화를 위한 키 재료 요청을 위해 사용된다. 이 메시지는 아직 이동 노드가 외부 링크에 대한 엑세스 권한을 얻지 못한 상태에서 사용되므로 DHCP(Dynamic Host Configuration Protocol) 서버를 통해 CoA를 할당 받았을지라도 이 주소를 사용할 수 없다. 그러므로 이 메시지는 2 계층 프로토콜인 EAPoL을 통해 Attendant로 전송된다. AMR 메시는 Diameter[8] 메시지로서 이동 노드가 보낸 인증 및 키 재료 교환 요청을 Attendant가 받아서 Diameter 메시지로 변경하고 AReq 메시지에 실려 있는 보안 파라메터를 이에 상응하는 AVP(Attribute Value Pair)들로 매핑한 후 AAA 서버로 전송한다. ACR 메시지는 AAA 서버가 상대 노드로 전송하는 메시지로서 경로 최적화를 위한 바인딩 키 생성 재료 요청 파라메터를 가진다. AAA 서버는 상대 노드로 메시지를 보내기 전에 Diameter 프로토콜을 통해 전송된 메시지를 상대 노드가 이해할 수 있는 프로토콜로 변환한 후 전송한다. ACA 메시지는 ACR 메시지에 대한 상대 노드로부터의 응답 메시지이다. AMA 메시지는 AAA 서버에 의해 Attendant로 전송되는 Diameter 메시지로서, AAA 서버는 AHR 메시지와 ACR 메시지에 대한 응답인 AHA 메시지와 ACA 메시

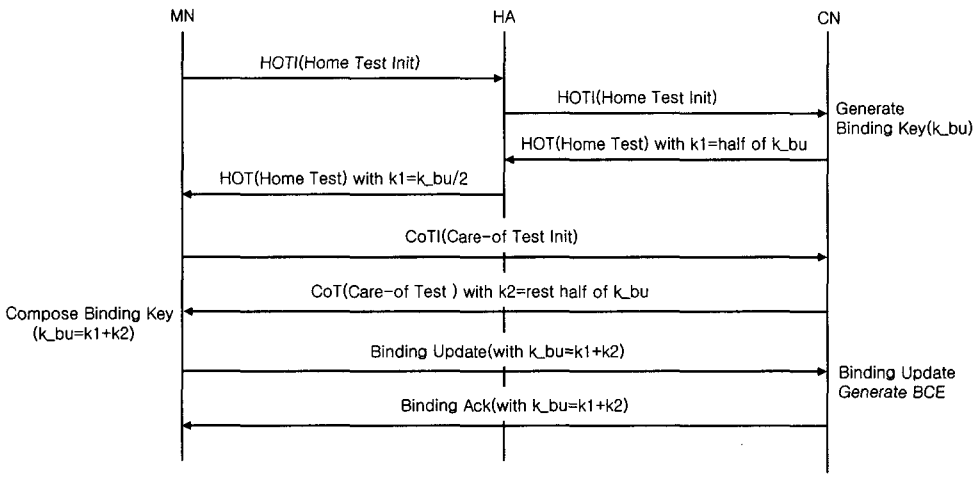

그림 3 RR을 이용한 경로 최적화 절차

지의 결과를 취합해서 Diameter 메시지 및 AVP로 변환한 후 전송한다. ARsp 메시지는 AReq 메시지에 대한 응답으로서 Attendant에 의해 EAPoL 메시지로 변환되어 이동 노드로 전송된다.

위에서 정의한 6개의 메시지를 통해 송수신되는 파라메터들은 다음과 같다. 먼저 'aaa_key' 이동 노드가 생성하는 키 재료(알고리즘, 암호화를 위한 secret 및 lifetime)를 가지며, 'attendant_key'는 이동 노드가 생성하는 키 재료로서 이동 노드와 Attendant간에 교환되는 메시지를 보호하기 위해 사용된다. 'CR'(MN Credential)은 MN을 인증하기 위해 H_AAA 서버에 의해서 사용되는 AAA Credential로서 이동 노드는 Diffie-Hellman 공개 값을 통해 자신을 인증하고 H_AAA 서버는 이동 노드가 보내온 Diffie-Hellman 공개 값을 검색함으로써 이동 노드를 인증할 수 있다. 'SecureParam_I'은 이동 노드가 전송하는 보안 파라메터로서 보안협약(SA) 설정항목(HASH_I, SA, Ni, KE등)을 포함하고 있으며, 'SecureParam_R'은 홈 에이전트 또는 상대 노드가 전송하는 보안 파라메터로서 보안협약(SA) 설정 항목을 포함하고 있다. HASH_R, SA, Nr, KE 등이 포함된다. 'NAI[4]'는 이동 노드에 대한 식별 값으로서, V_AAA 서버가 이 식별 값에 포함된 도메인 정보를 참조해서 메시지를 전달할 최종 H_AAA 서버를 알게 된다. 'RPI'(Replay Protection Indicator)는 이동 노드와 H_AAA 서버 사이에서 발생할 수 있는 재실행 공격(Replay Attack)을 방지하기 위한 랜덤 값으로서 타임스탬프, 넌스 값 또는 쿠키 값이 사용될 수 있다. 'HoA'와 'HaA'는 각각 이동 노드 및 홈 에이전트의 주소이며 RC(Result Code)는 AAA 응답 메시지 처리 결과를 나타낸다. 이동 노드와 상대 노드가 같은 도메인에 속한 노드인 경우 다음 그림 4와 같은 메시지 교환이 발생한다.

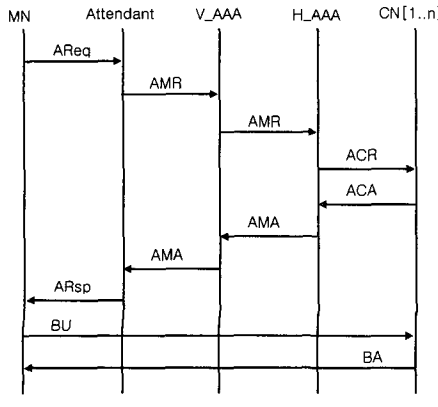

그림 4 동일 도메인 노드간 인증 및 바인딩 키 교환

단계 1에서 이동 노드는 인증 및 키 재료를 얻기 위해 EAPoL을 통해 다음 요청 메시지를 Attendant로 전송한다. 이때 LC, MN의 NAI, RPI, MN의 홈 주소, MN의 홈 에이전트 주소, CN의 주소, aaa_key, attendant_key, SecureParam_I 및 CR이 포함된다. 메시지를 수신하는 Attendant는 자신의 AAA 서버로 요청 메시지를 전달한다. 이때, EAPoL을 통해 MN으로부터 받은 메시지를 Diameter 프로토콜 메시지로 변환하여 전송한다. AVP들로는 Address AVP(Home-Address-Option, Home-Agent-Address-Option, CN-Address-Option), Security AVP(Nonce-Option, AAA-Key-Option, Attendant-Key-Option, Security-Parameter-Option, Authenticator-Option)등이 포함된다. V_AAA 서버는 Diameter 메시지에 포함된 NAI 옵션을 참조해서 이동 노드의 홈 AAA 서버를 알아낸 후 이 메시지를 그대로 포워딩하고 홈 AAA 서버는 이동 노드가 보낸 키 재료를 상대 노드로 전달한다. 이때 H_AAA는 Diameter 메시지의 AVP 옵션을 통해 수신된 CnA를 값을 참조해서 CN의 주소를 알 수 있다. 만일 이 옵션에 설정된 CN이 여러 개가 존재하는 경우 즉, 메시지 내에 CnA 옵션이 N개 존재하는 경우 N개의 CN에 대해 동일한 메시지(ACR)를 전송한다. H_AAA 서버는 Diameter 메시지를 상대 노드가 이해할 수 있는 다른 메시지 형태로 변환한 후 전송한다. 여기에는 MN의 홈 주소 및 SecureParam_I가 포함된다. CN은 ACR에 대한 응답 메시지로서 앞에서 수신한 SecureParam_I를 안전한 장소에 저장하고, 자신이 생성한 보안 협약 설정 관련 항목을 가지는 SecureParam_R을 리턴한다. H_AAA는 ACR 메시지에 대한 응답인 ACR을 수신한 후 H_AAA는 Diameter 메시지를 구성한 후 전송한다. 메시지에는 SecureParam_R 및 메시지 처리 결과 코드가 각각 Security AVP(Security-Parameter-Option) 및 Action AVP(Result-Code-Option) 형태로 변환된다. 방문망의 V_AAA서버는 H_AAA로부터 수신한 AMA 메시지에 로컬 보안을 위해 넌스값, attendant_key 및 CN의 SecureParam_R을 포함해서 Attendant로 보낸다. 이때 Attendant는 Nonce-Option 및 Attendant-Key-Option을 통해 로컬 보안을 위한 값을 추출하며, MN으로의 파라메터 전송을 위한 EAPoL 메시지를 생성한 후 AMA를 통해 수신된 나머지 파라메터들을 EAPoL 메시지에 실어서 MN으로 전송한다. 여기에는 LC, RPI, HoA, HaA, attendant_key, SecureParam_R 및 RC가 포함된다. 이동 노드는 상대 노드로부터 수신한 SecureParam_R을 통해 보안 키를 생성하고 BU/BA 메시지 보호를 위해 사용된다. 이동 노드와 상대 노드가 다른 도메인에 속한 노드인 경우

다음 그림 5와 같은 메시지 교환이 발생한다.

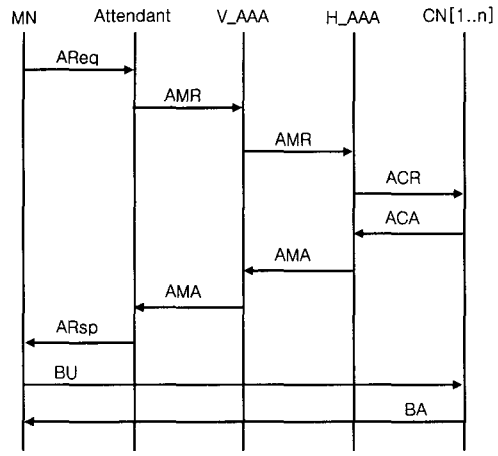

그림 5 다른 도메인에 속한 노드간의 인증 및 바인딩 키 교환

이 경우 홈 등록은 앞에서 기술한 방식을 따라 진행된다. 그러나 경로 최적화를 위한 바인딩 키 교환의 경우, 다음과 같은 점이 고려되어야 한다(m <= n).

- V_AAA[1..m]: CN이 현재 방문하고 있는 방문 망의 로컬 AAA 서버
- CN[1..n]: MN과 통신중인 또는 MN이 통신하고자 하는 하나 이상의 상대 노드

여기서 MN은 하나 이상의 상대 노드와 통신 경로 최적화를 위한 키 재료 교환을 요청할 수 있으며, 각각의 CN들은 임의의 시점에서 서로 다른 도메인의 방문 링크 상에 존재하거나(m=n) 또는 하나 이상의 CN이 같은 도메인에 존재할 수 있으므로(m<n), MN이 현재 속한 로컬 도메인의 AAA 서버는 CN의 주소를 기반으로 CN이 현재 속한 도메인을 알 수 있는 기능을 가져야 한다. CN이 SecureParam_I를 수신하면 이를 저장하고 SecureParam_R을 리턴한다.

4. 성능 평가

4.1 시스템 모델

성능 평가 기준은 제안 방식과 RR 방식 사용에 있어서 홈 등록 이후 경로 최적화를 수행하기 위해 MN이 CN에 등록을 완료하기까지의 기간 동안에 발생되는 비용 산출을 기반으로 하며 이때 노드간의 거리와 각 노드에서의 처리 시간 및 처리 지연으로 인해 발생하는 시간 동안 발생되는 데이타 패킷의 터널링 비용 등을 고려하여 계산하였다. 제안하는 구조에 포함된 여러 엔티티 간의 거리는 그림 6과 같다. 그림 6은 MN이 홈 등록을 마친 후 경로 최적화를 수행하기 위해 CN으로 바인딩 등록을 하는 과정에서 발생하는 비용 분석을 위한 시스템 모델로서 모델에 포함되는 각 엔티티 및 엔티티간의 거리를 보여 준다. 본 논문에서는 [9,10]에 기술된 접근 방법을 참조하였다.

CN은 λ 비율로 MN에게 패킷을 전송하고, MN은 μ 비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정한다. 이때 MN은 CN과의 평균 세션 유지 시간당 평균 몇 번 이동하는가에 관점을 둔다. 본 논문에서는 MN이 이동 때마다 CN으로부터 수신되는 평균 패킷 수를 Packet to Mobility Ratio(PMR)이라고 정의하고 수식 $p=\lambda/\mu$으로 정의한다. 본 논문에서는 패킷을 각각 제어 패킷과 데이타 패킷으로 구분하는데 제어 패킷의 평균 길이를 l_c 라 하고, 데이타 패킷의 평균 길이를 l_d 라고 정의하며, 비율은 $l = l_d/l_c$ 라고 정의한다. 즉, 제어 패킷을 전송하는 비용은 송신자와 수신자의 거리에 의해 주어지며 데이타 패킷의 전송 비용은 제어 패킷에 비해 평균 l배 크다고 정의한다. 그리고 한 호스트에서 제어 패킷을 처리하는 평균 비용은 r이라고 가정한다.

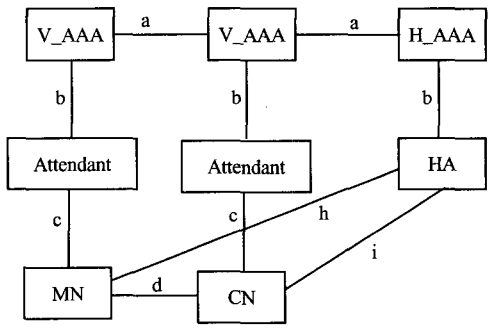

그림 6 비용 분석을 위한 시스템 모델

모델에서 각 엔티티는 외부 및 내부 링크로 서로 연결되어 있으며, 본 논문에서는 내부 엔티티간의 링크 가중치를 1로 정의하고 외부 링크의 경우 2로 정의한다. 즉, a=2, b=1, c=1, d=2, i=2 및 h=2로 정의할 수 있다. 이동 노드가 다른 서브넷으로 이동한 경우 자신의 홈 에이전트로 위치를 등록해야 한다. 홈 등록을 완료하기까지 CN이 MN으로 전송하는 모든 패킷은 분실 비용으로 처리된다. MN이 홈 등록을 완료하면 CN이 MN으로 보내는 패킷은 MN의 홈 에이전트를 경유해 터널링되어 전달되므로 이는 터널링 비용으로 처리될 수 있다. 따라서 MN이 이동했을 때 전체 비용을 계산하기 위한 타임 그래프는 다음과 같다. 따라서 전체 비용은 Loss 비용과 터널링 비용의 합으로 얻어질 수 있다.

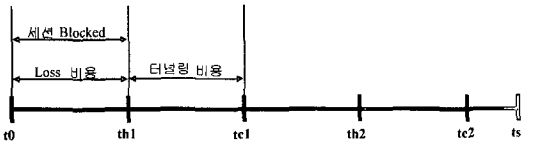

그림 7 전체 비용 타임 그래프

4.2 Mobile IPv6를 위한 AAA 인증 비용 분석

RR 바인딩 절차에서[3], MN이 이동 후 CN으로의 최종 바인딩 갱신을 완료하기까지의 시간 동안 발생하는 전체 비용은 (1)에 의해서 C_{RR}로 정의하며, 이동 노드가 홈 등록을 완료하는 비용($C_{BUHA-RR}$),홈 등록을 완료하기 전까지 데이타그램이 손실되는 비용($C_{loss-RR}$)과 홈 등록 후 MN이 CN에 바인딩을 갱신하는 비용(C_{BU-RR}) 및 CN에 바인딩 갱신하는 동안 CN이 HA를 경유해 MN으로 패킷을 터널링해서 보내는 비용(C_{dt-RR})의 합으로 다음과 같이 정의할 수 있다.

$$C_{RR}=(C_{BUHA-RR}+C_{loss-RR})+(C_{BU-RR}+C_{dt-RR}) \quad (1)$$

여기서 $C_{BUHA-RR}$는 MN의 홈 등록 비용($2h+3r$)이고, $C_{loss-RR}$는 MN의 홈 등록이 지연되는 동안 CN이 MN으로 전송한 패킷들로서, 홈 등록 이전의 모든 패킷은 분실된다. Mobile IP에서 등록 지연 동안 발생하는 단일 데이타 패킷의 터널링 비용 C_{data}는 $l(i+h)+3r$로 나타낼 수 있는데 이는 HA에서의 터널링을 통해 CN으로부터 MN으로 전달되는 비용을 의미한다.

$$C_{loss-RR}=\lambda \cdot t_{BUHA-RR} \cdot C_{data}=\lambda(2t_h+3t_r) \cdot l((i+h)+3r) \quad (2)$$

MN이 홈 등록을 마치고 RR을 이용한 경로 최적화를 위해 바인딩 갱신을 완료하는 비용은 (3)에 의해서 C_{BU-RR}로 정의하며, 그림 6의 구조에 의해 노드간 거리와 각 노드에서 처리하는 비용의 합으로서 다음과 같은 식으로 표현할 수 있다.

$$C_{BU-RR}=2(i+h)+4d+9r=2(2d+i+h)+9r \quad (3)$$

RR 처리가 지연되는 동안 CN에서 MN으로 보내는 패킷은 MN의 HA를 통해 터널링된다. 이때 터널링 비용을 C_{dt-RR}라고 두면, RR 지연동안 터널링되는 비용은 RR 지연 시간(t_{BU-RR}) 동안 전송되는 패킷에 대한 비용이므로 다음 식으로 나타낼 수 있다.

$$C_{dt-RR}=\lambda \times t_{BU-RR} \times C_{data} \quad (4)$$

RR 처리 지연 시간은 그림 6의 시스템 모델에 따라 각 링크 간 전송 시간 및 패킷 처리 시간의 합으로서 식 (5)와 같이 표현할 수 있다.

$$t_{BU-RR}=2(2t_d+t_i+t_h)+9t_r \quad (5)$$

그러므로 RR 방식에서의 CN 인증 및 바인딩 갱신의 전체 비용인 식 (1)을 정리하면 다음과 같다.

$$C_{RR}=2(2d+i+2h)+12r+\lambda(2(2t_d+t_i+2t_h)+12t_r) \times (l(i+h)+3r) \quad (6)$$

제안된 인증 기능을 가지는 바인딩 절차의 경우, MN이 이동 후 CN으로의 최종 바인딩 갱신을 완료하기까지의 시간 동안 발생하는 전체 비용 C_{AAA}은 RR 인증 및 바인딩 갱신의 경우와 마찬가지로 다음과 같이 표현할 수 있다.

$$C_{AAA}=(C_{BUHA-AAA}+C_{loss-AAA})+(C_{BU-AAA}+C_{dt-AAA}) \quad (7)$$

여기서 $C_{BUHA-AAA}$는 MN이 새로운 서브넷으로 이동한 후 수행하는 홈 등록 비용($2h+3r$)을 의미하며, $C_{loss-AAA}$는 MN이 홈 등록을 완료할 때까지 지연되는 시간동안 CN이 MN으로 보내는 패킷을 의미하는데, MN이 이동한 후 아직 홈 등록을 마치지 않았으므로 홈 등록이 처리되는 시간 동안($t_{BUHA-AAA}$) 패킷은 MN으로 전달되지 못하고 분실된다. 따라서 식 (8)과 같이 나타낼 수 있다. 여기서 Mobile IP에서 등록지연 동안 발생하는 단일 데이타 패킷의 터널링 비용 C_{data}는 $l(i+h)+3r$로 나타낼 수 있는데 이는 HA에서의 터널링을 통해 CN으로부터 MN으로 전달되는 비용을 의미한다.

$$C_{loss-AAA}=\lambda \cdot t_{BUHA-AAA} \cdot C_{data}=\lambda((2t_h+3t_r) \cdot l((i+h)+3r) \quad (8)$$

제안한 구조에서 새로운 서브 네트워크에서 MN의 인증 및 등록 비용, C_{BU-AAA}은 식 (9)와 같이 표현할 수 있다.

$$C_{BU-AAA}=4(b+c)+2(a+d)+13r \quad (9)$$

인증 및 CN으로의 등록 지연 시간(t_{BU-AAA}) 동안 CN이 MN으로 전송하는 패킷은 MN의 홈 에이전트를 통해 터널링 되는데, 이는 AAA를 통해 인증 및 바인딩 갱신이 진행되는 동안 CN이 MN으로 전송하는 패킷 비용으로서 식 (10)과 같다.

$$C_{dt-AAA}=\lambda \cdot t_{BU-AAA} \cdot C_{data} \quad (10)$$

여기서 Mobile IP에서 등록지연 동안 발생하는 단일 데이타 패킷의 터널링 비용 C_{data}는 $l(i+h)+3r$로 나타낼 수 있는데 이는 HA에서의 터널링을 통해 CN으로부터 MN으로 전달되는 비용을 의미한다. 그리고 제안하는 구조에서 인증 및 등록 지연 시간은 식 (11)에 의해 나타낼 수 있다.

$$t_{BU-AAA}=4(t_b+t_c)+2(t_a+t_d)+13tr \quad (11)$$

따라서, 제안하는 인증 및 등록 경우 식 (7)을 정리하면 전체 비용은 식 (12)와 같다.

$$C_{AAA} = (4(b+c)+2(a+d+h)+16r)+\lambda(4(t_b+t_c) +2(t_a+t_d+t_h)+16t_r)\times(l(i+h)+3r) \quad (12)$$

RR 인증 절차에 대한 비용과 제안하는 인증 절차에 대한 비율(C_{AAA}/C_{RR})을 (11)과 같이 도입할 수 있다. 또한 λ는 4.1절에 정의한 PMR($\rho=\frac{\lambda}{\mu}$)에 의해 $\rho\cdot\mu$로 나타낼 수 있다. 이는 PMR 변화에 따른 C_{RR} 비용 및 C_{AAA} 비용에 대한 상대적인 비교 값을 구하기 위한 것이다.

$$\frac{C_{BUHA-AAA}+C_{loss-AAA}+C_{BU-AAA}+C_{dt-AAA}}{C_{BUHA-RR}+C_{loss-RR}+C_{BU-RR}+C_{dt-RR}} = \frac{4(b+c)+2(a+d+h)+16r+p\times\mu\times t_{BU-AAA}\times C_{data}}{2(2d+i+2h)+12r+p\times\mu\times t_{BU-RR}\times C_{data}} \quad (13)$$

모델 이동성을 나타내기 위해 Uniform Fluid Model을 적용하였으며, 서브넷의 평균 크기를 150미터로 가정하고 차량 및 보행 이동 속도를 각각 60/mph와 2mph로 가정하였을 때 이동률(μ)은 각각 0.2와 0.01값을 가진다[9]. (5),(11)과 같이 인증 지연을 계산하기 위해, 라운드 트립 시간 분석 곡선 결과를 사용하였다[9]. 이 시간은 (14)와 (15)으로 나타낼 수 있다. 여기서 h는 노드 간 홉 수를 의미하며, k는 패킷의 길이를 나타낸다.

$$t_{RT\text{-}wire}(h,k) = 3.63k + 3.21(h-1) \quad (14)$$

$$t_{RT\text{-}wireless}(k) = 17.1k \quad (15)$$

4.3 이동 특성에 따른 비용 효율성 평가

본 절에서는 앞 절에서 기술한 시스템 모델 및 비용 분석 결과를 기반으로 제안된 모델의 성능 평가 결과를 기술한다. 한 노드에서 메시지 처리 비용은 동일(r=1)하다고 가정한다. 또한 같은 도메인 안에서의 거리에 대한 비용은 1(b=c=1)이고 가까운 두 도메인 간의 거리에 대한 비용은 2(a=h=i=d=2)로 가정할 때 차량 및 보행자의 이동 속도에 대한 PMR 즉, p 값에 따르는 비용 비율인 식 (13)의 결과는 그림 8, 그림 9와 같이 구해진다. 그림 8은 이동 노드가 차량의 속도로 이동하는 빠른 이동 특성을 가지는 경우(μ=0.2) PMR 값에 따른 인증 비용률(C_{AAA}/C_{RR}) 변화를 보여 준다. PMR 값은 0에서 100 사이의 값을 가지며, PMR 변경에 따른 인증 비용률(C_{AAA}/C_{RR})을 계산하여, 데이타 양이 각각 100 바이트와 1024 바이트인 경우에 대해 C_{RR}을 기준으로 상대적인 인증 비용 값인 C_{AAA}를 구하여 그래프로 나타내었다. 이동당 수신 패킷률이 크면 PMR 값이 증가하는데 이는 멀티미디어 전송과 같이 경로 최적화를 필요로 하는 대량 데이타 트래픽 특성을 가지는 세션임을 의미한다. RR 및 AAA를 이용한 인증 및 경로 최적화 비용을 비교해 보면, PMR 값이 증가함에 따라 인증 비용률이 감소하는데 수신되는 데이타 패킷의 평균길이가 큰 경우 더 빨리 감소함을 볼 수 있다. 즉, 대량의 트래픽 전송 특성을 가지는 세션에 대해 RR을 통한 경로 최적화시 발생되는 지연 및 분실 비용보다 AAA를 이용한 지연 및 분실 비용이 더 적게 든다. 데이타 패킷의 평균 길이가 1024바이트인 경우 PMR이 3인 지점과 데이타 패킷의 평균 길이가 100바이트인 경우 PRM이 35인 지점을 지나면 전체 인증 및 경로 최적화 비용율은 대략 0.80을 유지한다. 즉, 이 경우 C_{AAA}는 C_{RR}에 비해 최대 20 퍼센트의 비용 우수성을 보인다.

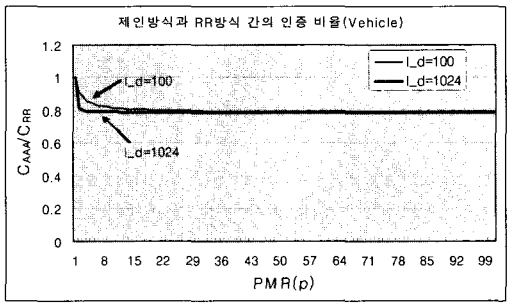

그림 8 차량 이동체의 이동 비용률(μ=0.2)

그림 9는 이동 노드가 보행자의 속도로 이동하는 특성을 가지는 경우(μ=0.01) PMR 값에 따른 인증 비용률(C_{AAA}/C_{RR})의 변화를 보여 준다. 이 경우 차량의 이동 속도로 움직이는 그림 8의 결과에 비해 비용률의 감소곡선은 서서히 감소하지만 PMR 값이 크고 송수신되는 평균 데이타양이 많을수록 전체 이동 비용률은 더 빠르게 감소한다. 그림 9에서 위의 곡선은 이동 당 평균 데이타패킷의 길이가 100 바이트인 예로서 RR 방식에 비해 PMR 증가에 따라 인증 및 경로 최적화 비용이 감소하며 PMR 값이 커지면 0.84값에 근사하며, 데이타 패킷의 평균 길이가 1024바이트인 경우 PMR이 증가하면서 비용률을 급격히 감소하고 PMR이 43인 지점에서 0.80 값으로 근사한다. 즉, 보행 속도로 이동하는 경우 PMR 변이에 따라 각각 최대 20퍼센트와 16 퍼센트의 비용 우수성 효과가 나타난다.

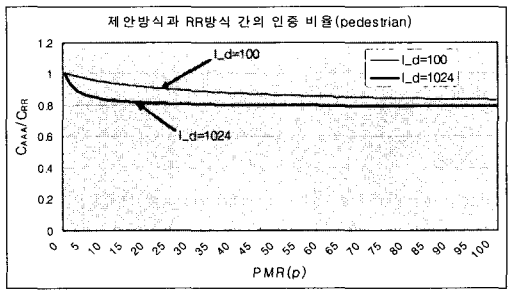

그림 9 보행자의 이동 비용률(μ=0.01)

5. 결 론

본 논문에서 제시한 방법은 이동 노드가 외부 링크 상에서 로밍 중에 홈 등록을 수행하고 상대 노드와의 경로 최적화를 위해 바인딩 등록을 하는 과정에서 안전하게 상호 인증이 가능하고 바인딩 키를 분배할 수 있는 방법을 제시한다. RR은 구조가 간단하지만 제공하는 보안 강도가 낮다. 즉, 공격자에 의해 바인딩 키를 노출당할 수 있다. 이는 매우 심각한 상황으로서 만일 이동 노드와 상대 노드 간 또는 상대 노드와 홈 에이전트 간에 존재하는 공격자에 의해 키가 노출된다면 경로 최적화 패킷은 위조될 수 있으며 이동 노드와 상대 노드간의 통신은 두절 되거나 악의적은 노드로 재 지정되어진다. 따라서 향상된 보안 강도를 제공하고 성능 저하를 줄이기 위한 방법이 모색되어야 한다. 본 논문에서는 보안 강도를 높이기 위한 방안으로서 AAA 인프라 구조를 사용한 인증 및 바인딩 키 분배 방법을 제안하고 있다. AAA는 유선 및 무선에 대한 인증 및 보안을 위한 안전한 인프라 구조로서 기존에 많은 ISP에서 적용하고 있는 기술이다. 특히, DIAMETER는 이전의 기술들(RADIUS등)의 단점을 보완하는 확장성 있는 안전한 구조를 가지고 있고, 향후 AAA는 DIAMETER로 발전해 나갈 것이므로, 본 연구에서는 DIAMETER 기반의 AAA 인프라 구조를 이용한 상호 인증 및 바인딩 키의 안전한 분배 방법을 제안하였다. 제안된 방법에서 MN과 CN간의 상호 인증 및 CN으로의 바인딩 등록을 위한 바인딩 키 분배는 AAA(DIAMETER)를 기반으로 이루어지므로 RR 에 비해 안전하다고 할 수 있다.

본 논문에서는 비용 분석을 위한 시스템 모델을 제안하였으며, MN이 지정된 세션에 대해 평균 이동비율 당 CN으로부터 수신하는 평균 패킷 수인 PMR을 정의하였다. 제안된 모델을 기반으로 한 RR 방식의 인증 및 등록 비용과 AAA를 기반으로 제안하는 방식의 인증 및 등록 비용에 대한 비용 비율을 계산하였으며, PMR 값의 증감 및 데이타양에 따르는 비용을 분석하였다. 결과적으로 PMR 값이 증가하는 경우 제안 방법의 인증 및 등록 비용이 RR 방식을 사용한 경우에 비해 낮아지고 이동 노드가 차량의 속도로 움직일 때 데이타 패킷의 평균 길이에 따라 차이가 있으나 각각 최대 20퍼센트의 비용 절감 효과를 얻을 수 있으며 이동 노드가 보행 속도로 움직이는 경우 데이타 패킷의 길이가 1024바이트인 경우와 100바이트인 경우 각각 최대 20% 및 16%의 비용 절감효과를 얻을 수 있다. 이 결과를 바탕으로 AAA 및 기존의 보안 인프라와의 통합된 구조를 염두에 둔 Mobile IP 보안 해결 방안에 적용할 수 있을 것이다.

참 고 문 헌

[1] F. Dupont, J. Bournelle: AAA for Mobile IPv6, draft-dupont-mipv6-aaa-01.txt, Internet Draft IETF, Nov. 2001.

[2] Pat R. Calhoun, Charels E. Perkins: Diameter Mobile IPv4 Application, Intener Draft, Internet Engineeri Task Force, Nov. 2001.

[3] David B. Johnson, Charles E. Perkins, Jari Arkko: Mobility Support in IPv6, draft-ietf-mobileip-ipv6-24.txt, Internet Draft IETF, Dec. 2003.

[4] P.Calhoun, C.Perkins: Mobile IP Network Access Identifier Extension for IPv4, RFC 2794, IETF, March, 2000.

[5] Franck Le, Basavaraj Patil, Charles E. Perkins: Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-03.txt, Internet Draft IETF, Oct. 2003.

[6] Allison Mankin, Basavaraj Patil, Dan Harkins, Erik Nordmark, Pekka Nikander, Phil Roberts, Thomas Narten: Threat Model introduced by Mobil IPv6 and Requirements for Security in Mobile IPv6, draft-ietf-mobileip-ipv6-scrty-reqts-02.txt, Internet Draft IETF, May, 2001.

[7] IEEE Std 802.1x-2001: Port-Based Network Access Control, June 2001.

[8] Pat R. Calhoun, Erik Guttman, Jari Arkko: Diameter Base Protocol, RFC3588, IETF, Sep. 2003.

[9] R. Jain, T.Raleigh, C. Graff and M. Bereschinsky: Mobile Interner Access and QoS Guarantees Using Mobile IP and RSVP with Location Registers, in Proc. ICC'98 Conf., pp.1690-1695, Atlanta, Jan. 1998.

[10] Thomas, R., H. Gilbert and G.Mazzioto: Infulence of the mobile station on the performance of a radio mobile cellualar network, Proc. 3rd Nordc Sem., paper 9.4, Copenhagen, Denmark, Sep. 1988.

김 미 영

1992년 전주우석대학교 전산학과 졸업(학사). 1995년 광운대학교 대학원 전산학과 졸업(석사). 1995년~1997년 (주)필컴 시스템 개발부 근무. 2000년~현재 숭실대학교 대학원 컴퓨터학과 박사과정. 관심분야는 Mobile IP, AAA, Network Security

문 영 성

연세대학교 전자공학 학사. 캐나다 Univ. of Alberta 전자공학 석사. Univ. of Texas, Arlington 컴퓨터공학 박사. 1992년 미국 Supercomputing 학술대회 최우수 학생논문상 수상. 숭실대학교 컴퓨터학부 부교수. Journal of Supercomputing 편집위원. 관심분야는 Mobile IP, IPv6, Grid networking