DOI: 10.3745/KIPSTC.2009.16-C.2.165

이동 네트워크(NEMO)에서 HMIPv6를 적용한 AAA 인증 방안 연구

최 경[†] · 김 미 희[††] · 채 기 준[†††]

요 약

Mobile IPv6는 시그널 양이 단말과 비례한다는 점에서 대역폭 낭비가 심하며 또한, 무선 이동 네트워크 분야에서는 바인딩 시그널 양과 트래픽, 효과적인 이동성을 지원할 수 있는 점이 강화되어야 한다. 이에 따라, Mobile IPv6를 확장한 NEMO(NEtwork MObility)에 대한 연구가 이루어지고 있다. NEMO는 여러 이동 단말과 하나 이상의 이동 라우터를 이동 네트워크라는 단위로 묶어 이동성을 제공한다. 이때 노드들은 이동 라우터를 통해 인터넷에 접속하기 때문에 이동 시 별도의 작업이 필요없는 투명성을 제공받고, 그만큼 바인딩 시그널이 줄어 바인딩 스톰 문제를 해결할 수 있다.

NEMO는 이동성 지원을 통해 여러 네트워크들이 계층적으로 이루어 질 수 있는 다양한 이동 구조를 갖게 되고, 이동 시 상위 네트워크 혹은 하위 네트워크들 간의 인증을 통해 안전성과 보안성을 향상되어야 함이 필수적이다. 또한, 안전한 인증 뿐만 아니라 빠른 핸드오프가 이루어져서 이동성에 따라 수반되는 효율성을 향상시킬 수 있는 방안에 관한 연구가 무엇보다 필요한 실정이다.

본 논문에서는 이를 위해 다양한 NEMO 이동 시나리오를 7가지로 정리하고, 각 시나리오별 AAA인증과 F+HMIPv6를 적용하여 안전한 인증과 빠른 핸드오프를 통한 인증 및 핸드오프 시 발생하는 시그널링 양과 패킷 지연률을 효과적으로 감소할 수 있는 방안을 제시한다.

키워드 : AAA, NEMO, HMIPv6, FMIPv6, NEMO 이동 시나리오, 빠른 핸드오프, 계층적 핸드오프, 인증

An Authentication and Handoff Mechanism using AAA and HMIPv6 on NEMO Environment

Kyung Choi[†] · Mihui Kim[††] · Kijoon Chae[†††]

ABSTRACT

Mobile IPv6 spends considerable bandwidth considering that its signal volume is proportional to the mobile and also it should be strengthened to support the binding signal volume, the traffic, and effective mobility. So, the study in NEMO(Network Mobility), an extended version of Mobile IPv6, has been conducted. NEMO provides its mobility by putting several mobiles and more than one portable router into one unit called as mobile network. Because nodes access Internet via the portable router at this time, it receives transparency without any additional work and that much reduces binding signal while solving binding storm.

By supporting mobility, NEMO is able to have various mobile structures which realize several networks hierarchically and it is necessary to improve its safety and security by authenticating among the upper networks or the lower ones while moving. Also, it is extremely required to begin a study in the device to improve efficiency accompanied with mobility, which is executed by the fast hand-off as well as the safe authentication.

For those reasons, this paper not only classifies various NEMO mobile scenarios into 7 ways, but also provides AAA authentication of each scenario, the authentication through the safety authentication and fast handoff authentication using F+HMIPv6 and the way to reduce both signaling volume and packet delays efficiently during the handoff.

Keywords : AAA, NEMO, HMIPv6, FMIPv6, NEMO Movement Scenario, Fast Handoff, Hierarchical Handoff, Authentication

1. 서 론

최근 네트워크를 구성하는 노드인 이동통신 단말기, 노트북, PDA 등 많은 기기들의 이동성 지원에 대한 필요성이 증가하고 있으며 이동성을 지원하는 Mobile IPv6 [1]의 표준화와 같은 프로토콜들이 제안되고 있다. 또한 노드의 이동성 뿐만 아니라 네트워크 자체의 이동성 지원을 위한

※ 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(NO. R01-2008-000-20062-0).
† 정 회 원 : 이화여자대학교 컴퓨터공학과 박사과정
†† 정 회 원 : North Carolina State University the department of computer science visiting scholar
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2008년 4월 16일
수 정 일 : 1차 2008년 10월 1일, 2차 2009년 1월 7일
심사완료 : 2009년 1월 14일

NEMO(Network Mobility)에 대한 연구도 활발하게 이루어지고 있다.

IETF(Internet Engineering Task Force)의 NEMO 워킹 그룹에서는 네트워크의 이동성을 지원하는 NEMO Basic Support Protocol [2]을 제안했으며 이와 관련된 다양한 연구가 진행되고 있다. 네트워크 이동성을 위한 NEMO는 이동 라우터(MR: Mobile Router)를 이용한 이동성 지원 및 이와 관련된 이동 노드(MN: Mobile Node)들의 이동과 관련한 투명한 IP 연결성을 지원한다.

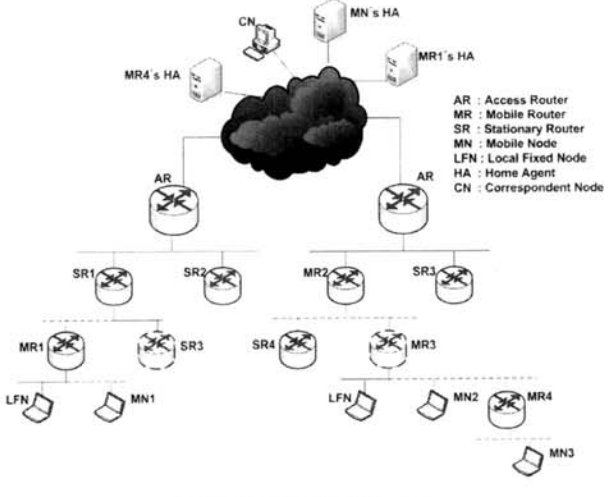
MN 혹은 MR이 이동하여 현재 속한 네트워크가 아닌 다른 도메인 네트워크로 이동 시, 자신의 홈 에이전트(HA: Home Agent)에게 새로운 위치에 대한 등록절차를 수행한다. 이러한 일련의 절차를 핸드오프라고 하며, 이동 시마다 핸드오프를 위한 많은 패킷 전송과 패킷 전송 지연 및 패킷 손실이 발생하고 있다.

이러한 문제들을 해결하기 위해 몇 가지 메커니즘이 제안되고 표준화되었는데, 그 중 빠른 핸드오프 메커니즘(FMIPv6 : Fast MIPv6) [3] 과 계층적 MIPv6(HMIPv6 : Hierarchical MIPv6) [4]가 있다.

FMIPv6는 MN이 외부 도메인으로 이동 시 필요한 핸드오프 지연 및 패킷 손실을 최소화하고자 핸드오프 절차 및 방안을 제안하였다. HMIPv6는 지역 이동성을 고려한 접근 방법으로써 MAP(Mobility Anchor Point)을 도입하여 외부 도메인내에서의 핸드오프 수행 시 MAP을 이용한 핸드오프 절차 간소화를 통해 MN과 HA 사이의 메시지 양을 줄임과 동시에 시간을 줄일 수 있도록 한다.

이동 시 핸드오프에 관한 연구 뿐만 아니라 안전한 이동 노드 인증을 통한 이동 네트워크 환경의 위협을 줄이기 위해 AAA(Authentication, Authorization, and Accounting)에 관한 연구[5]가 이루어지고 있다. AAA 서비스를 다양한 기술 분야별로 도입 연구가 이루어지고 있는 실정인데, 관련 연구는 Mobile IPv6를 위한 AAA연구[6]와 더불어 NEMO에 적용한 AAA[7] 등이 있다.

NEMO는 이동 네트워크 환경으로써 고정 라우터, 이동 라우터, 이동 노드, 고정 노드 등의 다양한 접속 및 이동이 발생하며, 이때 중첩 네트워크(Nested Network)를 이루게 된다. (그림 1.1 참조)



(그림 1.1) NEMO 계층 구조

NEMO의 중첩 네트워크 환경에서 발생하는 다양한 이동 시나리오와 이에 따른 핸드오프 시 패킷 지연 및 손실과 패킷 전송 비용을 최소화하는 방안 연구가 필요하며, 아울러 핸드오프 시 각 MR, MN 등의 노드 인증을 적용하여 플러딩 공격(Flooding Attack), 리다이렉트 공격(Redirect Attack) 등의 DoS공격 등의 위협으로부터 보안을 강화해야 한다.

NEMO의 이동 네트워크 환경에서의 AAA를 적용한 인증 방안에 관한 연구는 이루어졌지만, 중첩 네트워크 환경 등의 다양한 이동 환경을 위한 빠른 핸드오프 및 인증을 접목한 연구는 이루어지지 못한 실정이다.

따라서, NEMO 이동 네트워크 환경에서 MR 및 MN의 이동 시나리오를 정리하고, 각 이동 시나리오별 효율적인 인증 및 핸드오프 방안을 제시한다.

이를 위해 NEMO 환경에서의 FMIPv6 도입으로 패킷 지연 및 손실을 최소화하도록 하며, HMIPv6를 같이 적용하여 외부 네트워크 도메인에서의 핸드오프 절차를 줄여 패킷 전송 절차의 간소화 및 패킷 전송 비용을 줄이는 효과를 준다.

또한 안전성 강화를 위한 인증 기법으로 AAA를 도입 적용하며, HMIPv6 수행 시 도입된 MAP에서 AAAL 역할을 같이 수행하도록 함으로써 효율성을 증대한다.

이동 시나리오별로 F+HMIPv6를 적용하며, AAA를 이용한 인증 및 핸드오프 절차를 제시하며 이에 따른 비용 및 성능 분석을 통해 효율성과 효과성을 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 NEMO의 구조 및 FMIPv6와 HMIPv6의 결합된 형태에 관하여 논의 및 NEMO에서의 AAA 인증 절차에 관하여 정의한다. 3장에서는 NEMO의 이동 시나리오를 정리하고 이동 시나리오별 F+HMIPv6와 AAA인증 절차를 결합한 방안을 제시하며, 4장에서는 제안된 방안의 비용을 분석하고 성능 평가 결과 및 안전성 분석을 기술한다. 마지막으로 5장에서는 결론을 맺는다.

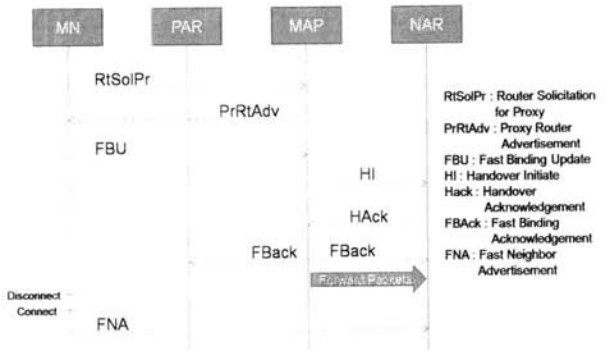
2. 관련 연구

2.1 F+HMIPv6

FMIPv6는 빠른 핸드오프 절차를 통해 핸드오프 시 발생할 수 있는 지연 및 패킷 손실을 줄이도록 제안[3]되었으며, HMIPv6는 지연과 시그널링 로드를 줄이고자 제안되었다.

[8]에서는 두 가지 프로토콜의 결합된 형태인 F+HMIPv6에 대해서 논의하고 있으며, MAP이 자신의 도메인에 속하는 Access Router(AR)과 관련된 IP 주소, IPv6 Prefix, 링크 주소 등에 대한 정보를 모두 알고 있다고 가정한다. 또한 이 구조에서는 MN의 위치를 나타내는 3가지 형태의 CoA(Care of Address)가 있다.

RCoA는 MN이 속한 MAP의 도메인을 의미하고 LCoA (on-Link Care-of Address)는 현재 이동 네트워크에서의 위



(그림 2.1) F+HMIPv6 빠른 핸드오프 절차

치를 나타내는 PLCoA(Previous on-Link Care-of Address)와 새로운 이동 네트워크로 이동했을 때 사용하게 될 NLCoA(New on-Link Care-of Address)로 나뉜다.

다음은 F+HMIPv6의 빠른 핸드오프 절차를 나타낸다.

- RtSolPr(Router Solicitation for Proxy)
  MN이 MAP에 속해 있는 AP의 정보를 얻기 위해 전송
- PrRtAdv(Proxy Router Advertisement)
  MNP(Mobile Network Prefix) 등의 정보를 포함하며, 이 정보를 통해 MN은 NLCoA를 설정
- FBU(Fast Binding Update)
  PLCoA와 이동하는 이동 네트워크에 대해서 MN이 설정한 NLCoA의 바인딩 및 MN의 새로운 위치로 패킷을 전달하기 위한 터널을 구성
- HI(Handover Initiate)
  NLCoA 전송
- HAck(Handover Acknowledgement)
  NLCoA 유효 검사 후 전송
- FBAck(Fast Binding Acknowledgement)
  핸드오프 절차 종료 알림
- FNA(Fast Neighbor Advertisement)
  접속을 알림. FNA를 받은 NAR은 터널을 통해 전달받아 저장하고 있던 패킷들을 MN에게 전송

2.2 AAA for NEMO

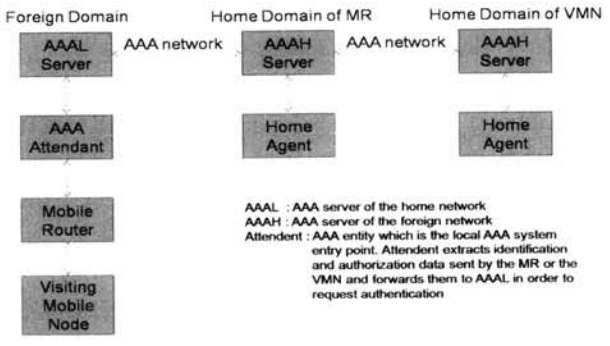
AAA(Authentication, Authorization and Account) 인프라 구조는 노드 인증 및 안전한 경로 최적화를 위한 키 분배를 제공한다. 이를 위해 Attendant, 방문 도메인의 AAA 서버, 홈 도메인의 AAA 서버 등의 엔티티를 이용한다.[7]

2.2.1 NEMO AAA Architecture

(그림 2.2)는 NEMO AAA 인증 구조를 나타내며, DIAMETER 프로토콜에 기초한다.

MR의 AAAH server는 MR에 대한 프로파일을 보유하며, MR과 long-term key를 공유한다. VMN의 AAAH server도 마찬가지로 VMN과 long-term key를 공유한다. AAAL server는 방문한 VMN이나 MR들을 위해 AAA 프로시저를 수행한다.

MR이 이동하여 외부 도메인에 접속한 경우, MR은 인증



(그림 2.2) NEMO AAA Architecture

을 통한 권한을 부여받아야 한다. Attendant는 이동 노드가 외부 도메인에서 가장 먼저 접속하게 되는 외부 엔티티로서 이동 노드가 전송하는 패킷에 대한 통과, 폐기, 보류 등의 정책을 수행할 수 있다. AAAL 서버는 방문 도메인의 AAA 인증 서버로서 이동 노드로부터 인증 요청을 수신하면 먼저 Attendant를 인증하고 메시지의 NAI나 홈 주소를 통해 이동 노드의 홈 도메인에 존재하는 AAA 인증 서버로 전송한다. AAAH 서버는 홈 도메인의 AAA 인증 서버로서, 이동 노드의 인증에 필요한 인증 정보들로 구성된 프로파일을 관리하고 있다. 이동 노드가 보내온 인증 정보를 기반으로 이동 노드에 대한 인증 처리 과정을 진행하고 결과를 AAAL 서버로 전송한다.

2.2.2 Inter-Domain AAA Procedure

NEMO는 외부 도메인 네트워크에 접속하게 되면, inter-domain AAA procedure를 수행한다. MR은 외부 도메인 네트워크의 AAAL 서버와 SA를 갖고 있지 않기에 MR의 홈 도메인 네트워크에 있는 AAAH 서버를 통해 인증 받아야 한다. (그림 2.3)은 inter-domain AAA procedure를 보여준다.

- AS(Attendant Solicit)
  MR이 Attendant에게 보내는 메시지로서, IPv6 router solicitation 메시지를 AAA 옵션으로 확장한 메시지.
- AA(Attendant Advertisement)
  Attendant가 LC(Local Challenge)를 포함한 AA 메시지를 MR에게 보낸다.
  AS 메시지 없이, Attendant가 주기적으로 AA 메시지를 브로드캐스트하기도 함.
- AReq(Authentication Request)
  MR은 LC값을 long-term SA로 암호화해서 CR(Credentia)를 만든다.
  AReq 메시지는 NAI, RPI, H@, HA@, LC, CR을 포함해서 전송한다.
  - NAI(Network Access Identifier) : MR 또는 VMN을 식별하는 정보.
  - RPI(Replay Protection Indicator) : Timestamp 또는 Random number.

- H@ : Home Address.
- HA@ : Home Agent Address.

• AMR(AA-Mobile-Router-Request)
Attendant는 전송 받은 정보들을 AMR(new DIAMETER message)로 바꾼다.

• AMR을 전송받은 AAAH 서버는 미리 설정된 SA로 CR을 복호화해서 전송받은 LC값과 비교해서 인증한다.
AAAH 서버는 동적인 키 두 쌍을 만든다.
- Key_local : 외부 방문 도메인에서 AAA 프로시저를 위해 사용되는 키.
- Key_home : MR과 MR의 HA 간 양방향 터널링을 위해 사용되는 키.

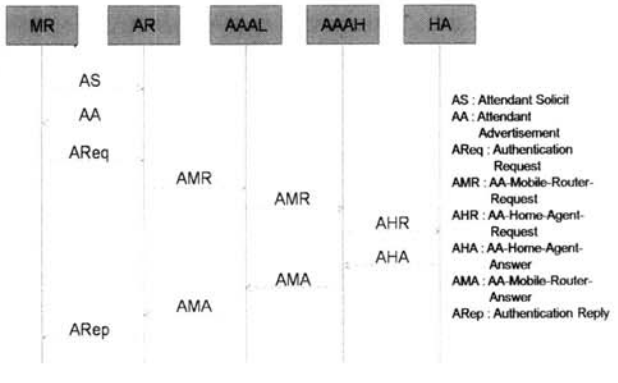
AAAH 서버는 SP_HOME과 SP_LOCAL 두 개의 Security Parameter 생성.

• AHR(AA-Home-Agent-Request)
AAAH 서버는 HA에게 NAI, RPI, H@, SP_HOME을 전송.
HA는 SP_HOME을 이용해서 key_home을 생성.

• AHA(AA-Home-Agent-Answer)
HA는 AAAH 서버에게 확인 메시지를 전송. NAI, H@ 포함.
AMA(AA-Mobile-Router-Answer)
AAAH 서버는 AAAL에게 NAI, RPI, H@, SP_LOCAL, SP_HOME을 전송.
AAAL 서버는 long-term key를 이용해서 메시지를 복호화 한 후, MR의 NAI를 저장한 후, key_local을 생성.

• ARep(Authentication Reply)
Attendant는 MR에게 NAI, RPI, H@, HA@, SP_HOME, SP_LOCAL을 전송.

MR은 Attendant(AR)에게 AS를 보내고, Attendant는 AS 메시지에 대한 응답으로 LC를 포함한 AA를 보낸다. MR은 받은 LC값을 AAAH 서버와 공유하고 있는 long-term SA(Security Association)를 이용해 암호화해서 CR을 만든다. MR은 LC, CR값을 포함한 AReq 메시지를 Attendant에게 전송한다. 또한, AReq 메시지는 AAAL 서버가 MR의 홈 도메인를 식별하도록 NAI 정보와 재생 공격(Replay Attack)을 방지하기 위한 RPI 정보를 포함해서 전송한다.



(그림 2.3) AAA procedure of MR : inter-domain handoff

Attendant가 AReq 메시지를 받으면, 새로운 DIAMETER 메시지인 AMR 메시지로 변환해서 외부 도메인에 있는 AAAL 서버에게 전송한다. AAAL 서버는 NAI 필드를 체크해서 MR을 AAAL 서버에서 자체적으로 인증할 정보를 갖고 있지 않다는 것을 확인하면, AMR 메시지를 MR의 AAAH 서버에게 포워딩한다. AAAH 서버가 AMR 메시지를 받으면, 미리 설정된 SA를 이용해 CR을 복호화하고 LC값과 결과를 비교해서 MR을 인증한다. 인증이 성공적으로 이루어지면 AAAH 서버는 두 개의 동적 키, key_local, key_home을 생성한다. 또한 AAAH 서버는 MR에서 key_local과 key_home을 생성할 수 있도록 SP_HOME과 SP_LOCAL을 생성한다. 이러한 보안 파라미터들은 MR과 AAAH 서버 간 long-term key를 사용해 암호화한다. 만약 AMR 메시지에 HA 주소가 없다면 AAAH 서버는 MR을 위한 HA를 할당한다.

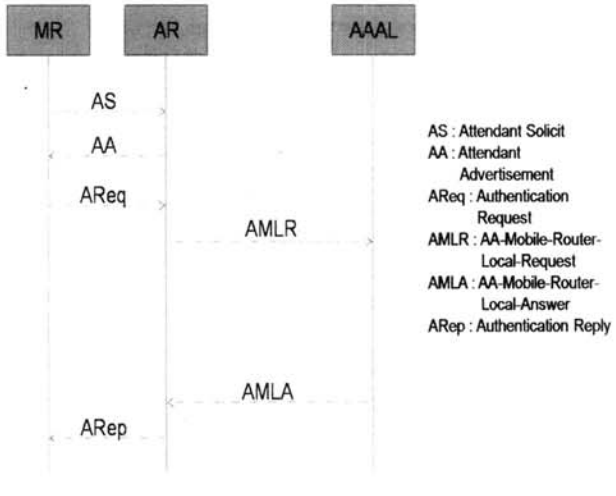
AAAH 서버는 AHR 메시지를 통해 HA에게 MR의 NAI와 SP_HOME 정보를 알린다. HA는 SP_HOME을 이용해 key_home을 생성하고, AHA 메시지로 확인 메시지를 보낸다. AAA의 결과로 AAAH 서버는 AMA 메시지를 AAAL 서버에게 전송한다. AAAL 서버는 인증 승인과 함께 AMA 메시지를 받으면, long-term key를 이용해 메시지를 복호화하고 MR의 NAI를 저장하고 key_local을 생성한다.

AAAL 서버는 Attendant에게 SP_LOCAL을 제외하고 AAAH 서버에게 받은 AMA 메시지를 전송한다. Attendant가 AMA 메시지를 받으면 MR이 인증되었음을 확인하고 MR의 네트워크 액세스를 허용한다. 또한 Attendant는 MR의 결과를 ARep 메시지를 통해 알려준다.

2.2.3 Intra-Domain AAA Procedure

NEMO는 외부 도메인 네트워크 내에서 이동하게 되면, intra-domain AAA procedure를 수행한다. (그림 2.4)는 intra-domain AAA procedure를 나타낸다. MR이나 VMN은 AAAL 서버와 인증 절차를 거치면 된다.

• AReq(Authentication Request)



(그림 2.4) AAA procedure of MR : intra-domain handoff

MR은 CR_L(Local Credential)을 Attendant에게 전송. CR_L은 CR과 다르며, key_local을 통해 생성되는 인증 코드.

- AMLR(AA-Mobile-Router-Local-Request)
  Attendant는 전송 받은 정보들을 AMLR(new DIAMETER message)로 바꾼다.
  Attendant는 NAI, RPI, H@, HA@, LC, CR_L을 AAAL 서버에게 전송.
  AAAL 서버는 이미 저장된 key_local을 이용해 MR을 인증.
- AMLA(AA-Mobile-Router-Local-Answer)
  AAAL 서버는 Attendant에게 NAI, RPI, H@, HA@과 함께 인증 결과 전송.
- ARep(Authentication Reply)
  Attendant는 MR에게 인증 결과를 전송.

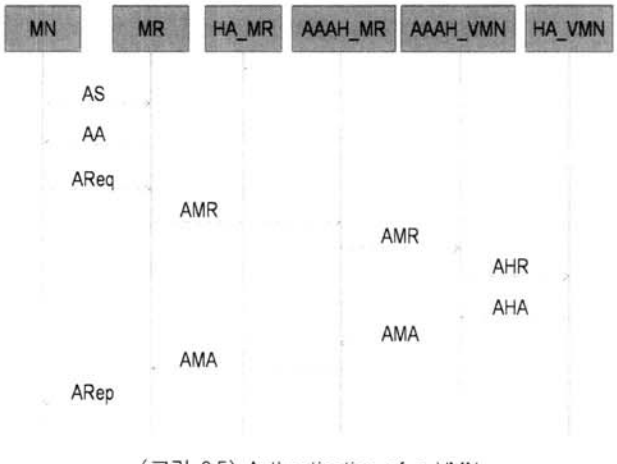
AA 메시지에 대한 응답으로, MR은 CR_L을 포함한 AReq 메시지를 Attendant에게 보낸다. Attendant는 AMLR DIAMETER 메시지를 생성해서 AAAL 서버에게 전송한다. AAAL 서버가 AMLR 메시지를 받으면, AAAL 서버는 저장된 key_local을 이용해 MR을 인증하고 AMLA 메시지를 결과로 Attendant에게 알려준다. 그러면 Attendant는 ARep 메시지를 통해 결과를 전달한다.

2.2.4 Authentication of a VMN

방문한 MN이 NEMO의 MR에 접속하는 경우로, (그림 2.5)와 같은 절차를 갖는다.

이때 MR은 Attendant로 동작한다. 인증 절차 과정은 inter-domain과 유사하다.

MR이 주기적으로 AA 메시지를 브로드캐스트하거나, VMN의 AS 메시지에 대한 응답으로 AA 메시지를 전송한다. VMN은 VMN의 AAAH 서버와 공유하는 SA를 이용해 CR을 생성하고 MR에게 AReq 메시지를 보낸다. MR은 AReq 메시지를 DIAMETER 메시지로 변환한 AMR 메시지를 MR의 AAAH 서버에게 전송한다. AAAH_MR이 AMR 메시지를 받으면, AAAH_MR은 VMN의 AAAH 서버에게 전달한다. AAAH_VMN은 VMN을 인증한다. 이 과정에서 inter-domain AAA 프로시저에서와 마찬가지로 key_home, key_local, SP_HOME, SP_LOCAL을 생성한다. 나머지 인증 과정은 inter-domain AAA 프로시저와 같다.



(그림 2.5) Authentication of a VMN

외부 네트워크에 로밍되어 있는 NEMO에 접속한 VMN은 NEMO가 접속 지점을 바꾸더라도 자신의 HA에게 위치를 등록할 필요가 없다. 이런 이동 투명성이 NEMO의 중요 장점이다.[2]

2.3 기존 연구 현황

Mobile IP에 관한 연구는 IETF(Internet Engineering Task Force)의 Mipshop 워킹그룹에서 Mobile IP에 관한 성능, 시그널링, 핸드오프 최적화 등에 관한 연구가 진행중이다. Mobile IPv6에서 핸드오프와 관련하여 FMIPv6와 HMIPv6 등이 RFC로 발표되었으며, 이를 적용한 다양한 연구들이 진행되고 있다.

또한 Mobile IP 환경에서 키를 이용한 인증 방안과 AAA를 이용한 인증 등 인증과 관련한 많은 연구들이 진행 중이며, AAA인증과 HMIPv6를 접목하여 인증의 효율성을 증가하는 방안에 관한 연구[9] 등이 있다.

NEMO와 관련된 연구는 IETF의 NEMO 워킹그룹에서 진행중이며, NEMO Basic Support Protocol은 RFC3963으로 발표되었으며[2], 이외에 NEMO에서의 핸드오프에 관련한 연구와 인증에 관한 연구 등 다양한 분야의 연구가 진행중이다.

핸드오프에 관한 연구는 빠른 핸드오프를 위한 FMIPv6와 HMIPv6를 적용하여 핸드오프 성능 분석 연구[10]와 NEMO와 결합된 HMIPv6에서 멀티캐스팅을 이용한 핸드오프 지원 기법[11] 연구 등 NMEO에서 빠른 핸드오프를 위한 연구들이 있다.

또한, NEMO에서 인증과 관련한 연구는 AAA와 연관된 연구가 주를 이루고 있는데, AAA for NEMO[7]가 draft로 발표되었으며, 이외에 키를 이용한 인증 메커니즘 등이 연구되고 있다.

하지만, 아직 NEMO에 대한 인증이나 핸드오프에 관한 연구는 활발히 연구되지 않은 상황이여서 앞으로 NEMO에 관한 많은 연구들이 진행되어야 한다.

또한 NEMO에서 이동 시 발생하는 시그널링 양과 지연을 줄이기 위한 빠른 핸드오프와 안전한 인증을 동시에 실행하는 통합 방안에 관한 연구가 부재한 실정이다.

3. 제안하는 인증 및 핸드오프 최적화 방안

본 장에서는 2장에서 살펴본 NEMO에서 F+HMIPv6를 적용한 빠른 핸드오프와 AAA를 이용한 인증을 효율적으로 수행하는 방안을 제안한다. 우선 이동 네트워크에서의 이동 시나리오를 7가지 정의하고, 각 시나리오별 효율적인 인증과 핸드오프 방안을 제시한다.

기존 AAA 인증 방식[6]에서는 지역 이동과는 무관하게 방문 도메인과 홈 도메인의 AAA서버간의 메시지 교환을 통한 인증처리를 제공하므로, 지역 이동성을 고려하여 NEMO에 적합하게 제안한 AAA for NEMO[7]을 기반으로 한다.

NEMO는 이동성을 중점으로 한 네트워크 환경이기에, 빈번한 이동이 발생할 수 있고 이로 인한 외부 네트워크 도메인 방문이 잦게 된다. 또한 이동 시 계층적 네트워크 환경에 접속할 수도 있기 때문에 이런 환경을 고려한 핸드오프와 인증 방안을 마련해야 한다. 지역 이동성을 고려한 접근 방법인 HMIPv6를 통해 핸드오프의 시그널링 로드를 줄이고, 이와 더불어 인증을 위임받은 MAP+AAAL을 이용해 홈 에이전트의 AAAH 서버를 대신해 지역 인증 처리 및 키 분배를 함으로써 패킷 전송 횟수를 줄임과 동시에 빠른 이동에 맞춘 빠른 인증 및 핸드오프 처리를 수행함으로써 효율성을 최대화하도록 한다.

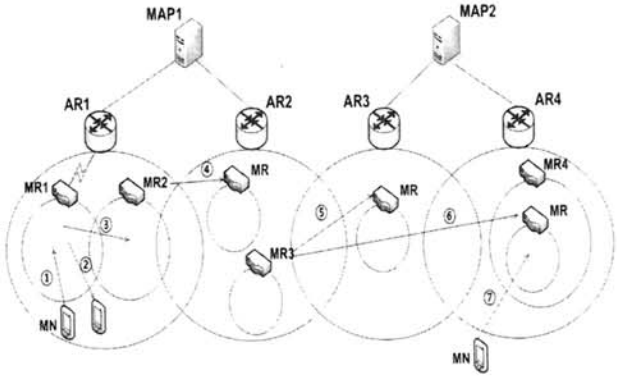
3.1 NEMO 이동 시나리오

NEMO의 다양한 이동 시나리오들 중 다음과 같이 4가지 MN의 이동과 3가지 MR의 이동에 대해서 정의한다. [10]

(그림 3.1)은 MN과 MR의 이동 시나리오를 보여주고 있다. 각 시나리오에서 이동개체는 새로운 위치로 이동 후, 자신의 새로운 주소를 MAP에게 알림으로써 MAP이 관리하는 바인딩 캐시를 업데이트한다.

시나리오 1 : MN이 이동 네트워크에 들어가는 경우
시나리오 2 : MN이 이동 네트워크에서 이탈하는 경우
시나리오 3 : MN이 이동 네트워크를 변경하는 경우
시나리오 4 : 동일한 MAP 도메인 내에서 AR을 변경하는 경우
시나리오 5 : 또 다른 MAP 도메인으로 AR을 변경하는 경우
시나리오 6 : 또 다른 MAP 도메인 내의 이동 네트워크와 연결되는 경우
시나리오 7 : VMN이 Nested 이동 네트워크에 들어가는 경우

3.2 제안하는 시나리오별 인증 및 핸드오프 절차

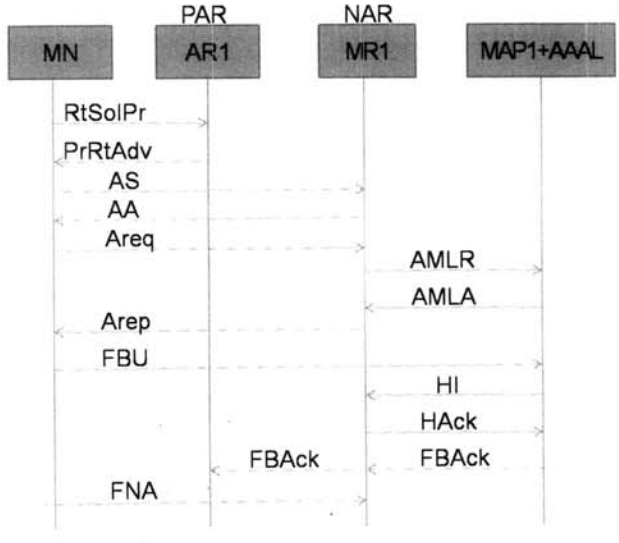


(그림 3.1) NEMO 이동 시나리오

3.2.1 MN이 이동 네트워크에 들어가는 경우

AR1에 접속해 있던 MN은 이동 네트워크인 MR1에 들어가기 위해 AR1에게 MAP에게 속해 있는 AP정보를 얻기 위해 RtSolPr 메시지를 보낸다. AR1은 MNP정보를 포함한 PrRtAdv 메시지를 전송하고, 이를 수신한 MN은 MNP를 통해 NLCoA를 생성한다. 바인딩 업데이트를 하기 전에 인증을 위해 접속하고자 하는 MR1에게 AS 메시지를 전송하고, MR1은 LC를 포함한 AA 메시지를 MN에게 전송한다. MN은 key_local을 이용해서 CR_L을 생성해서 MR1에게 인증 요청 메시지 AReq를 보낸다. MR1은 MAP1+AAAL에게 AAA DIAMETER 메시지로 전환하여 AMLR을 전송한다. MAP+AAAL은 key_local을 이용해서 MN을 인증한 후, 결과 메시지 AMLA를 MR1에게 전송하고, MR1은 이 메시지를 ARep로 전환하여 MN에게 전송한다.

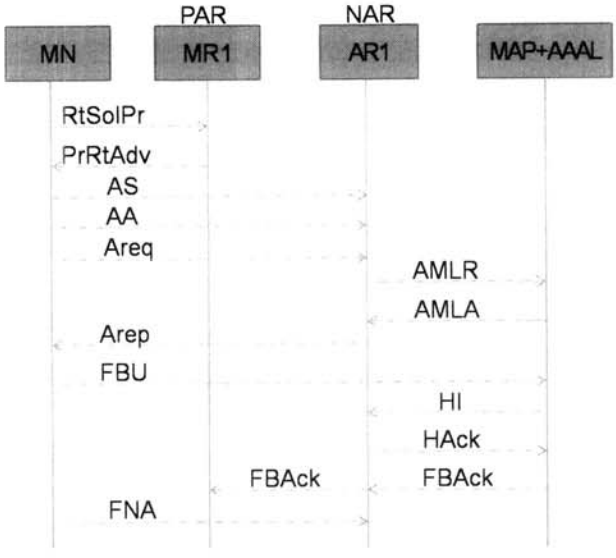
인증 과정이 성공적으로 수행되면, MN은 MAP1+ AAAL에게 생성한 NLCoA를 등록하기 위해 바인딩 업데이트 메시지를 보낸다. MAP1+AAAL은 NLCoA를 저장한 후, MR1에게 NLCoA를 포함한 HI 메시지를 전송하고, MR1은 NLCoA의 유효성 검사 후 HAck 메시지를 MAP1+AAAL에게 보낸다. MAP+AAAL은 성공적인 핸드오프 절차 종료를 알리는 FBAck 메시지를 AR1과 MR1에게 전송하고, MR1에게 패킷을 전송한다. MN은 AR1과 접속을 종료하고, MR1에게 접속을 알리는 FNA 메시지를 전송한다. FNA를 받은 MR1은 터널을 통해 전송받아 저장하고 있던 패킷들을 MN에게 전송함으로써 성공적인 인증과 핸드오프 절차가 종료된다.



(그림 3.2) 제안1 : MN이 이동 네트워크에 들어가는 경우

3.2.2 MN이 이동 네트워크에서 이탈하는 경우

MN이 이동 네트워크인 MR1에서 이탈해서 AR1으로 이동하는 경우로, 절차는 (그림 3.3)과 같다. PAR(Previous Access Router)이 MR1이고, NAR(Next Access Router)이 AR1으로 바뀐 경우로, 3.2.1의 경우와 마찬가지 절차를 거치게 된다. 이때도 RCoA는 변함없이 NLCoA만 새로 등록 및



(그림 3.3) 제안2 : MN이 이동 네트워크에서 이탈하는 경우

인증하는 과정을 수행한다.

3.2.3 MN이 이동 네트워크를 변경하는 경우

MN이 AR1 내의 MR1 이동 네트워크에서 MR2 이동 네트워크로 이동하는 경우로, AR1에게 RtSolPr 메시지를 보내서 AP정보를 얻고, 이동하고자 하는 MR2를 통해 인증 과정을 거친 후, 생성한 NLCoA를 바인딩 업데이트 절차를 거친다.

이 경우도 홈 에이전트의 AAAH 서버로의 인증이나 새로운 CoA를 홈 에이전트에 등록할 필요없이, MAP+AAAL을 통해 인증과 새로운 NLCoA 바인딩 업데이트로 시그널링 로드를 현격히 줄일 수 있다.

3.2.4 동일한 MAP 도메인 내에서 AR을 변경하는 경우

이동 네트워크 MR이 동일한 MAP 도메인 내의 AR을 변경하는 경우로, MR의 마이크로 이동에 해당한다. 이 경우는 MR의 이동과 AR의 변경이라는 점 외에는 이전 세 가지 제안안과 인증 및 핸드오프 절차가 동일하다.

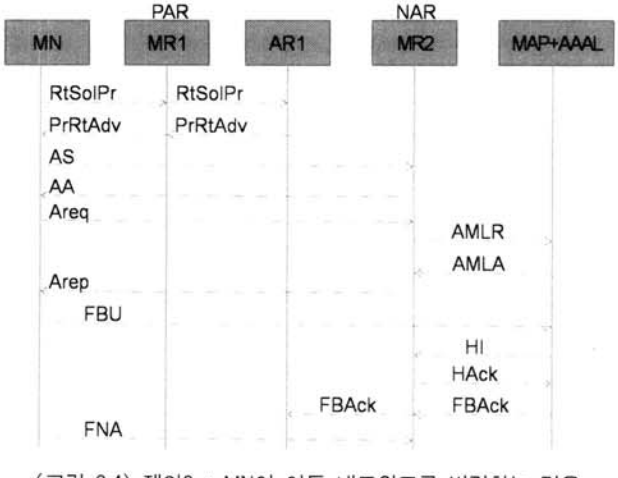
이 경우 역시 MR이 홈 에이전트의 AAAH 서버로의 인증 절차나 MR 자신의 변경되는 위치 정보를 MR의 홈 에이전트로 바인딩 업데이트 할 필요가 없어, 인증 및 핸드오프의 효율성을 가진다.

3.2.5 또 다른 MAP 도메인으로 AR을 변경하는 경우

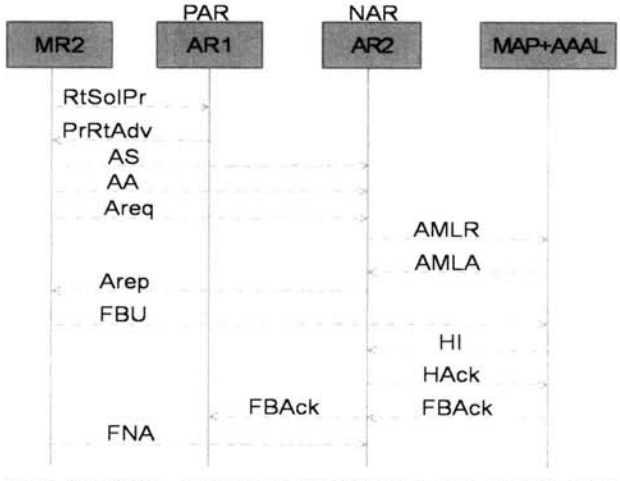
이동 네트워크 MR이 MAP 도메인 경계에서 다른 MAP 도메인으로 이동하는 경우의 인증 및 바인딩 절차를 보여준다. MR3는 현재 접속중인 AR2에게 이동 AP 정보를 얻고자 RtSolPr을 보내고, AR2는 MNP를 포함한 정보를 MR3에게 전송해 준다. MR3는 MNP 정보를 이용해 새로운 위치 정보인 RCoA와 LCoA를 생성한다.

MR3는 이동하고자 하는 다른 도메인의 AR3에게 인증하고자 LC를 long-term SA를 이용해 암호화 해서 CR을 생성한 후 AReq 메시지를 보낸다. AR3는 AAA DIAMETER 메시지 형태로 변환하여 AMR 메시지를 MAP2+AAAL로 전송한다.

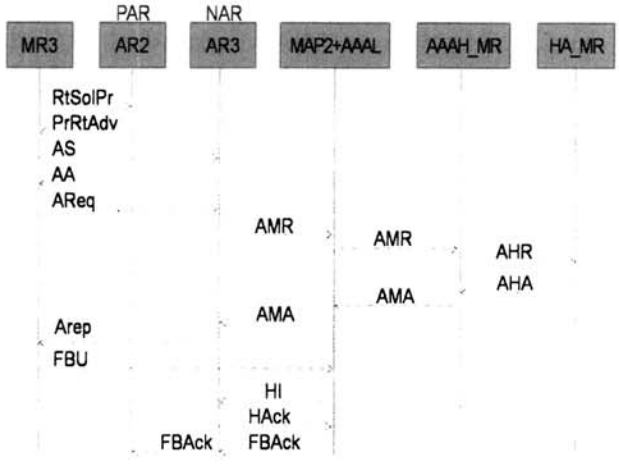
MAP2+AAAL은 NAI를 체크해서 MR이 지역적으로 인증할 수 없는 것을 탐지한 후 AMR 메시지를 MR의 AAAH 서버로 포워딩한다. AAAH 서버는 미리 저장된 SA로 CR을 복호화해서 LC값과 비교해서 인증한다. AAAH 서버는 MR을 성공적으로 인증하면, 두 개의 다이나믹 키를 생성한다. 하나는 외부 도메인에서 지역 내 AAA 절차를 수행 시 사용할 key_local이고, 또 하나는 MR과 MR의 HA와 양방향 터널링에 사용할 key_home이다. MR에서 key_local과 key_home을 구성할 수 있도록 하기 위해서, SP_HOME과 SP_LOCAL을 생성한다. 이 보안 파라미터들은 MR과 AAAH 서버 간 long-term key를 사용해 암호화한다. AAAH 서버는 AHR 메시지를 통해 MR의 NAI와 SP_HOME을 알린다. HA는 SP_HOME을 이용해 key_home을 구조화하고 AHA 메시지로 승인을 알린다. AHA 메시지를 받은 AAAH 서버는 AMA 메시지를 통해 MAP2+AAAL에게 인증 결과를 통보한다. 승인 결과를 받은 MAP2+AAAL은 long-term key를 이용해서 메시지를 복호화한 후 MR의 NAI를 저장하고 key_local을 구성한다. MAP2+AAAL은 AMA 메시지를 AR3에게 전달한다. AR3는 MR



(그림 3.4) 제안3 : MN이 이동 네트워크를 변경하는 경우



(그림 3.5) 제안4 : 동일한 MAP 도메인 내에서 AR을 변경하는 경우



(그림 3.6) 제안5 : 또 다른 MAP 도메인으로 AR을 변경하는 경우

의 인증을 확인하고, SP_HOME, SP_LOCAL, 홈 에이전트 주소 등의 정보를 포함한 ARep 메시지를 MR에게 전달한다.

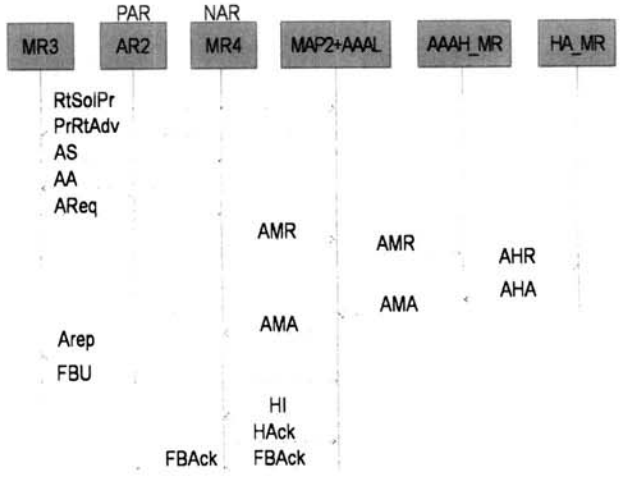
MR은 성공적인 인증을 확인한 후, 생성한 RCoA와 LCoA를 MAP2+AAAL에게 바인딩 업데이트한다. 또한 MR은 RCoA를 자신의 홈 에이전트에게 바인딩 업데이트한다.

3.2.6 또 다른 MAP 도메인 내의 이동 네트워크와 연결되는 경우

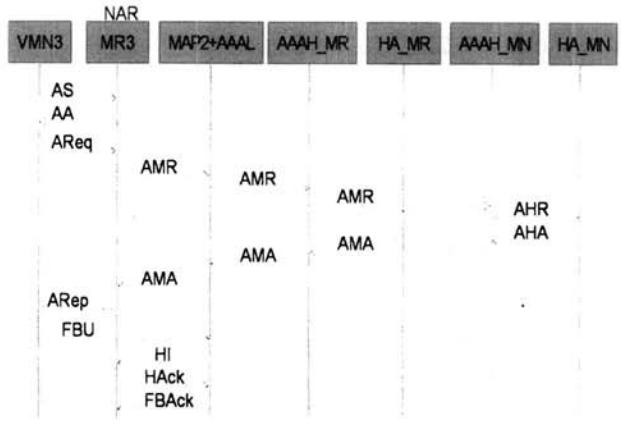
제안 5의 경우와 핸드오프 절차는 거의 같지만, 또 다른 MAP 도메인 내의 이동 네트워크로 이동하는 경우이므로, MR은 RtSolPr 메시지를 MAP2+AAAL에게 전달하고, 받은 MNP정보를 통해 새로운 RCoA와 LCoA를생성한 후 인증 절차를 거친다. 성공적인 인증을 마치면, MAP2+AAAL에게 RCoA와 LCoA를 등록하는 핸드오프 절차를 수행하고, 홈 에이전트에게 RCoA를 바인딩 업데이트 한다.

3.2.7 VMN이 Nested 이동 네트워크에 들어가는 경우

방문 MN이 Nested된 이동 네트워크에 들어가는 경우로, 이전 네트워크 AP로부터 이동할 AP에 대한 정보를 받은



(그림 3.7) 제안6 : 또 다른 MAP 도메인 내의 이동 네트워크와 연결되는 경우



(그림 3.8) 제안7 : VMN이 Nested 이동 네트워크에 들어가는 경우

후, RCoA와 LCoA를 생성한다.

VMN이 MR3에게 인증 요청을 시작하고, AMR 메시지는 MAP2+AAAL로 전해지고 다시 MR의 AAAH에게 전달된다. AMR 메시지를 받은 MR의 AAAH 서버는 이 메시지를 VMN의 AAAH 서버에게 전송한다. VMN의 AAAH 서버는 VMN을 인증한 후 key_home, key_local, SP_HOME, SP_LOCAL을 생성한다. VMN의 HA에게 AHR 메시지를 보내고, VMN의 HA는 승인한 후 결과 메시지를 응답한다.

인증 절차가 성공적으로 수행되면, VMN은 MAP2+AAAL에 RCoA와 LCoA를 바인딩 업데이트하고, VMN의 HA에게 RCoA를 업데이트 한다.

3.3 제안하는 인증 및 핸드오프 단축 절차

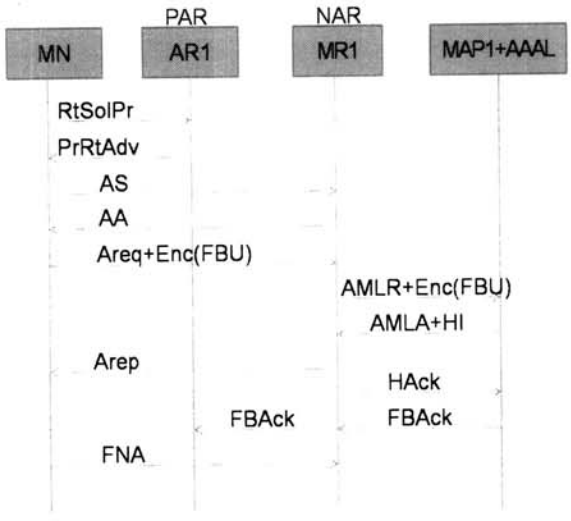
3.2절에서는 NEMO의 7가지 이동 시나리오를 정의하고 이동 시나리오별 AAA를 이용한 인증 및 F+HMIPv6를 접목한 빠른 핸드오프 절차를 제시하였다. 무선 환경의 취약점을 보안하기 위해서 핸드오프 절차 이전에 노드 인증을 먼저 거친후 생성된 키를 통한 안전한 핸드오프 절차를 수행하도록 하였다. 이번 절에서는 시그널링 로드를 좀 더 줄이고자 인증 및 핸드오프 절차를 동시에 진행하는 방식을 제안한다. 이는 안전성과 빠른 핸드오프를 동시에 수행함으로써 효율성을 좀 더 극대화하였다.

NEMO 이동 시나리오 중 MAP 도메인 내에서의 이동 시나리오의 경우와 MAP 도메인간 이동의 경우 두 가지에 대해서 안을 제시한다.

3.3.1 MAP 내에서의 지역 이동

3.2절의 제안1의 경우와 같은 이동 시나리오에서 인증과 핸드오프 절차를 동시에 진행하는 안을 제시한다. 인증 요청 메시지인 AReq를 보낼때, CR을 생성할 때 사용했던 key_local을 이용해서 새로운 위치 정보인 NLCoA를 암호화해서 같이 MR1에게 전송한다. MR1은 DIAMETER로 변환해서 AMLR 메시지를 생성하고, 전달받은 암호화된 주소 정보를 같이 MAP1+AAAL에게 전송한다.

MAP1+AAAL은 key_local로 CR_L을 복호화해서 MN을 인증하고 동시에 Enc(FBU) 메시지를 key_local로 복호화해



(그림 3.9) MAP 내에서의 지역 이동

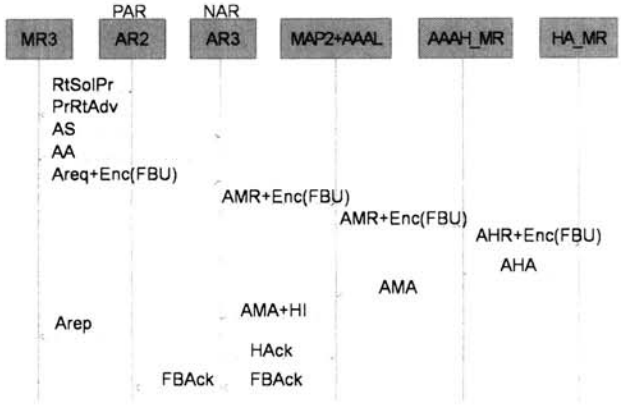
서 NLCoA 정보를 확인한다. 인증 승인 메시지 AMLA와 바인딩 업데이트 정보인 NLCoA를 포함한 HI를 같이 MR1에게 전송한다. MR1은 전송 받은 인증 승인 결과를 ARep 메시지로 MN에게 전송하며, 동시에 NLCoA 유효성 검사 후 HAck을 MAP1+AAAL에게 전송한다. MAP1+AAAL은 NLCoA를 저장하고, 핸드오프 종료 메시지를 AR1과 MR1에게 전송한다.

MAP1+AAAL은 터널을 통해 패킷들을 MR1에게 전송하고, MN이 AR1과 연결을 종료하고 MR1과 연결 후, FNA 메시지를 보내면, MR1은 전송받아 저장하고 있던 패킷들을 MN에게 전송한다.

이는 인증 및 핸드오프 절차를 동시에 진행함으로써 메시지 전송 회수를 줄임과 함께 프로시저 시간을 절감할 수 있는 효과를 볼 수 있다.

3.3.2 MAP 도메인 간 이동

이동 네트워크 MR이 또 다른 MAP 도메인으로 AR을 변경하는 경우의 절차로 인증과 핸드오프를 동시에 진행한다. 이 경우 MR의 홈 에이전트(HA)에게 바인딩 업데이트 하는 과정까지 줄여줌으로써 효율성이 증대된다.



(그림 3.10) MAP 도메인 간 이동

4. 성능 평가

4.1 시스템 모델

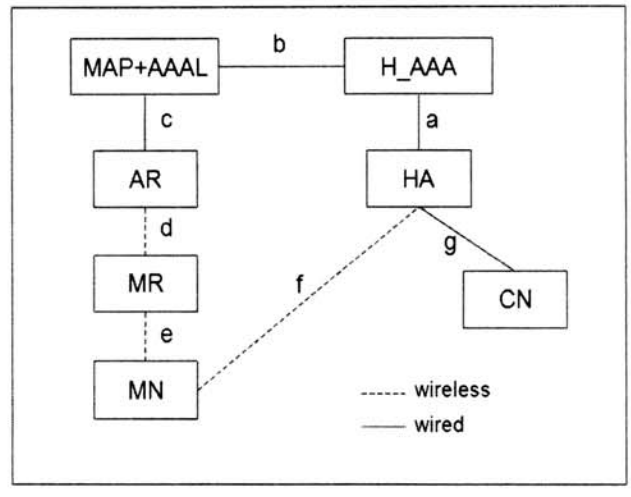
성능 평가 기준은 이동 노드(MN) 또는 이동 라우터(MR)가 이동 시에 홈 등록 절차와 노드 인증 절차를 완료하기까지 과정 동안에 발생하는 비용 산출을 기반으로 한다. 비용은 노드간의 거리와 노드에서의 처리 시간을 비용 산출하였다. 이때 노드간의 거리와 노드의 처리 시간에 대한 단위가 다르므로 노드에서의 처리 시간을 거리로 환산하여 비용 함수를 유도했다. 본 논문에서는 비용 분석을 위해 [12], [13], [14]에서 제안한 접근 방법을 참조하였다.

시스템 모델은 서브 네트워크 간 이동 시 비용 분석을 위해 제안하였으며, (그림 4.1)과 같다. CM은 λ비율로 MN에게 데이터 패킷을 전송하고, MN은 μ비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정한다. MN이 이동할 때마다 CN으로부터 수신되는 평균 패킷수를 PMR(Packet to Mobility Ratio)라고 정의한다. 이동 및 패킷 생성 과정은 독립적이고, 고정적이며, 상당한 시간이 지난 후에도 비슷한 조건으로 돌아가는 것으로 가정하며, PMR은 $p = \lambda/\mu$로 정의한다.

두 호스트 간 거리는 홉(hop) 수로 정한다. 같은 서브 네트워크에 있는 호스트들 간은 1로, 서로 다른 서브 네트워크에 있는 호스트들의 거리는 평가 시 일정한 값 또는 증가하는 값으로 가정한다. 데이터 패킷의 평균 길이는 ld 라고 정의하고, 제어 패킷의 평균 길이는 lc 라 정의하며, 비율은 $l = ld / lc$ 라 정의한다. 본 논문의 분석에서는 ld = 1024 bytes, lc = 100 bytes를 사용한다. 제어 패킷을 전송하는 비용은 송신자와 수신자의 거리에 의해 주어지며 데이터 패킷의 전송 비용은 제어 패킷에 비해 평균 l 배 크다고 정의한다. 그리고 한 호스트에서 제어 패킷을 처리하는 평균 비용은 r 로 정의한다.

4.2 비용 분석

MN이 한 서브넷 네트워크에서 다른 서브넷 네트워크로



(그림 4.1) 비용 분석을 위한 시스템 모델

이동 시 MN의 COA를 HA에 등록하는 핸드오프 과정 및 MN을 인증하는 인증 절차를 거치게 된다. 이때 HA에 등록하기 이전에 보안성을 위해서 노드 인증 과정을 먼저 수행해야 한다. 구하고자 하는 인증 및 핸드오프 비용을 (1)과 같이 정의하며, 인증 비용(C_{Auth})과 핸드오프 비용($C_{handoff}$) 및 인증과 핸드오프 동안 이전 도메인으로 송신되어 손실된 패킷을 재전송하는 비용(C_{oldFA})의 합으로 구성된다.

$$C = C_{Auth} + C_{handoff} + C_{oldFA} \quad (1)$$

일반적인 MN을 인증 및 핸드오프하는 비용은 (2)와 같이 C_g로 정의하며, (그림 4.1)에서와 같이 MN이 H_AAA로 인증(C_{Auth-g}) 및 HA로 CoA를 등록하는 비용($C_{handoff-g}$)을 나타낸다.

$$C_g = C_{Auth-g} + C_{handoff-g} + C_{oldFA-g} \quad (2)$$

노드를 인증하는 일반 비용 C_{Auth-g}는 다음 식으로 표현할 수 있다.

$$C_{Auth-g} = 2(a+b+c+d+e) + 11r \quad (3)$$

노드 이동 시 CoA를 홈에 등록하는 비용은 $C_{handoff-g}$로 (4)와 같다.

$$C_{handoff-g} = 2(a+b+c+d+e) + 11r \quad (4)$$

한 개의 패킷이 CN에서 HA를 통해 MN까지 재전송되는 비용을 C_{dt}라고 하면, 인증 및 핸드오프 지연 동안에 발생하는 이전 도메인으로 전달되는 데이터 패킷의 손실에 따른 재전송 비용($C_{oldFA-g}$)은 인증 및 핸드오프에 소요되는 시간 동안 전송된 패킷에 대한 비용이므로 (5)와 같이 나타낼 수 있다.

$$C_{oldFA-g} = \lambda \times t_{auth-handoff-g} \times C_{dt} \quad (5)$$

$$C_{dt} = l(f+g) + r \quad (6)$$

C_{dt}는 식 (6)과 같이 나타낼 수 있으며, 이는 HA에서 터널링을 통해 CN으로부터 MN으로 전달되는 단일 데이터 패킷의 비용을 의미한다.

인증 및 핸드오프 지연 시간($t_{auth-handoff-g}$)은 식 (7)과 같이 표현할 수 있다.

$$t_{auth-handoff-g} = 4(t_a + t_b + t_c + t_d + t_e) + 22t_r \quad (7)$$

따라서, 일반적인 인증 및 핸드오프 비용인 C_g는 다음과 같다.

$$C_g = 4(a+b+c+d+e) + 22r + \lambda \times t_{auth-handoff-g} \times C_{dt} \quad (8)$$

제안된 절차 중 첫 번째 안인 3.2.1절에 있는 절차의 경우와 같이 홈이 아닌 외부 서브 네트워크내에서 MN의 이동 시 발생되는 전체 비용을 분석하며, 다음과 같이 표현할 수 있다.

$$C_d = C_{Auth-handoff-d} + C_{oldFA-d} \quad (9)$$

노드 MN을 인증하는 비용 $C_{Auth-handoff-d}$는 서브 네트워크 도메인 MAP내에서의 이동이므로 MAP+ AAAL에서만 인증 및 NLCoA 등록 절차를 거치면 된다. 이를 비용으로 표현하면 다음과 같다.

$$C_{Auth-handoff-d} = 3e + 6(c+d) + 10r \quad (10)$$

한 개의 패킷이 CN에서 HA를 통해 MN까지 재전송되는 비용을 C_{dt}라고 하면, 인증 및 핸드오프 지연 동안에 발생하는 이전 도메인으로 전달되는 데이터 패킷의 손실에 따른 재전송 비용($C_{oldFA-d}$)은 인증 및 핸드오프에 소요되는 시간 동안 전송된 패킷에 대한 비용이므로 (11)와 같이 나타낼 수 있다.

$$C_{oldFA-d} = \lambda \times t_{auth-handoff-d} \times C_{dt} \quad (11)$$

C_{dt}는 식 (6)과 같으며, HA에서 터널링을 통해 CN으로부터 MN으로 전달되는 단일 데이터 패킷의 비용을 의미한다.

제안한 안을 위한 인증 및 핸드오프 지연 시간($t_{auth-handoff-d}$)은 식 (12)과 같이 표현할 수 있다.

$$t_{auth-handoff-d} = 3t_c + 6t_d + 6t_e + 10t_r \quad (12)$$

따라서, 제안한 인증 및 핸드오프 비용인 C_d는 다음과 같다.

$$C_d = 3e + 6(c+d) + 10r + \lambda \times t_{auth-handoff-d} \times C_{dt} \quad (13)$$

4.1 절에서 이동 비율을 나타내는 $\rho = \lambda/\mu$ 정의를 이용하여 $\lambda = \rho \times \mu$ 를 식에 대입하고, 제시한 방안에 대한 비용과 일반적인 비용에 대한 비율을 (14)와 같이 정의하여 성능 분석을 시도하였다.

$$\frac{C_d}{C_g} = \frac{3e + 6(c+d) + 10r + \lambda \times t_{auth-handoff-d} \times C_{dt}}{4(a+b+c+d+e) + 22r + \lambda \times t_{auth-handoff-g} \times C_{dt}} \quad (14)$$

제안 3.3 절의 3.3.1의 MAP내에서의 이동 시, 좀 더 최적화된 절차에 대한 비용(C_o) 분석을 수행하도록 한다. 전체 비용은 식 (15)와 같다.

$$C_o = C_{Auth-handoff-o} + C_{oldFA-o} \quad (15)$$

이는 인증 절차와 핸드오프 절차를 동시에 진행하기 때문에 (15)와 같이 표현할 수 있다.

노드 MN을 인증하는 절차와 핸드오프 절차를 동시에 진행할 수 있도록 제안함으로써 비용 $C_{Auth-handoff-o}$는 서브 네트워크 도메인 MAP내에서 MAP+AAAL과 인증 및 핸드오프 절차를 동시에 진행하면 된다.

$$C_{Auth-handoff-o} = 2e + 3(c+d) + 8r \quad (16)$$

인증 및 핸드오프 지연 동안에 발생하는 이전 도메인으로 전달되는 데이터 패킷의 손실에 따른 재전송 비용($C_{oldFA-o}$)은 인증 및 핸드오프에 소요되는 시간 동안 전송된 패킷에 대한 비용이므로 (17)와 같이 나타낼 수 있다.

$$C_{oldFA-o} = \lambda \times t_{auth-handoff-o} \times C_{dt} \quad (17)$$

제안한 안을 위한 인증 및 핸드오프 지연 시간은 식 (18)과 같이 표현할 수 있다.

$$t_{auth-handoff-o} = 3t_c + 3t_d + 2t_e + 8t_r \quad (18)$$

따라서, 제안한 인증 및 핸드오프 비용인 C_o는 다음과 같다.

$$C_o = 2e + 3(c+d) + 8r + \lambda \times t_{auth-handoff-o} \times C_{dt} \quad (19)$$

4.1 절에서 이동 비율을 나타내는 $\rho = \lambda/\mu$ 정의를 이용하여 $\lambda = \rho \times \mu$ 를 식에 대입하고, 제시한 방안에 대한 비용과 일반적인 비용에 대한 비율을 (20)과 같이 정의하여 성능 분석을 하였다.

$$\frac{C_o}{C_g} = \frac{2e + 3(c+d) + 8r + \lambda \times t_{auth-handoff-o} \times C_{dt}}{4(a+b+c+d+e) + 22r + \lambda \times t_{auth-handoff-g} \times C_{dt}} \quad (20)$$

4.3 성능 평가

4.3.1 통신 및 이동성 모델

CN, HA 등 유선 네트워크 연결의 인증 지연을 계산하기 위해서 라운드 트립 시간 분석 결과를 이용하였다.[12] 라운드 트립 시간은 $t_{RT}(h,k) = 3.63k + 3.21(h-1)$이며, k는 패킷의 길이이며 KB단위이고, h는 홉수를 나타낸다. 단방향 시간은 라운드 트립 시간의 절반으로 가정한다. 무선 링크는 $w_{RT}(k) = 17.1k$ 이고, k는 패킷 길이이며 싱글 무선 홉에서의 라운드 트립 지연은 ms로 주어진다.

이동성 모델을 위해서, 잘 알려진 Uniform Fluid Model [13]을 추가적으로 사용하였다. 한 서브 네트워크의 평균 크기는 150m로 가정하고, 보행 속도는 3mph로, μ=0.01, 차량 이동 속도는 평균 60mph로, μ=0.2로 가정한다.

또한, 한 노드에서 통신 비용과 한 메시지의 처리 비용은 같다고 가정한다. (r =1)

같은 도메인 안에서의 거리에 대한 비용은 1(a=c=d=e=1)이고 가까운 두 도메인 간의 거리에 대한 비용(b=f=g)은 일정 비율로 증가하면서 같은 비율로 홉수도 증가하는 것으로 가정한다.

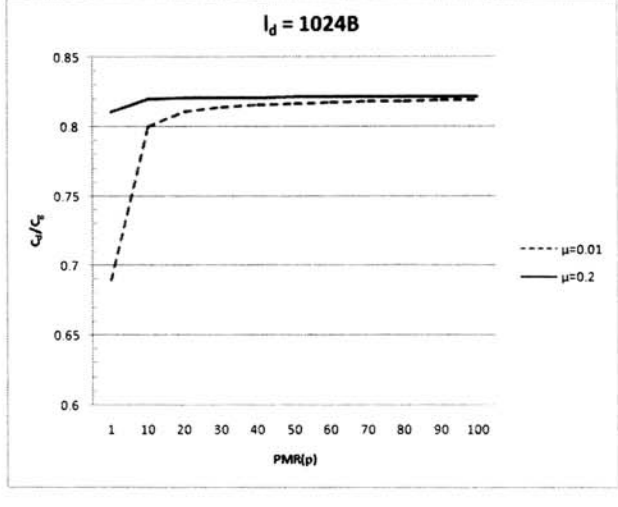
4.3.2 비용 평가

4.3.2.1 PMR 값 변화에 따른 비용 평가

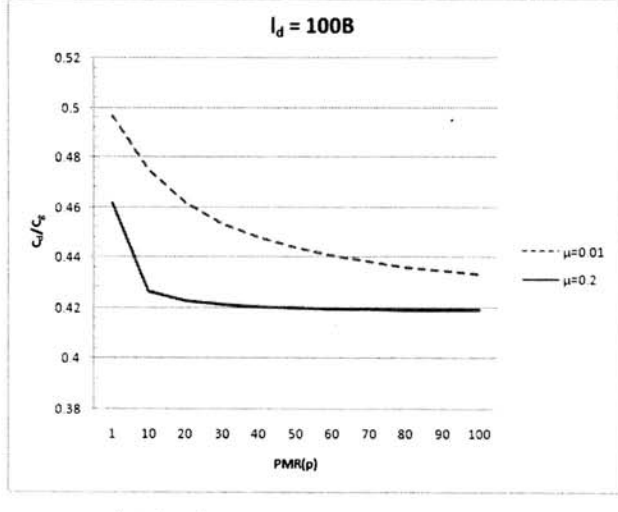
위 절에서와 같은 가정 하에 이동성 PMR 값에 따른 인증 및 핸드오프 비용률(C_d/C_g)을 홉수와 거리에 대한 비용에 따라 구해 보면, 먼저 거리에 대한 비용(b=f=g=3) 및 홉수(h)를 3으로 가정하고 차량 이동률과 보행 이동률에 따라 각각 구해보면 (그림 4.2), (그림 4.3)과 같이 값을 구할 수 있다.

PMR 값은 1에서 100 사이 값을 가지며, PMR 값이 증가함에 따라 ld=1KB의 경우, 보행자 이동의 비율값은 0.819에 가까워지고, 차량 이동체의 비율값은 0.821에 가까워진다. 이 결과는 기존 인증 및 핸드오프 절차보다 대략 1.2배의 비용 효과를 볼 수 있음을 나타낸다.

ld=100B의 경우엔, 보행자 이동의 경우 비율값이 0.433에



(그림 4.2) l_d = 1024B(1KB)의 이동 비용률 (C_d/C_g)



(그림 4.3) l_d = 100B의 이동 비용률 (C_d/C_g)

가까워지고, 차량 이동체의 경우 비율값이 0.418에 가까워진다. 이 결과는 기존 인증 및 핸드오프 절차보다 각각 2.3배와 2.38배 비용 효과를 볼 수 있음을 보여준다.

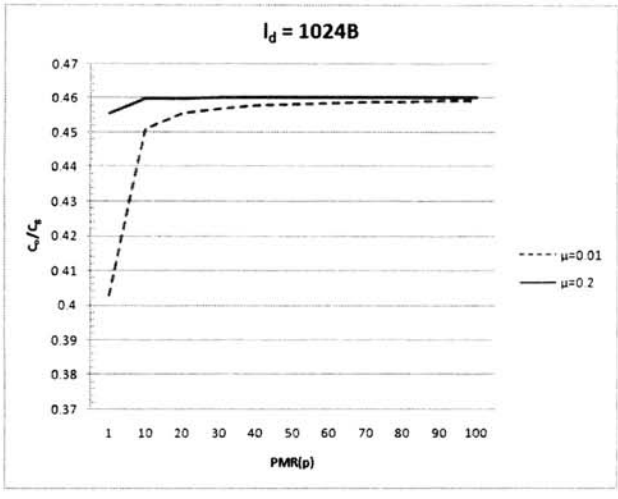
두 번째로 최적화된 방안에 대한 인증 및 핸드오프 비용(C_o/C_g) 분석 결과는 (그림 4.4), (그림 4.5)와 같다.

PMR 값이 증가함에 따라 ld=1KB의 경우 보행자의 이동 비용율은 0.459값에 가까워지며, 차량 이동체 비용율은 0.46에 가까워지며 보행자의 이동 비용률의 값 차이가 근소하다. 비용률 값 0.459와 0.46은 일반 인증 및 핸드오프 비용에 비해 제안한 최적안의 인증 및 핸드오프 비용이 2.17배의 비용 효율성을 가짐을 보여준다.

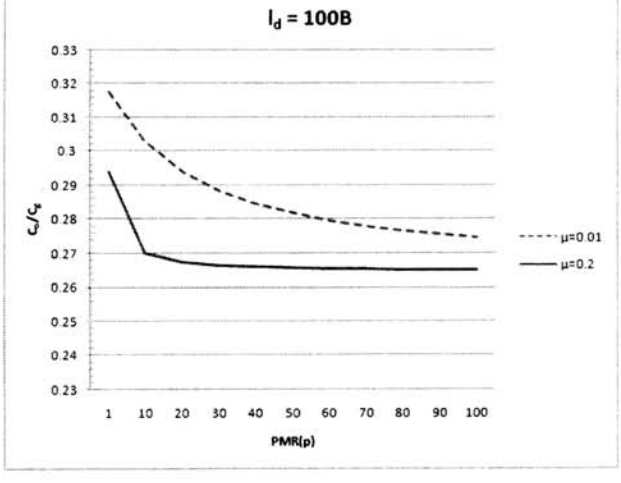
또한, ld=100B의 경우 보행자의 이동 비용율은 0.275에 가까워지며, 차량 이동체 비용율은 0.265에 가까워지며, 이 값은 기존 인증 및 핸드오프 절차에 비해 3.64배와 3.77배의 비용 효율을 나타낸다.

이번엔 거리에 대한 비용(b=f=g=30) 및 홉수(h)를 30으로 가정하고 차량 이동률과 보행 이동률에 따라 각각 구해보면 다음 그림과 같이 값을 구할 수 있다.

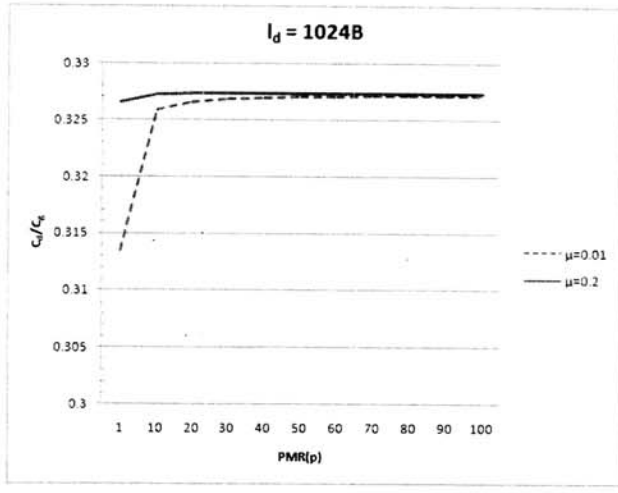
PMR 값이 증가함에 따라 ld=1KB의 경우, 보행자 이동의



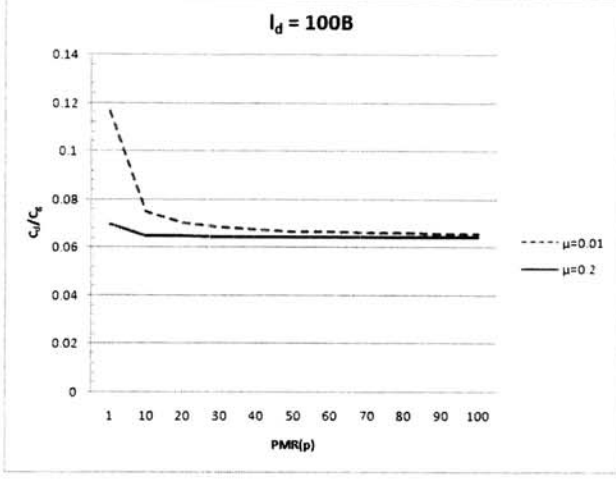
(그림 4.4) l_d=1KB의 이동 비용률 (C_o/C_g)



(그림 4.5) l_d=100B의 이동 비용률 (C_o/C_g)



(그림 4.6) l_d=1024B(1KB)의 이동 비용률 (C_d/C_g), 홉수30



(그림 4.7) l_d=100B의 이동 비용률 (C_d/C_g), 홉수 30

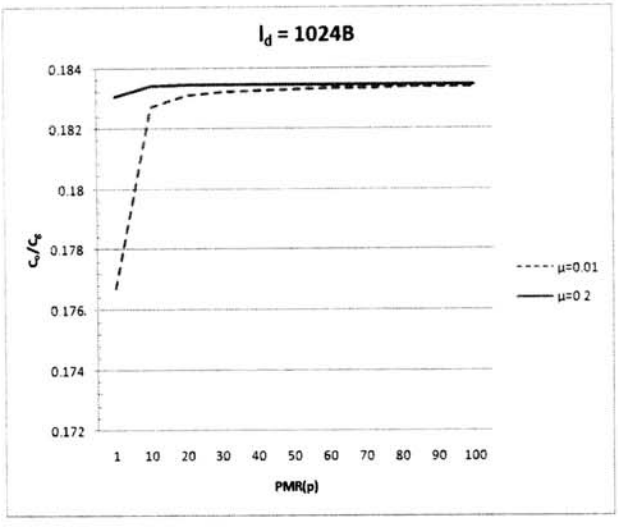
비율값은 0.327에 가까워지고, 차량 이동체의 비율값은 0.327로 보행자 이동 비율값과 거의 같은 값을 가진다. 이 결과는 기존 인증 및 핸드오프 절차보다 대략 3배의 비용 효과를 볼 수 있음을 나타낸다.

ld=100B의 경우엔, 보행자 이동의 경우 비율값이 0.065에 가까워지고, 차량 이동체의 경우 비율값이 0.064에 가까워진다. 이 결과는 기존 인증 및 핸드오프 절차보다 각각 15.2배와 15.5배 비용 효과를 볼 수 있음을 보여준다.

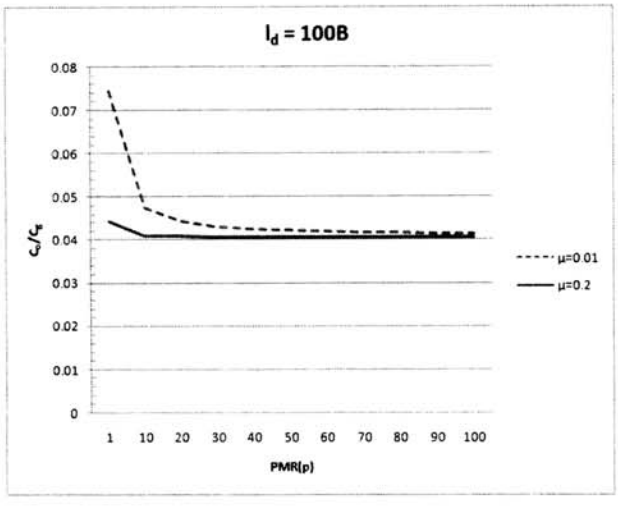
거리 비용 및 홉수가 30인 경우에 최적화된 방안에 대한 인증 및 핸드오프 비용(C_o/C_g) 분석 결과는 다음과 같다.

PMR 값이 증가함에 따라 ld=1KB의 경우 보행자의 이동 비용율은 0.183값에 가까워지며, 차량 이동체 비용율은 0.183으로 거의 같은 값에 가까워지며 보행자의 이동 비용률의 값 차이가 근소하다. 이는 일반 인증 및 핸드오프 비용에 비해 제안한 최적안의 인증 및 핸드오프 비용이 5.45배의 비용 효율성을 가짐을 보여준다.

또한, (그림 4.9)와 같이 ld=100B의 경우 보행자의 이동 비용율은 0.041에 가까워지며, 차량 이동체 비용율도 거의 비슷한 0.04에 가까워지며, 이 값은 기존 인증 및 핸드오프



(그림 4.8) l_d=1KB의 이동 비용률 (C_o/C_g), 홉수 30



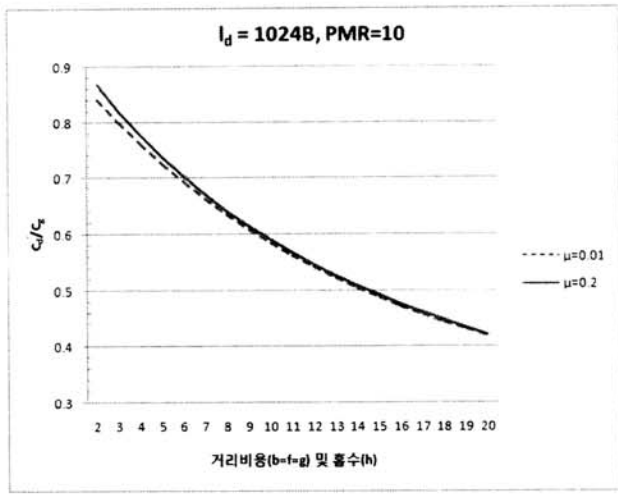
(그림 4.9) l_d=100B의 이동 비용률 (C_o/C_g), 홉수 30

절차에 비해 24.1배와 24.5배의 비용 효율을 나타낸다.

위의 평가들에서 보듯이, 이동성 PMR값의 증가에 따라 각각의 경우들은 일정한 비율값에 수렴하며, 거리비용과 홉 수가 적은 값과 큰 값의 경우를 비교해보면 거리와 홉 수가 클수록 비용 효율성이 크게 좋아짐을 보여준다. 이번 절에서 평가한 결과를 정리하면 다음 <표 4.1>와 같다.

4.3.2.2 홉수 및 거리 변화에 따른 비용 평가

일정한 이동성 PMR 값을 가지며, 거리비용과 홉 수를 일정 비율로 증가하는 경우 비용 효율성 변화를 평가한다.



(그림 4.10) l_d=1024B(1KB), PMR=10의 이동 비용률 (C_d/C_g)

PMR 값이 10과 100인 경우에 대해 ld=1024B인 경우와 ld=100B인 각각의 경우에 대해 평가해 보면, 다음과 같이 값을 구할 수 있다.

이동성 PMR 값이 10이며, ld=1024B의 경우, 거리비용(b=f=g)과 홉 수(h)를 2에서 20까지 증가하면 보행자 이동의 비율값은 0.418에 가까워지고, 차량 이동체의 비율값은 0.421에 가까워진다. (그림 4.10 참조) 이 결과는 기존 인증 및 핸드오프 절차보다 각각 1.84배와 1.83배의 비용 효과를 볼 수 있음을 나타낸다. 홉 수가 점점 증가할 수록 비용률 값은 점차 0에 가까운 값으로 계속 감소함을 보이며, 이는 홉 수의 증가에 따라 비용 효율성도 향상됨을 보여준다.

이동성 PMR 값이 10이며, ld=100B의 경우, 보행자 이동의 비율값은 0.113에 가까워지고, 차량 이동체의 비율값은 0.095에 가까워진다. 이는 기존 핸드오프 및 인증 비용보다 각각 5.33배, 6.5배의 비용 효율성 향상을 나타낸다. (그림 4.11 참조)

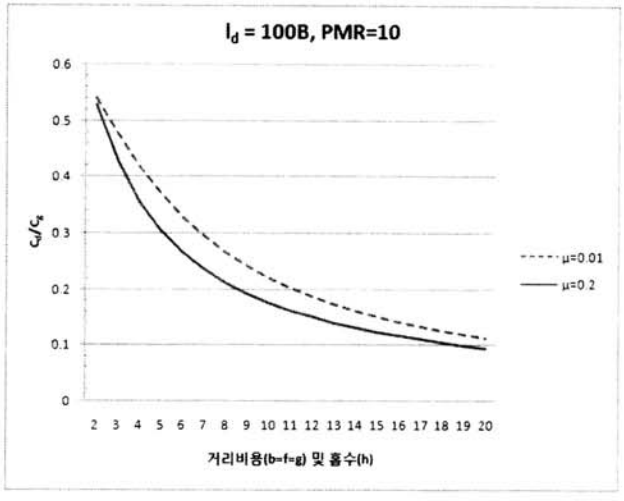
다음은 제안한 최적화 방안의 경우에 대한 비용률 값을 나타낸다.

PMR값이 10이며 ld=1024B인 경우, 홉 수를 2에서 20까지 증가하며 보행자의 경우와 차량 이동체의 이동률에 따른 비용률 값을 구해보면, 보행자 이동률(μ=0.01)은 0.2347값에 가까워지며 차량 이동체의 이동률(μ=0.2)은 0.2359에 가까워지며 이는 각각 4.26배, 4.24배의 비용 효율성 향상을 보여준다. (그림 4.12)를 참조 한다.

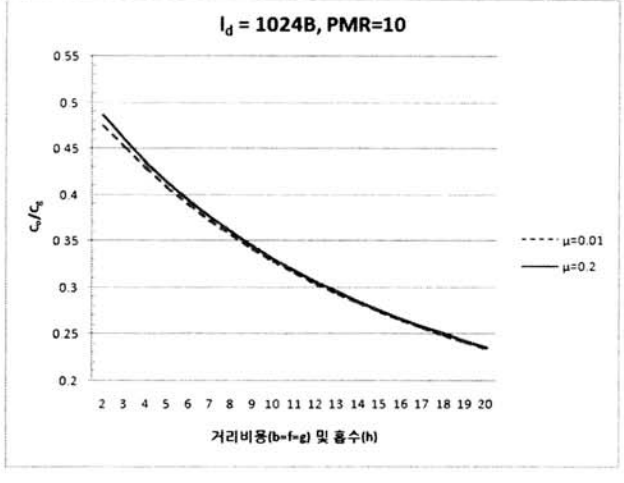
위와 같은 조건하에 ld=100B인 경우, 보행자 이동률은 0.072값을 가지며 차량 이동체는 0.06값을 나타낸다. 이는

〈표 4.1〉 PMR 증가에 따른 비용률

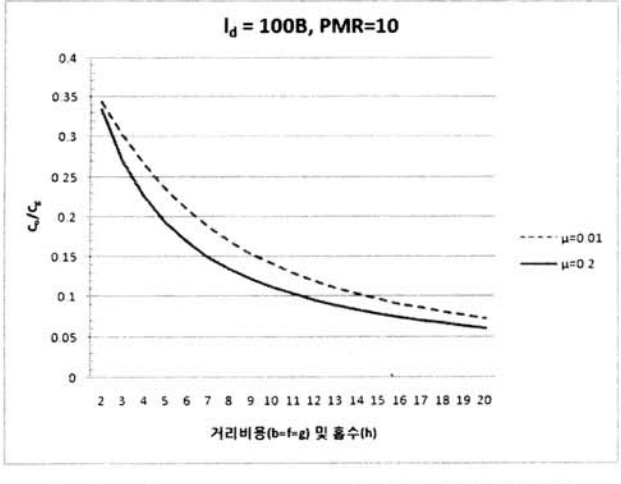
홉 수	ld	Cd/Cg		Co/Cg	
		μ=0.01	μ=0.2	μ=0.01	μ=0.2
3	1024B	0.819162855	0.82127589	0.459325511	0.460247923
	100B	0.433171078	0.418953177	0.274689215	0.265049313
30	1024B	0.32721499	0.327357997	0.065522516	0.064409796
	100B	0.183378924	0.183448413	0.041460795	0.04074297



(그림 4.11) l_d = 100B, PMR = 10의 이동 비용률 (C_d/C_g)



(그림 4.12) l_d = 1024B, PMR = 10의 이동 비용률 (C_d/C_g)



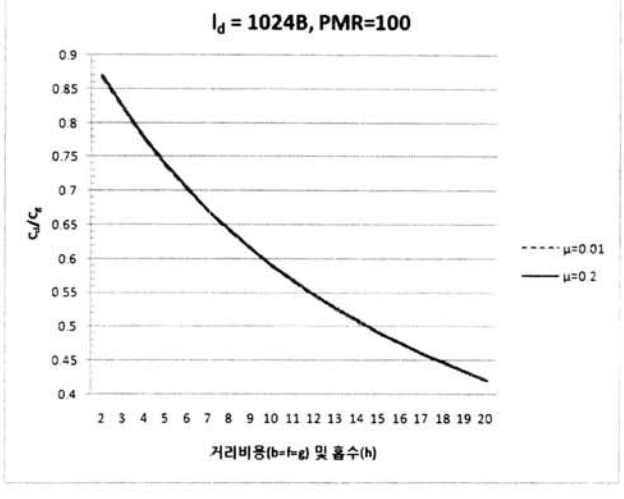
(그림 4.13) l_d = 100B, PMR = 10의 이동 비용률 (C_d/C_g)

13.8배와 16.6배의 비용 효율성 향상을 보여준다. 다음 (그림 4.13)을 참조한다.

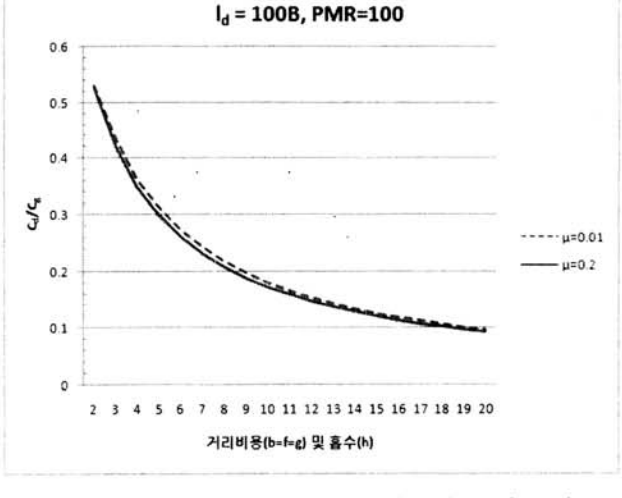
다음은 PMR이 100인 경우에 거리비용 및 홉수 증가에 따른 비용률 변화를 살펴본다. 우선 제안한 안(C_d)에 대하여 비용률 변화 추이를 보면, ld=1024B일 때 보행자 이동률의 경우 0.42값에 가까워지며 차량 이동체의 이동률일 경우엔 0.421에 가까워진다. 즉, 보행자 이동률은 일반 핸드오프 및 인증 비용보다 1.83배 향상 값을 나타내며, 차량 이동체의 이동률은 1.829배 향상됨을 보여준다. (그림 4.14 참조)

ld=100B일때는 앞서보다 더 향상된 값을 나타내는데, 보행자 이동률의 값은 0.096의 근사값과 차량 이동체 이동률의 값은 0.094 근사값을 나타낸다. 이는 기존 핸드오프 및 인증 시 발생하는 비용 대비 각각 6.54배, 6.76배의 비용 효율성 향상 정도를 보여주는 값이다. 이와 관련된 사항은 (그림 4.15)를 참조한다.

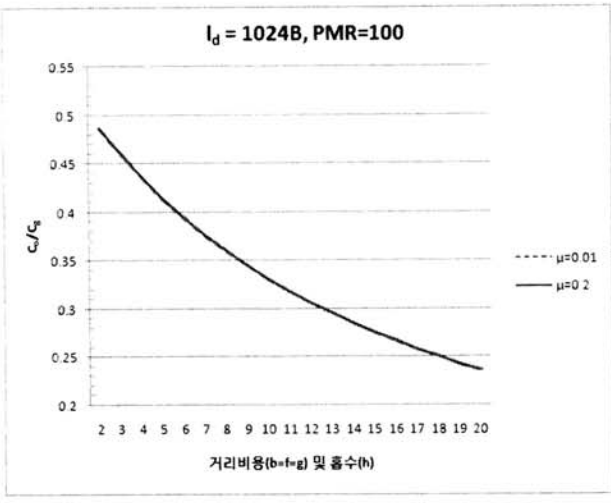
제안한 최적화 방안(C_o)에 대한 PMR이 100인 경우에 거리비용 및 홉수 증가(2~20)에 따른 비용률 변화를 살펴보면, ld=1024B일 때 보행자 이동률의 경우 0.2359값에 가까워지며 차량 이동체의 이동률일 경우엔 0.236으로 보행자 이동률과 거의 근사한 변화 추이를 보인다. 이는 일반 핸드오프 및 인증 비용보다 보행자 이동률은 4.239배, 차량 이동체 이동률은 4.236배 향상 값을 나타낸다. (그림 4.16)을 참조한다.



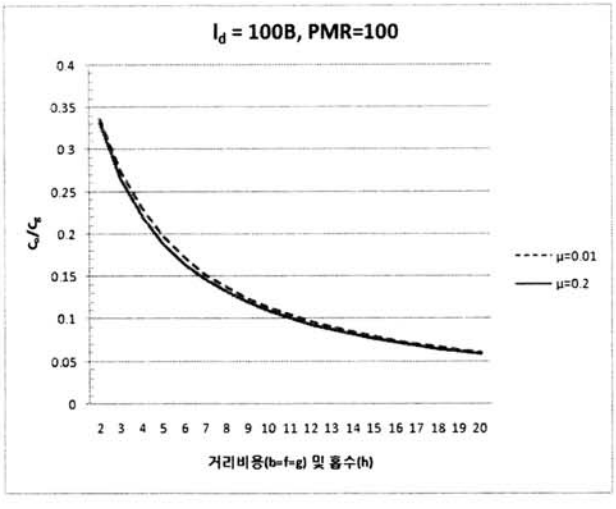
(그림 4.14) l_d = 1024B, PMR = 100의 이동 비용률 (C_d/C_g)



(그림 4.15) l_d = 100B, PMR = 100의 이동 비용률 (C_d/C_g)



(그림 4.16) l_d = 1024B, PMR = 100의 이동 비용률 (C_o/C_g)



(그림 4.17) l_d = 100B, PMR = 100의 이동 비용률 (C_o/C_g)

또한, ld=100B일때는 앞서보다 더 향상된 값을 나타내는데, 보행자 이동률의 값은 0.06에 가까워지며, 차량 이동체 이동률의 값은 0.059에 가까워지며 마찬가지로 비슷한 변화 추이를 보여준다. 이는 보행자 이동률의 경우 16.44배, 차량 이동체 이동률의 경우 16.84배의 비용 효율성 향상 정도를 보여준다. (그림 4.17)을 참조한다.

이번 절에서 평가한 거리비용과 홉 수 증가에 따른 변화 추이를 정리해 보면 다음 <표 4.2>와 같다.

거리비용의 변화나 PMR값의 증감보다 홉 수의 증가가 더 큰 영향을 준다는 점을 위의 비용 평가를 통해 알 수 있다. 홉 수를 20정도까지 비용 평가해 보았지만, 홉 수 값이 증가할 수록 비용률값은 0에 가까워져 비용 효율성이 증가한다.

4.4 안전성 분석

본 절에서는 NEMO에서 발생 가능한 DoS공격과 대응방안에 대해 분석하고자 한다.

첫째, NEMO 표준 관련 문서[15]에는 다음과 같은 BU 메시지 변조에 의한 DoS공격의 위협 분석 내용을 다루고 있다. 기본적으로 NEMO 표준[2]에서는 바인딩 업데이트와 관련된 에러 프로세스에서 에러 상태가 142로 설정되었을 때, Implicit mode인 경우엔 'fatal error'를 의미하고, Explicit mode인 경우엔 'Not Authorized for Prefix'의 경우에 해당한다. 이 때, MR은 같은 종류의 바인딩 업데이트를 같은 홈 링크에 있는 다른 홈 에이전트에게 전송하게 되는데, 만약 홈 에이전트에서 적절한 응답이 없다면 MR은 홈 링크 상에 있는 다른 홈 에이전트에게 보내는 바인딩 업데이트를 제거한다. 또한, 홈 에이전트는 모바일 네트워크에서 라우터 광고(Router Advertisements)와 관련된 프리픽스(Prefix) 광고를 중단해야 하고, 그에 따른 자신의 포워딩 정보들을 수정해야 한다. 다음으로 이 MR은 같은 홈 링크에 있는 홈 에이전트에게 다른 모드(예를 들면, implicit 모드)로 바인딩 업데이트를 보낼 수 있다.

그러나 만약 악의적인 MR이 다른 MR에게 속한 MNP (Mobile Network Prefix)를 요청하며 HA에게 explicit mode로 BU를 보내면, HA는 MNP가 유효하지 않음을 알리고 142 코드와 BA를 보낼 것이다. 이렇게 되면, HA는 해당 MNP에게 광고 메시지 전송을 중단하게 되고 이미 MNP를 사용하고 있는 MR에게는 DoS공격이 수행되게 된다. 또한 악의적인 MR이 HA에게 다른 유효하지 않은 MNP를 보내면, MNP들은 서비스 중단이 발생하게 된다. 그러나 이와 같은 공격은 AAA을 이용한 인증을 통해 악의적인 MR의 BU가 이루어지지 않도록 대응할 수 있다.

둘째, 합법적인 MR의 Care-of-Address를 스푸핑하여 공격하는 MR에 대한 DoS공격 위협이 존재한다[16]. NEMO에서 해당 공격은 다음과 같이 적용 가능하다: 합법적인 MR이 prefix MNP를 갖고 있고 공격자 MR은 다른 prefix를 갖고 있으며 둘 다 같은 HA에 속해있다. 각 MR은 HA와

〈표 4.2〉 거리비용 및 홉 수 증가에 따른 비용률

PMR	ld	Cd/Cg		Co/Cg	
		μ=0.01	μ=0.2	μ=0.01	μ=0.2
10	1024B	0.418537526	0.42105483	0.234757514	0.235965348
	100B	0.113783389	0.094913879	0.072241522	0.06005348
100	1024B	0.420920813	0.421175593	0.235901045	0.236023291
	100B	0.096086206	0.093838299	0.060810701	0.059358751

key를 공유한다. 공격자 MR은 바인딩 캐쉬에서 HA가 MNP를 합법적인 MR의 홈 어드레스 대신에 자신의 홈 어드레스로 추가하도록 지정할 수 있다. 그러므로 공격자 MR에게 향하도록 MNP에 모든 트래픽이 리다이렉팅 되도록 함으로써 합법적인 MR에게 서비스 거절하는 공격이 이루어진다. HA가 IPSec을 사용하더라도, 공격자 MR이 합법적 MR의 MNP를 요구하는 것에 대해 방어되지 않는다. 하지만 AAA를 이용한 인증을 통해 공격자 MR이 공격 대상 MR의 홈 어드레스를 지정하는 것을 막을 수 있다.

셋째, 중첩 이동 네트워크에서 DoS공격 위협이 존재한다[16]. 여러 이동 네트워크는 중첩된 이동 네트워크를 구성하여 다른 네트워크 하위로 접속할 수 있다. 일반적으로 최상위 수준에 있는 MR은 모든 이동 네트워크에 접속된 트래픽을 전달하게 되어 레벨의 단계가 커지면, 최상위 수준에 있는 MR에 부하를 주게 된다. 이를 악용하여 DoS공격이 가능하다. 이에 대응하기 위해 이동 네트워크에 중첩되는 레벨의 수를 제한하는 것이 필요하다. 이는 Tunnel Encapsulation 옵션을 모바일 네트워크 하위 레벨 수를 제한하도록 설정함으로써 가능하고, 중첩 이동 설정은 모바일 호스트가 모바일 네트워크를 방문할 때도 해당된다. 그러나 모든 모바일 호스트들이 항상 같은 레벨에 속하게 되지는 않는다. 모바일 네트워크에서 모바일 호스트가 추가될 때 한 레벨 이상 중첩되지 않도록 설정하는 것은 불가능하다. 따라서, 위에서 언급된 중첩 설정에 대한 위협은 모바일 호스트가 추가되는 경우에는 해당하지 않는다.

마지막으로 멀티 홈 이동 네트워크에서의 MR에 대한 DoS공격 위협이 있다[17]. MR은 이동성을 갖기 때문에, 링크 접속은 항상 무선 채널을 이용하므로 간단한 채널 재밍(jamming)에 의한 DoS공격이 가능하다. 그리고 MR에 대한 패킷 플러딩은 이동 네트워크에서 일반 서비스가 불가능하도록 유도할 수 있다. MR은 바인딩 업데이트 목록과 홈 에이전트 목록을 유지한다. 만약 어떤 악의적인 노드들이 바인딩 업데이트 정보를 갖는다면 또는 라우팅 최적화 요청을 CN에게 보낸다면, MR은 이런 데이터 구조에서 오버플로우 될 수 있다. 이런 DoS공격은 MR의 데이터 구조와 관련된 바인딩에서의 DoS공격으로 분류될 수 있다. 이런 공격을 예방하기 위해서, 데이터 구조는 요청 노드에 대한 검증 후에 업데이트 되어야 한다. 그리고, 바인딩 업데이트 목록에서 이미 지난 바인딩 업데이트 정보를 효율적으로 관리되어야 한다. 이를 위해서 AAA를 이용한 노드 검증을 통해 바인딩에서 DoS공격을 예방할 수 있다. AAA를 이용한 인증뿐만 아니라 권한부여(Authorization) 기능을 이용하게 되면 서비스 접속을 위해서 접속 권한을 얻어야만 하기 때문에, Authorization 서버에 대한 DoS공격을 예방할 수 있다[18].

위와 같이 NEMO에서 가능한 DoS공격과 이에 대한 대응 방안들을 검토해 보았다. 하지만, AAAL, AAAH서버에 대한 DoS공격은 여전히 가능하며 이는 추가적인 공격 대응 방안들을 사용함으로써 대응 가능하다. 이에 적용 가능한 방안들로는 첫째, 특정 서버에 대한 DDoS공격 피해를 완화하는 목적으로 오버레이 라우팅을 이용해 정상 서비스 트래픽 포워딩의 랜덤화와 익명성을 높인 SOS구조와[19], 둘째, DoS공격에 대비한 자원 재할당 및 서버 중복 방안[20]이 있다. 후자의 경우 컴퓨팅 노드의 자원을 고갈시켜서 본래 의도한 서비스 제공을 방해하려는 DoS공격에 대한 대응 방안으로, 첫 단계는 한 컴퓨팅 노드 내에서 선택된 필수 서비스에 대해 자원을 동적으로 할당하여 공격이 성공한 후에도 필수 서비스가 유지될 수 있도록 한다. 이 조치에도 불구하고 노드 내에서의 충분한 자원 확보가 불가능해지면 두 번째 단계로 미리 준비된 다른 컴퓨팅 노드에서 사용자에게 투명하게 필수 서비스가 제공될 수 있도록 중복성을 적용할 수 있다.

이상과 같이 NEMO 구조에서도 다양한 DoS공격에 대한 취약점을 가지고 있다. 이에 본 논문에서 제시한 AAA서버 인증 구조에 의해 어느 정도 대응 가능함을 알 수 있고, 다만 AAA서버 자체에 대한 DoS공격은 기존에 제안된 서버에 대한 DoS공격 대응 방안을 추가로 적용하여 대응 가능하다.

5. 결 론

본 논문에서는 NEMO의 다양한 이동 환경에서 발생할 수 있는 여러 시나리오 중 7가지 시나리오를 채택하고, 각 시나리오별 F+HMIPv6와 AAA인증 방안을 동시에 적용한 절차를 정의함과 동시에 좀 더 효율적인 성능 향상을 위해 인증과 핸드오프를 병행 진행하는 최적화된 방안을 제안하였다. 이를 통해 이동 네트워크에서의 이동 라우터 혹은 이동 노드가 외부 네트워크에서의 이동 중 발생하는 홈 등록을 효율적으로 수행하며, 동시에 인증을 먼저 수행함으로써 안전성을 강화해서 홈 등록 과정 또한 보안성을 강화한 형태로 수행할 수 있는 방안을 제시하였다. 외부 네트워크에서 한 서브네트워크 내에서의 이동 발생 시, MAP+AAAL에게 인증 및 홈 등록의 위임을 통해 먼저 제시한 안의 경우, PMR이 증가하고 거리비용 및 홉 수가 일정한 값을 가질 때, 각각 1.2배, 2.3배 효율성 향상과 최적화한 안의 경우는 이보다 향상된 2.17배, 3.7배의 효율성 향상의 성과를 보여준다.

또한, PMR은 일정한 값을 유지하고 거리비용 및 홉 수의 값(2~20)을 증가하는 경우에 먼저 제안한 안은 1.84배, 6.6배의 비용 효율성 향상 및 최적화 안의 경우는 이보다 훨씬 향상된 4.25배, 16.6배 향상된 성과를 보인다. 홉 수가 20이상 값으로 증가하는 경우 효율성 향상은 더더욱 좋아짐을 보인다.

빠른 혹은 빈번한 이동성에 맞춘 빠른 핸드오프와 인증을 무엇보다 필요로 하는 이동 네트워크(NEMO)에서의 이를 해결하기 위한 인증 및 핸드오프 통합 방안을 제시함으로써 이동 네트워크 환경에서의 효과성과 보안성 향상을 제고할 수 있었다.

참 고 문 헌

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, , IETF, June, 2004.

[2] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility(NEMO) Basic Support Protocol", RFC 3963, IETF, January, 2005.

[3] R. Koodli, "Fast Handover for Mobile IPv6", RFC 4068, IETF, July, 2005.

[4] H. Soliman, C. Castelluccia, K. El-Malki, L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, IETF, Augus,t 2005.

[5] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", RFC 2977, IETF, October, 2000.

[6] F. Dupont, J. Bournelle, "AAA for Mobile IPv6", draft-dupont-mipv6-aaa-01.txt," Internet draft, IETF, November, 2001.

[7] T. Kwon, S. Baek, S. Pack, Y. Choi, "AAA for NEMO", draft-kwon-aaa-nemo-00.txt, Internet draft, IETF, July, 2005.

[8] Hee Young Jung, SeokJoo Koh, "Fast Handover Support in Hierarchical Mobile IPv6", The 6th International Conference on Advanced Communication Technology, Vol.2, pp.551-554, February, 2004.

[9] 김미영, 문영성, "AAA기반의 인증을 이용한 HMIPv6 성능 개선 기법", 정보과학회논문지, 제32권 제5호, 2005.

[10] SeungJoon Choi, Dong SU, Sang-Jo Yoo, "Handover Mobility Scenario Classification and Fast Handover Performance Analysis in NEMO Network", 한국통신학회논문지, Vol.31, No.11B, November, 2006..

[11] Kyung Taeg Rho, "Multicast Handoff Scheme for Network Mobility with Hierarchical Mobile IPv6", 한국컴퓨터정보학회 논문지, September, 2004.

[12] R. Jain, T.Raleigh, C. Graft and M. Bereschinsky, "Mobile Internet Access and QoS Guarantees Using Mobile IP and RSVP with Location Registers", in Proc, ICC'98 Conf, pp.1690-1695.

[13] Thomas, R., H. Gilbert and G. Mazzioto, "Influence of the mobile station on the performance of a radio mobile cellular network", Proc. 3rd Nordic Sem., paper 9.4, Copenhagen, Denmark, September, 1988.

[14] 김미영, 문영성, "Mobile IPv6에서 AAA를 이용한 이동 노드와 홈 에이전트간의 최적화된 인증 방안", 정보과학회논문지, 제30권 제6호, 2003.

[15] Souhwan Jung, Fan Zhao, S. Felix Wu, UC Davis, HyunGon Kim, SungWon Sohn, "Threat Analysis on NEMO Basic Operations", draft-jung-nemo-threat-analysis-02, IETF, February, 2004.

[16] A. Petrescu, A. Olivereau, C. Janneteau, H.-Y. Lach, "Threats for Basic Network Mobility Support (NEMO threats)", draft-petrescu-nemo-threats-01.txt, IETF, January, 2004.

[17] Seongho Cho, Jongkeun Na, Chongkwon Kim, Sungjin Lee, Hyunjung Kang, Changhoi Koo, "Threat for Multi-homed Mobile Networks", draft-cho-nemo-threat-multihoming-00, IETF, February, 2004.

[18] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, "AAA Authorization Framework", RFC 2904, IETF, August, 2000.

[19] Angelos Keromytis, Vishal Misra, Dan Rubenstein, "SOS: An Architecture for Mitigating DDoS Attacks," IEEE Journal on Selected Areas in Communications (JSAC), Vol.22, No.1, January, 2004.

[20] 민병준, 김성기, 나용희, 이호재, 최중섭, 김홍근, "서비스 거부 공격에 대비한 자원 재할당 및 서버 중복 방안", 한국정보처리학회논문지A, Vol.10-A, No.1, pp.7-14, March, 2003.

최 경

e-mail: cbk0907@gmail.com

1995년 연세대학교 전자계산학과(학사)

1994년~1996년 동서증권

1996년~1999년 동아정보처리학원

1999년~2000년 세진직업전문학교

2000년~2002년 (주)청우FBS

2002년~2003년 (주)미래넷

2003년~2006년 (주)안랩시큐브레인

2008년 이화여자대학교 정보과학대학원 인터넷기술전공(석사)

2008년~현 재 이화여자대학교 컴퓨터공학과 박사과정

관심분야 : 서버 보안, 네트워크 보안, NEMO(Network Mobility) 보안, 유비쿼터스 컴퓨팅 보안

김 미 희

e-mail: mihui.kim@ewha.ac.kr

1997년 이화여자대학교 전자계산학과(학사)

1999년 이화여자대학교 컴퓨터학과(석사)

1999년~2003년 한국전자통신연구원 연구원

2003년~2007년 이화여자대학교 컴퓨터학과 (박사)

2007년 ~ 2008년 이화여자대학교 컴퓨터공학과 전임강사

2009년 ~ 현 재 North Carolina State University the department of computer science visiting scholar

관심분야 : 네트워크 보안, NEMO(NEtwork MObility) 보안, 센서 네트워크 보안, 유비쿼터스 네트워크 보안

채 기 준

e-mail: kjchae@ewha.ac.kr

1982년 연세대학교 수학과(학사)

1984년 미국Syracuse University 컴퓨터학과 (석사)

1990년 미국 North Carolina State University 컴퓨터공학과(박사)

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현 재 이화여자대학교 컴퓨터학과 교수

관심분야: 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석, 센서 네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅