VPN 환경에서 Mobile IPv6 노드의 이동성 제공을 위한 AAA 기반의 인증

(Authentication using AAA for the Mobility Support of Mobile IPv6 Nodes in VPN Environments)

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

요 약 기업의 서비스 망은 DMZ(De-Militarized Zone)를 기준으로 인터넷과 인트라넷으로 분할된다. Mobile IP 의 설계 철학은 망의 토폴로지 및 서비스 형태와 무관하게 지속적인 이동성 제공을 위한 투명성을 제공하는 것이다. 그러나 기존의 기술 사양에서는 이러한 사설망으로의 원활한 로밍을 제공하지 못한다. 즉, 로밍 시 보안 정책 수용을 위한 다양한 접근 방법을 수용하지 못한다. 본 논문에서는 인터넷에 있는 기업 사용자가 VPN(Virtual Private Network) 게이트웨이를 통한 인트라넷 엑세스를 가능하도록 하기 위해 AAA(Authentication, Authorization, Accounting) 인프라 기반의 인증 및 세션 키 교환에 관해 기술하고 제안된 방식에 대한 성능 분석결과를 제시한다.

키워드 : Mobile IPv6, AAA, Authentication

Abstract The enterprise service network is composed of internet, intranet and DMZ. The design rationale of Mobile IP is providing of seamless mobility transparency without regarding to the type of network topology and services. However, Mobile IP specification does not include the mobility support in case of using VPN environment and define the access scenarios to get into the VPN intranet without disturbing existing security policy. In this paper, we propose an authentication method using AAA infrastructure and keying material exchange to enable an user in internet to be able to access the intranet through the VPN gateway. Finally, performance analysis for the proposed scheme is provided.

Key words : Mobile IPv6, AAA, Authentication

1. 서 론

무선 랜(IEEE 802.11)이 핫스폿 지역에 설치되고 핸드폰 등 이동 단말을 이용한 인터넷 엑세스가 잦아짐에 따라 기업 이동 사용자에 대한 서비스 지역성에 대한 경계가 확장되고 있다. 기업 사용자가 사설 망 내부에서 외부로 로밍 하는 경우 사설 망 내부의 자원에 대한 지속적인 연결을 제공받기 위해서 내부의 홈 에이전트와의 연결성이 보장 되어야 하며, 이때 VPN의 보안 정책을 반드시 만족해야만 한다[1]. 외부에서 사내 망으로 접속을 원하는 경우, 이동 단말은 우선 외부 망에 대한 인증을 완료하고 사내 망으로의 접근이 가능한지 여부를 확인하기 위한 별도의 인증 과정을 수행해야 한다. 이를 위해 유무선망의 사용자 인증 서비스의 대표적 인프라인 AAA가 사용된다[2,3]. AAA는 인증, 권한 부여 및 과금을 위한 보안 및 확장성을 제공하는 인프라로서, 기업 사용자에 대한 인증 요구를 충족시킬 수 있다.

본 논문에서는 VPN 환경에서 Mobile IP가 공존하는 상황에서 Mobile IP의 현재 기술상의 문제점을 분석하고 VPN 환경 하에서도 기존의 이동성을 제공하기 위한 다양한 접근 시나리오를 제공하였다. 이를 위해 VPN 통과를 위한 요구 사항을 정리하고 문제점을 분석하였으며, 다양한 설치 시나리오 소개 및 각 시나리오별 장단점을 분석하였다. 먼저 Mobile IPv6(Internet Protocal version 6) 상에서 AAA 인프라를 사용한 인증 모델 및 엔티티를 정의함으로써 외부 인터넷 망에서 기

· 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2004-005-D00147)
† 정 회 원 : 숭실대학교 정보미디어기술연구소
mizero31@sunny.ssu.ac.kr
†† 종신회원 : 숭실대학교 컴퓨터학부
mun@computing.ssu.ac.kr
논문접수 : 2004년 12월 6일
심사완료 : 2006년 2월 2일

업 내부 망으로의 접근을 위한 AAA 기반의 인증 및 세션 키 분배에 관해 기술하고 로밍 사용자를 위한 기업 내부 홈 망의 인증 및 접근 시나리오를 제공하며, 제안된 방식에 대한 알고리즘 및 성능 분석 결과를 제시한다.

2. VPN 환경에서의 AAA 인증 모델 및 엔티티

그림 1은 VPN 게이트웨이를 사용하는 기업 망 환경에서, 이동 노드가 인터넷 상에 있는 외부 망으로 이동한 경우 해당 망과 이동 노드간의 상호 인증을 가능하게 하고, 인트라넷 내부에 존재하는 홈 에이전트로 바인딩 등록을 성공적으로 처리하고 상대 노드와의 통신을 재개할 수 있도록 해 주는 AAA, Mobile IP 및 VPN의 서비스 통합을 위한 모델 및 역할에 의해 정의되는 각 엔티티를 나타낸다.

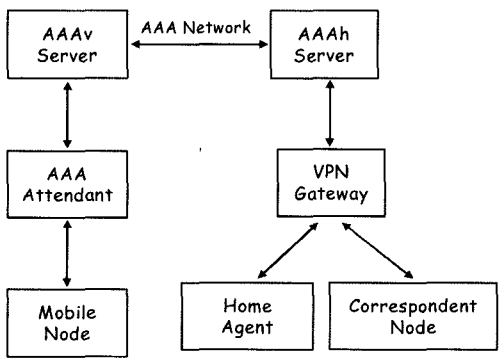

그림 1 VPN AAA 인증 모델

이동 노드는 MIPv6에서 정의한 이동 노드의 기능을 가지는 노드로서 외부로의 로밍 시 외부 링크 및 노드 인증을 위해 NAI(Network Address Identifier)[4], 홈 주소 등의 인증 정보를 제공하며 [5]에서 정의한 모든 기능을 만족한다. Attendant는 이동 노드가 외부 링크에 접속한 후(Association) 인증을 위한 최초의 통신을 담당하는 AAA 엔티티로서 노드로부터 인증 정보를 받아서 로컬 AAA 서버로 릴레이를 하고 결과를 처리한다. 802.1x 표준에서 정의하고 있는 포트제어 기능을 구현한 엔티티로서 이동 노드 패킷의 통과 여부를 결정하는 패킷 제어 정책 및 엑세스 리스트를 유지하고 있다. AAAv(Authentication, Authorization, Accounting visited)는 외부 링크 사용을 위한 인증 서버로서 이동 노드가 이동 후 외부망의 자원의 사용 여부를 결정하는 엔티티이다. AAAv는 외부 링크의 AAA(DIAMETER) 인증 서버로서 이동 노드로부터 인증 요청을 수신하면 먼저 Attendant를 인증하고 메시지의 NAI나 홈 주소를 통해 이동 노드의 홈 도메인에 존재하는 AAA 인증 서버로 전송한다. AnT(AAAh and Tunneling)는 이동 노드의 홈 AAA 서버로서 인터넷 상에 존재하며 VPN 게이트웨이와의 사전에 정의된 IPsec-ESP(Internet Protocol security-Encapsulating Security Payload) 터널을 갖는다. 사전에 협의된 로밍 계약에 따라 AAAv의 인증 요청을 처리하고, 노드 인증 확인 응답을 해 준다. 또한 인트라넷으로의 진입을 위한 엔티티로서 노드가 이동시 매번 IKEv1(Internet Key Exchange version 1)/IKEv2(Internet Key Exchange version 2) 교환을 통해 IPsec-ESP협상을 수행할 필요 없이 AnT 엔티티가 사전에 미리 구성한 IPsec-ESP 협상키를 제공함으로써, 이동시 발생하는 빈번한 키 협상 오버헤드를 줄이며, 안전하게 패킷을 암호화할 수 있도록 해준다. 이동 노드가 다른 망으로 로밍을 한 경우, 이동 노드는 자신의 현재 위치를 파악할 필요가 있다. 이는 인트라넷 내부와 인트라넷 외부의 존재 여부에 따라 홈 망의 자원에 대한 엑세스 방식이 달라지기 때문이다. x-HA (external-Home Agent)[6]는 이러한 위치 파악을 위한 기준점으로서 인터넷 상에 존재 한다. 이동 노드는 이동시 x-HA로 바인딩 갱신을 시도하며, 성공하는 경우 노드의 현 위치는 인터넷 상으로 결정된다. 만일 실패한다면 이동 노드는 인트라넷 내부에 존재하게 된다[6]. VPN 게이트웨이는 인트라넷으로의 진입을 위한 보안 엔티티로서 외부로부터의 허용된 패킷에 대해서만 통과시킬 수 있는 보안 정책을 가진다. 일반적으로 IPsec-ESP 터널 협상에 의해 허용된 소스로부터의 패킷만 통과시킬 수 있다. AnT 엔티티와 사전에 미리 IPsec-ESP 터널을 구성하고 있으며 AnT 엔티티로부터의 모든 패킷을 수용한다. 보안 정책에 의해 주기적으로 AnT 엔티티와 키를 재협상할 수 있으며, IPsec-ESP 터널을 재구성할 수 있다. i-HA[6]는 이동 노드의 내부 홈 망에 존재하는 홈 에이전트로서 이동 노드가 인트라넷에 존재하는 경우 일반적인 홈 에이전트 기능을 처리한다. 이동 노드가 외부 인터넷에 존재하는 경우 노드의 현 위치를 파악하기 위한 기준 엔티티로 사용된다. 이동 노드는 i-HA로 바인딩 갱신 메시지를 보내는데 만일 i-HA(internal-Home Agent)[6]로부터 바인딩 응답이 오면 노드의 현 위치는 인트라넷 내부로 결정 된다. 마지막으로, CN은 이동 노드와 세션을 유지하고 있는 노드로서 인트라넷 내부의 노드이거나 인터넷 상의 노드일 수 있다. 이 논문에서는 이동 노드가 인트라넷 내부의 자원에 접근하는 경우를 기술한다.

3. VPN 환경에서의 이동 노드 인증 및 홈 등록

이동성 제공을 위한 기술인 Mobile IP에서는 VPN

환경 하에서의 이동성을 직접 제공하지 못한다. 이는 이동 노드가 이동 중에 임시로 할당하는 CoA(Care of Address)에 대한 SA(Security Association)를 사전에 제공하지 않기 때문이며, 이동 노드가 빈번하게 이동하는 경우 IKE등의 프로토콜을 통해 매번 IPsec-ESP 터널 구성을 위한 키 협상을 해야 하므로 단말의 부하가 증가하게 된다. 이 장에서는 이동 발생 시 안전하게 이동 노드를 인증하고 이동 노드의 홈 망(VPN 내부 인트라넷)에 있는 홈 에이전트로의 성공적인 바인딩 등록을 위한 방법을 제안한다.

3.1 배경

이동 노드가 기업 망 가입자이고 기업 인트라넷으로부터 외부의 인터넷으로 이동하는 경우 Mobile IP 기술 사양에 의해 이동 노드가 외부 망에서 구성한 CoA를 자신의 홈 에이전트로 위치 등록해야 한다. 그러나 VPN 게이트웨이가 설치된 경우, VPN 게이트웨이로 패킷을 통과시키기 위해서는 VPN 게이트웨이에서 설정한 보안 정책을 만족해야 하는데, 이동 노드의 CoA는 일반적으로 VPN 게이트웨이의 보안 정책을 만족하지 못하고[1,6], 이동 노드가 동적인 SA 설정을 위해 빈번한 이동 발생 시마다 새로 IKE 절차를 시작하고 터널을 구성해야 하므로 이동 노드로서는 상대적인 부하가 증가하게 된다. 따라서 인터넷 상에 고정된 엔티티를 두고 그 엔티티와 VPN 게이트웨이 간에 고정적인 터널을 구성하도록 함으로써 이동 발생 시 이동 노드는 그 엔티티에 MIP 터널을 통해 패킷을 전송하도록 하면, 직접적으로 VPN 게이트웨이와의 IPsec-ESP 터널을 구성할 필요가 없으므로 이동 발생에 대한 IKE 교환 및 IPsec-ESP 터널 처리 비용이 제거된다[6]. 그러나 [6]에서 정의하고 있는 방식은 인증에 관한 해결책을 제공하지 못하고 있다. 이에 본 연구에서는 터널 프록시 역할과 AAA 홈 서버 역할을 통합한 'AnT(AAAh+Tunneling) 엔티티를 정의함으로써, DIAMETER 기반의 성공적인 인증 및 이동 노드 대신 IPsec-ESP 터널 구성을 담당하도록 하여 이동 노드의 처리 부하를 줄이는 방안을 제안하였다.

3.2 관련 연구

[6]에서는 이동 노드의 위치에 따른 엑세스 모드를 정의하고 있다. 먼저 이동 노드가 인트라넷 외부에 존재하고 외부 에이전트(FA)를 통해 CoA를 구성한 경우와 DHCP(Dynamic Host Configuration Protocol) 서버로부터 주소를 할당 받은 경우에 대해 각각 fvc, cvc 모드를 정의하고 각 경우에 대한 엑세스 시나리오를 제공한다. 또한 이동 노드가 현재 인트라넷 내부에 존재하는지, 외부에 존재하는지의 여부를 판단하기 위한 방법으로 외부 홈 에이전트(x-HA)를 두어서 바인딩 갱신 메시지에 대한 응답 수신여부를 통해 위치를 판단한다. 'cvc' 모드에서의 처리 과정은 그림 2와 같다.

만일 이동 노드가 외부 에이전트로부터 CoA를 구성하였다면, 그림 3과 같은 'fvc' 메시지 처리 과정을 따른다.

먼저 x-HA와 i-HA로 BU를 동시에 전송하고 x-HA로부터 응답이 수신되는 경우 이동 노드는 인터넷상에 존재하며, 만일 i-HA로부터 응답이 수신되는 경우 인트라넷에 존재한다. 위치 판단한 후 각 엑세스 모드에 따라 IKE, 홈 바인딩 등록 과정을 진행한다. 그러나 이동 노드가 외부 망으로 이동한 경우, 위치 판단, IKE 협상 및 홈 바인딩 등록에 앞서서 반드시 방문 망을 인증해야 하고 방문망은 이동 노드를 인증해야 한다. 기존의 방법에서는 이러한 과정을 제공하지 않는다. 따라서 본 연구에서는 DIAMETER 기반의 안전한 인증 처리를 위해 기존에 제안된 방식[6]과 AAA 인프라 구조([7,8])를 통합한다.

3.3 VPN 상에서 AAA 기반의 이동 노드 인증 및 홈 등록 처리 방법

이 장에서는 본 논문에서 제안하고 있는 VPN상에서 AAA인프라 구조(DIAMETER)를 이용한 이동 노드 인증 및 VPN 게이트웨이를 통한 인트라넷 내부 자원의 엑세스에 관한 방법을 기술한다.

3.3.1 엔티티

본 논문에서 제시한 인증 방법의 기본 모델은 그림 1을 따르며 2장에서 정의한 엔티티 정의를 따른다. 본 논문에서는 기존의 홈 AAA서버인 AAAh와 터널링 프록시 역할을 통합하는 새로운 엔티티인 AnT 엔티티를 도입하고 기능을 정의하였다.

3.3.2 메시지 처리 과정

본 논문에서 제안하고 있는 메시지 처리 과정은 다음과 같다.

이 절에서는 이동 노드가 인트라넷 내부에 존재하는 CN과의 세션을 유지한 채 외부 인터넷 망으로 로밍할 경우 세션의 재설정 및 VPN 통과를 위한 IPsec-ESP 터널 재협상 과정을 거치지 않고 안전하게 이동성을 제공받을 수 있도록 하기 위해 그림 4에서 정의한 메시지 교환 절차에 따른 각 엔티티의 동작에 관해 기술한다. 먼저 이동 노드는 새로운 서브넷으로 이동한 후 자신의 현 위치가 인트라넷 내부인지 외부인지의 여부를 파악하기 위해 바인딩 갱신 메시지를 i-HA와 x-HA로 동시에 전송한다. 이때 바인딩 응답이 x-HA로 부터 온다면 MN은 인트라넷 외부에 존재한다고 판단한다. 마찬가지로 i-HA로부터 응답을 받으면 인트라넷 내부에 존재한다. 만일 응답이 없으면 MN은 주기적으로 i-HA와 x-HA로의 바인딩 갱신 등록을 반복해야 한다. MN은 x-HA 및 i-HA와 서전에 협의된 SA을 가지므로 이

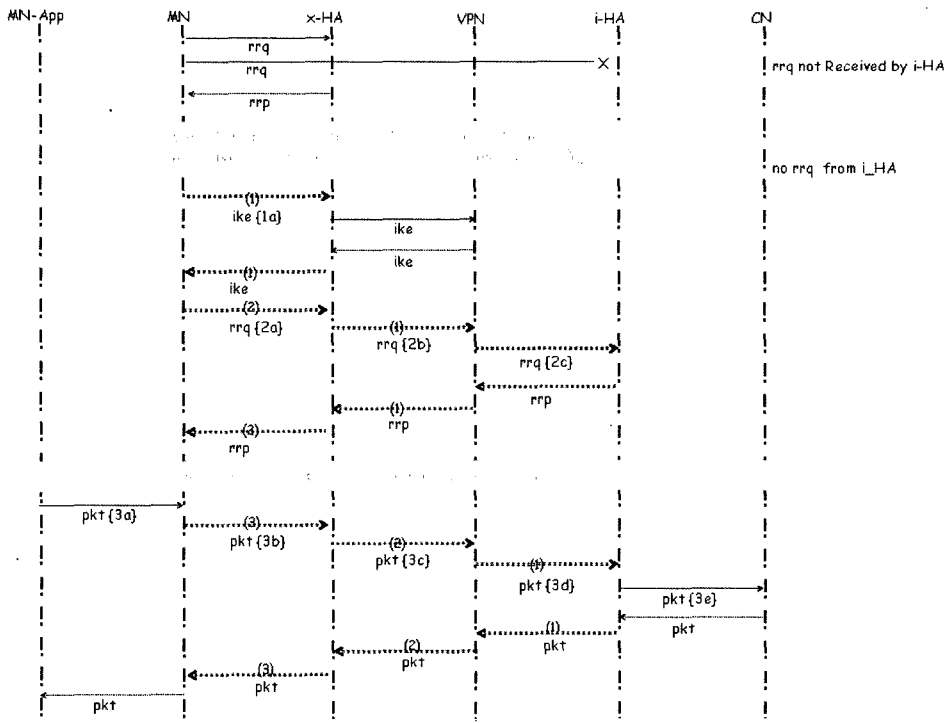

그림 2 'cvc' 모드에서의 메시지 처리과정

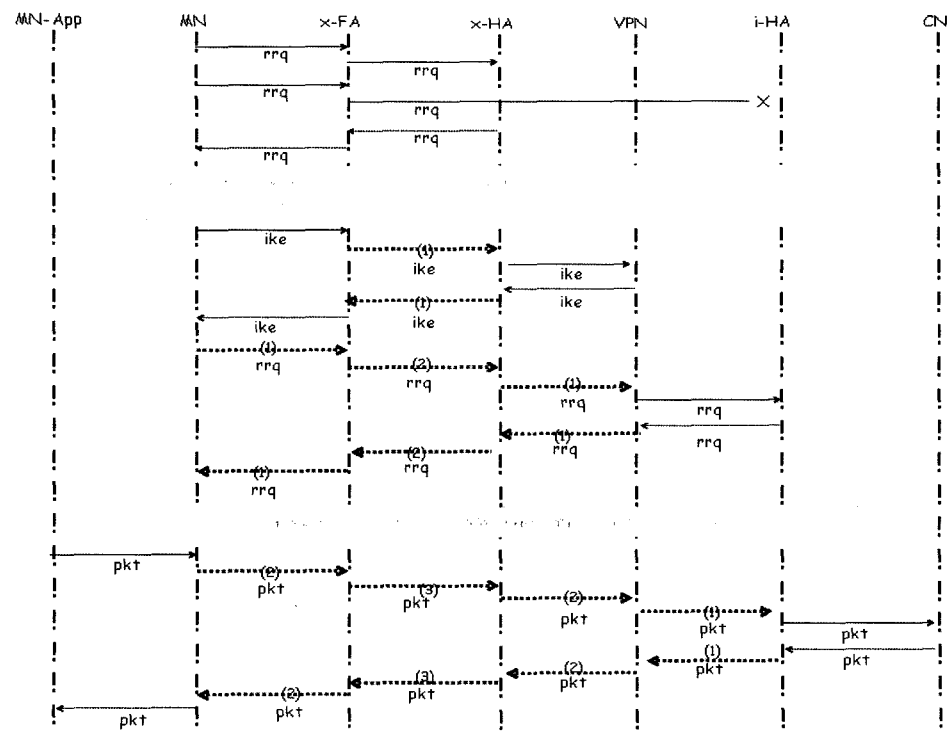

그림 3 'fvc' 모드에서의 메시지 처리과정

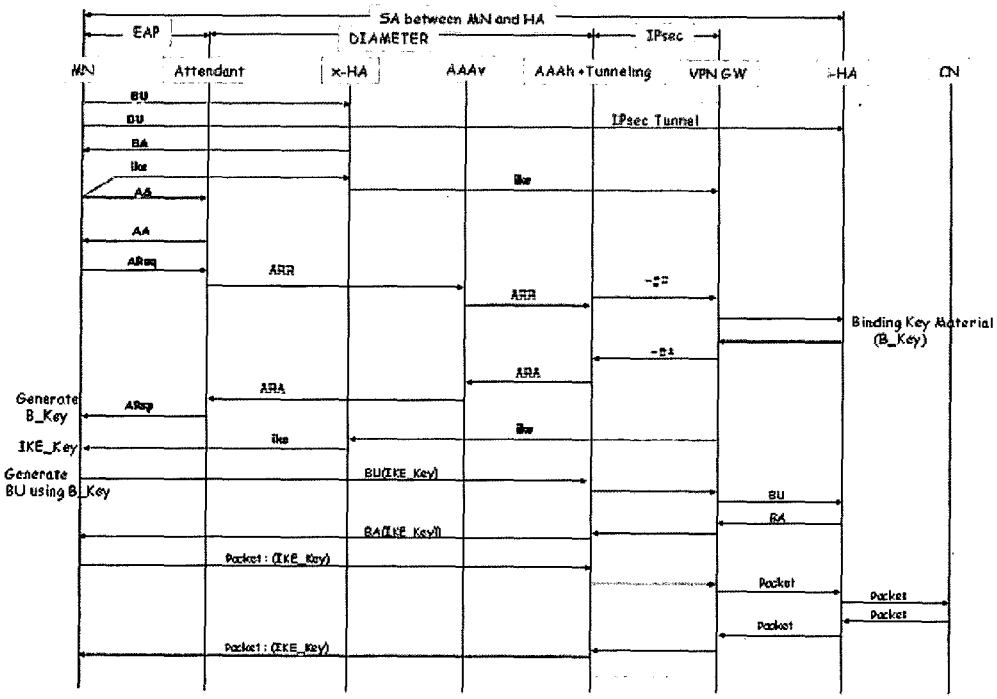

그림 4 VPN 환경에서 제안된 모델에 따르는 메시지 처리 과정

메시지는 안전하다고 가정한다. 위치를 탐지한 후, MN은 Attendant 탐지를 위한 AS(Attendant Solicitation) 메시지를 멀티캐스트 함과 동시에 IKE 협상을 위한 메시지를 AAAh+Tunneling(AnT) 엔티티로 전송한다. AnT는 VPN 게이트웨이의 보안 정책을 만족하는 엔티티로서 VPN 게이트웨이와 IPsec-ESP 터널을 유지하고 있으며, 주기적으로 또는 관리자의 요구에 의해 수동으로 터널을 재설정할 수 있다. AnT는 외부에서 VPN 게이트웨이에 접근하기 위한 엔티티로서 사설망 외부에서 위치하는 MN이 VPN 접근시 인증 및 VPN 터널 처리를 위한 정보를 제공해 주며 VPN 접근을 위한 터널을 제공한다. AnT는 사설 망 외부에 존재하는 엔티티이므로 VPN 게이트웨이와 AnT간에는 IPSec에 의한 보안 협약이 설정되어 있어야 하고, VPN 접근을 위한 터널이 형성되어 있어야 한다. MN이 보내는 IKE 메시지는 현재 AnT와 VPN 게이트웨이 간에 설정된 터널에 대한 키 재료를 얻기 위한 메시지로서 MN은 이 정보를 통해 AnT와 VPN 게이트웨이에 접근할 수 있는 키를 얻게 된다. MN의 인증 과정은 DIAMETER 인프라 구조를 갖는 AAA 엔티티의 연동을 통해 제공된다. AAA 엔티티는 Attendant, AAAv 및 AAAh가 있다. 먼저 MN은 Attendant로 인증 요청 메시지(AReq)를 전송한다. 이때 포함되는 파라메터는 Local Challenge, MN's NAI, RPI(Replay Protection Indicator), MN의 홈 주소, MN의 CoA, MN의 홈 에이전트 주소, 보안 파라메터(SecureParam_I), Credentials(Authenticator)와 Binding Key Request가 있으며, MN이 AReq를 보낸 후 인증이 완료되면 인증 응답(ARsp) 메시지를 수신하는데 여기에는 Local Challenge, RPI(Replay Protection Indicator), MN의 홈 주소, MN의 홈 에이전트 주소, 보안 파라메터(SecureParam_R), Credentials (Authenticator)와 Binding Key Response가 있다. MN은 수신된 보안 파라메터(SecureParam_R)을 통해 바인딩 키 재료를 얻고 바인딩 등록시 필요한 키(Kbu)를 생성한다. 마지막으로 MN은 인트라넷 내부에 있는 자신의 홈 에이전트(i-HA)로 바인딩 등록 메시지를 전송한다. 이때 바인딩 등록 메시지는 Kbu에 의해 암호화 처리를 하고, 바인딩 갱신 메시지를 페이로드로 가지는 외부의 패킷은 IKE 키로 보호된다. MN이 보낸 바인딩 등록 패킷은 AnT로 전송되며, AnT에 의해 IKE 복호화 과정 및 터널링 처리를 통해 인트라넷 내부의 i-HA로 보내지게 된다. i-HA는 Kbu를 사용해서 수신된 바인딩 등록 메시지에 대한 검증 과정을 수행하고 문제가 없는 경우 바인딩 등록 처리를 수행하게 된다. Attendant는 MN으로부터 받은 인증 요청 메시지를 DIAMETER 메시지 형태로 변환해서 방문방의 AAA

서버와의 상호 연동을 수행하는 엔티티이다. MN으로부터 AReq 메시지를 수신하면 이를 DIAMETER 메시지인 ARR로 변경해서 필요한 AVP를 엔코딩한 후 AAAv로 전송 한다. Address AVP는 주소에 관련된 옵션에 관한 것으로서, Home-Address-Option(MN의 홈 주소), Home- Agent-Address-Option(MN의 홈 에이전트 주소),Care-Of-Address-Option(MN의 CoA)가 있다. Security AVP는 보안에 관련된 옵션에 관한 것으로서, Nonce-Option(RPI), Security-Parameter-Option(SecureParam_I), Authenticator-Option(CR)가 있다. Authentication-Path AVP는 인증 정보를 표시하기 위한 것으로서, NAI-Option(MN의 NAI)이 있다. ARR 메시지에 대한 응답으로 Attendant는 AAAv로부터 ARR 메시지를 수신한다. 이때, Address AVP는 주소에 관련된 옵션이며, Home-Address-Option(MN의 홈 주소), Home-Agent-Address -Option(MN의 홈 에이전트 주소)가 존재한다. Security AVP는 보안에 관련된 것으로서, Authenticator-Option, Security-Parameter-Option(SecureParam_R),Nonce-Option(RPI)가 포함된다. Action AVP는 인증 요청에 대한 처리 결과를 엔코딩하며, Result-Code-Option(명령처리 결과(Success, Fail))가 포함된다. 이때, 결과 코드가 'Success'인 경우, SecureParam_R에는 바인딩 키(Kbu)를 생성 하는데 필요한 키 생성 재료가 들어가며, MN은 이 정보를 통해 바인딩 키를 유도할 수 있다. DIAMETER 메시지인 ARR를 수신하면 Attendant는 Option을 추출하여 ARsp 메시지를 생성한 후 MN으로 전송한다. x-HA는 이동 노드의 현재 위치를 파악하기 위한 용도로 사용되는 엔티티로서 이동 노드와 사전에 협의된 SA를 가진다. x-HA는 인트라넷 외부에 존재하며 이동 노드가 인트라넷 외부에 있는 경우 보내온 바인딩 갱신(BU)에 응답을 함으로써 이동 노드가 자신의 현재 위치를 판단할 수 있도록 해 준다. 또한 이동 노드가 보내온 IKE 요청을 대신 처리해야 하는데 이는 이동 노드가 매번 이동 발생시 VPN 게이트웨이로 IKE 협상을 해야 하는 보안 처리과정의 부하를 없애 준다. 방문 망의 AAA 엔티티인 AAAv는 이동 노드의 홈 AAA 엔티티인 AAAh와 사전에 협의된 로밍 계약을 유지해야 한다. 만일 로밍 협약이 없다면 이동 노드는 불법적인 노드로 간주되고 인증은 실패하며, 이동 노드가 보내는 패킷은 방문 링크상의 보안 엔티티(예: 라우터, AP등)에 의해 차단된다. AnT는 두 가지의 복합적인 기능 요소를 가지는 엔티티이다. 먼저 AAA 인증 엔티티로서 외부 망에 로밍중인 MN의 인증 요청을 AAAv를 통해 수신하면, MN의 인증 정보를 검증하고 AAAv와 사전에 협의된 로밍 계약에 따라 인증 절차를 수행한다. MN의 NAI, Authenticator, MN의 홈 주소 등을 기반으로 MN 인증을 처리하는데 MN 인증이 성공적으로 완료되면 ARR 메시지를 AAAv로 전송한다. AnT가 전송해 준 ARR 메시지를 AAAv는 그대로 Attendant로 전달해 주게 된다. AnT의 또 다른 기능은 'Tunneling Entry Point'로서 인트라넷 외부에 존재하는 MN이 인트라넷 내부의 자원(홈에이전트, CN, 데이타베이스 및 프린터 공유등)을 엑세스하기 위해 VPN 게이트웨이를 통과하기 위한 터널 진입지점이 된다. VPN 게이트웨이는 AnT와 항상 터널을 유지하고 있으며, VPN 게이트웨이는 AnT를 통해 들어오는 패킷을 통과시킨다. 즉, AnT는 '터널 프락시' 역할을 수행하는데, 기존의 VPN 클라이언트를 사용하는 경우에 비해 이 구조에서의 장점은 MN이 이동시 직접 VPN 게이트웨이와 터널을 재협상할 필요가 없으므로 실시간 응용에 적합하고, MN의 트래픽 처리 부하를 줄일 수 있는 것이다. 여러개의 MN에 대해 터널 유지 비용을 AnT가 전담하므로 MN은 그만큼 소프트웨어 처리가 간단하고, 기존의 Mobile IPv6 기술사양을 크게 벗어나지 않게 되며 추가적인 패킷처리 부하를 줄이게 된다. i-HA는 인트라넷 내부에 존재하는 이동 노드의 홈 에이전트로서 Mobile IPv6 기술 사양에서 정의하고 있는 기본 동작을 모두 만족한다. 이동 노드가 인트라넷 외부에 존재하는 경우 AAA 인증 과정을 통해 보안 파라메터(Secure-Param_R)를 노드에게 제공한다.

4. 성능 평가

4.1 비용 분석 모델

성능 평가 기준은 VPN 환경 하에서 제안된 AnT 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 데이타 패킷의 비용 등을 고려하였다. 제안하는 구조에 포함된 여러 엔티티간의 거리는 그림 5와 같다. 이동 노드가 인트라넷 외부로 로밍하면서 다른 외부 도메인으로 진입하는 경우 안전한 인증 처리 및 바인딩 키를 얻기 위해 AAA 인프라 구조를 사용하고 빈번한 IKE 협상을 없애기 위해 AnT 엔티티를 통해 홈 등록 및 패킷 전송을 하기 위한 시스템 모델을 제안하였다. 본 논문에서는 비용 분석을 위해 [9]에 기술된 접근 방법을 참조하였다. CN은 λ 비율로 MN에게 데이타 패킷을 전송하고, MN은 μ 비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정한다. 본 논문에서는 MN이 이동 특성에 따른 이동 비율로 이동하면서 CN으로부터 수신하는 평균 패킷 수를 Packet to

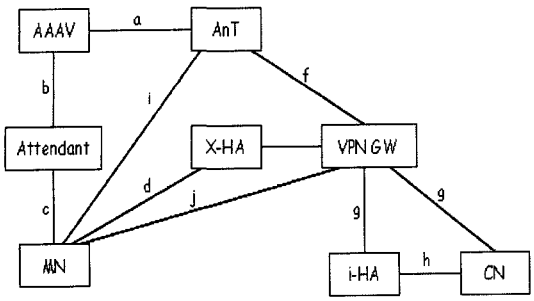

그림 5 VPN 환경 하에서의 AAA 인증 및 홈 등록 모델

Mobility Ratio(PMR) 이라고 정의하고 수식 $P=\lambda/\mu$ 로 정의한다. 본 논문에서는 한 호스트에서 제어 패킷을 처리하는 평균 비용은 r 이라고 가정한다.

인트라넷으로의 패킷 전송을 위해서는 우선 VPN 게이트웨이의 보안 정책을 만족해야 하는데 이를 위해서 먼저 IKE 프로토콜을 통해 터널링 및 키 협상을 마무리해야 한다. 이동 노드는 자주 이동하는 속성을 가지므로 이동 발생마다 IKE 프로토콜 협상을 수행하는 것은 노드 부하 및 서비스 지연 요인이 될 수 있다. 또한 외부 망에서 이동 노드가 외부 링크 사용을 허용 받기 위해서는 AAA 인프라 기반의 상호 인증 방법이 제공되어야 한다. 이를 처리하기 위한 엔티티로 본 논문에서는 AnT를 정의하고 있다. 즉 AnT를 통해 인증 및 터널링 처리가 가능하다. 이동 노드가 새로운 이동 발생 탐지 후 AnT를 통한 인증, 터널링 및 키 처리 후 홈 등록을 완료하기 전까지 상대 노드가 이동 노드로 보내는 모든 패킷은 분실 비용으로 처리할 수 있다. 따라서 인트라넷 외부 로밍 중 이동 노드가 인트라넷 내부에 존재하는 자신의 홈 에이전트로 바인딩 등록을 완료하기까지의 비용은 이동 노드의 위치 탐지 기간, AAA 인증 및 IKE 처리 지연 시간 및 바인딩 등록 처리 지연 시간 동안 발생하는 패킷 분실 비용의 합으로 구할 수 있다.

암호 연산 및 데이타 전송을 위해 필요한 각 파라메터별 계산 값과 프로토콜 처리 계층 별 오버헤드는 다음과 같이 계산된다[10].

4.2 Mobile IPv6를 위한 AAA 인증 및 바인딩 등록 비용 분석

이 절에서는 기존의 방식과 본 연구에서 제안된 방식을 평가하기 위한 비용 분석을 제시한다. 전체 비용(Ctotal)은 이동 노드가 인트라넷 외부에서 AAA 인증 및 VPN 게이트웨이를 통한 홈 바인딩 등록을 완료 후 서브넷에 머물기까지의 시간 동안 발생하는 패킷 분실 비용(C_{loss})과 인증 및 등록을 처리하는 동안 상대 노드와의 트래픽 처리 비용의 합으로서 식 (1)과 같다.

$$C_{total} = C_{loss} + C_{process} + C_{CN} \quad (1)$$

4.2.1 이동 확률 및 패킷 처리 전송시간/오버헤드

이동 노드가 다른 서브넷으로 이동한 후 인증을 완료하고 VPN 게이트웨이를 통한 홈 바인딩 등록을 완료하기까지 기간 동안 상대 노드와 이동 노드간의 패킷은 분실된다. 따라서 패킷 분실이 발생하는 동안 처리 과정에서 이동 노드의 행위를 보면 (1)이동 발생, (2)위치

표 1 파라메터별 값과 프로토콜 처리계층별 오버헤드

패킷 필드	값
호스트 이름(Host Name)	20 바이트
망 식별값(NAI)	20 바이트
인증자 라이프타임	4 바이트
메시지 인증자(Authenticator)	MD5(16)/SHA-1(20) 바이트
TCP 헤더(옵션 없음)	20 바이트
ESP-헤더	8 바이트
ESP-인증 확장	20 바이트
IP 헤더(옵션 없음)	20 바이트

암호학적 연산 알고리즘	처리 시간
Hashing 512비트(MD5)	1.5 μs
Hashing 512비트(SHA-1)	3.73 μs
Encrypting n*64 비트(DES)	3.06 μs + n*1.51 μs
Encrypting n*64 비트(3DES)	9.17 μs + n*4.14 μs

프로토콜 계층	처리 오버헤드
물리층 처리 오버헤드	192 μs
MAC층 처리 오버헤드	136 μs
IP층 처리 오버헤드	80 μs
UDP층 처리 오버헤드	32 μs

탐지, (3)인증, (4)SA 설정, (5)홈 바인딩 등록으로 나누어 생각할 수 있다. 즉, 이동 노드의 중요 행위가 발생한 시간 동안 발생한 비용의 합을 전체 분실 비용으로 처리할 수 있다. 이동 발생 시 두 가지 측면을 고려할 수 있다. 먼저 이동이 발생했지만 같은 로컬 AAA 서버에 의해 관리되는 영역 내에서 이동한 경우이다. 이 경우 만일 이전에 설정한 SA에 대한 라이프 타임이 아직 유효하다면 별도의 키를 얻을 필요가 없다. 만일 라이프 타임이 더 이상 유효하지 않다면 인증 및 IKE 키 교환 작업을 실행해야 한다. 이동 노드가 다른 서브넷으로 이동할 확률을 P_{MOVE}이라고 정의할 때 다음과 같은 수식을 적용할 수 있다. 모델 이동성을 나타내기 위해, [8]의 uniform fluid model을 적용하였으며, 이 모델에서 보행 속도로 이동하는 경우 $\mu=0.01$이고 차량의 속도로 이동하는 경우 $\mu=0.2$로 정의하였다.

$$P_{MOVE}=\frac{k\mu}{e^{T_s}} \tag{2}$$

여기서 Ts는 노드가 한 서브넷에 머무는 시간을 의미하며 μ는 노드의 이동률(보행=0.01, 차량=0.2)을 의미한다. k는 가중치 요소(weighting factor)이동률에 대한 변위 값을 의미한다. 만일 노드가 한 서브넷에 머무는 시간이 길면 $Ts\rightarrow\infty$가 되고 $P_{MOVE}=0$ 가 된다. 즉, 노드가 한 서브넷에 오래 머물게 되면 이동 확률은 매우 작아진다. 만일 노드가 한 서브넷에 머무는 시간이 짧다면 $Ts\rightarrow 0$이 되고 이때 $P_{MOVE}=k\mu$가 된다. 즉, 빈번한 이동이 발생하는 경우 노드의 이동률에 의해 확률이 결정된다.

한 서브넷에 머무는 시간이 길면 이동성은 낮아지고 시간이 짧으면 이동 확률은 높아지게 된다. PMR (Packet to Mobile Ratio)는 이동 노드의 트래픽으로서

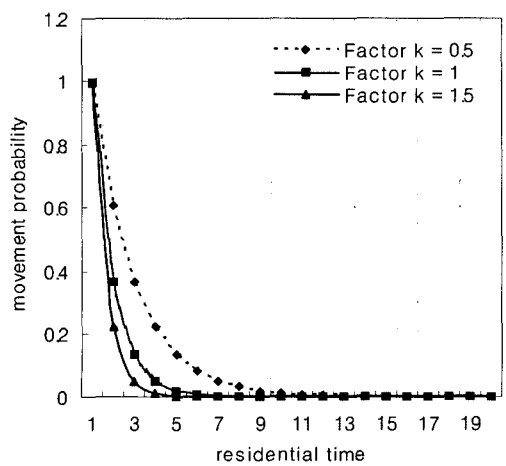

그림 6 μ값에 대한 노드의 이동 확률

이동 당 송수신되는 패킷의 수로 정의하며 $PMR(p)=\lambda/\mu$로 정의할 수 있다. 여기서 λ는 평균 패킷 길이를 의미한다. 이동 노드는 평균 5개의 진행 중인 세션을 유지하고 있고 이때 데이타 패킷의 평균 길이는 1024바이트, 제어 패킷의 평균 길이는 100바이트로 정의하였다. 이동 노드가 새로운 서브넷으로 이동하는 사건의 발생은 포아송 분포를 따르며 새로운 서브넷에서 서비스를 완료하고 다른 서브넷으로 이동하는 사건은 가우스분포(정규분포)를 따른다. 이때 서비스에는 인증, SA 설정, 홈 바인딩 등록 및 CN과의 통신이 포함된다. 또한 로컬 AAA 서버와 홈 AAA 서버는 정해진 처리용량에 따라 동작하므로 평균 처리 용량을 넘어서는 경우 버퍼 값에 따른 대기 행렬로 표현할 수 있으며, 버퍼 용량에 따른 처리 변화를 알 수 있다. 또한 이동 노드가 CN과 통신을 하는 비용의 경우 기존 방식의 경우 IPsec-ESP 터널링을 3회 처리해야 하며, 새로 제안된 방법에서는 IP-in-IP 터널링을 1회 수행하므로 각 터널링을 처리하는데 소요되는 시간을 상수 값으로 취해서 이를 자세히 계산할 수 있다. IP-in-IP 터널링의 경우 옵션을 제외한 나머지헤더에 대한 처리 오버헤드가 추가된다. 이동 노드가 한 서브넷에 도착할 확률은 포아송 분포를 따르며 다음 수식과 같다.

$$P(\gamma)=\frac{e^{-\eta}\eta^{x}}{x!} \tag{3}$$

여기서 x는 이동 노드의 수, η은 다른 서브넷으로의 평균 이동 비율로서 보행자 및 차량 속도의 이동 노드에 대한 이동 사건 발생에 대한 기댓값이다. 한 서브넷에 존재할 수 있는 최대 노드의 개수는 200로 이동 특성을 가지는 노드는 100개이고 이들 중 보행 이동노드와 차량 이동노드의 수를 각각 80및 20으로 가정했을 때, 보행 및 차량 이동 노드에 대한 다른 서브넷으로의 이동 비율을 각각 0.01과 0.2 이므로 보행 이동 노드와 차량 이동 노드의 평균 이동 값은 각각 0.8과 4값을 가진다.

그림 7은 한 도메인에 존재하는 이동 노드의 수에 따른 보행 및 차량 속도의 이동 노드에 대한 도착 확률을 보여 준다. 전체 이동 노드의 수가 증가하면 보행 이동 노드의 도메인 간 이동 확률은 줄어들게 되며 이때 차량 이동 노드의 이동 확률은 이동 초기에 증가하지만 0.2퍼센트 지점을 지나게 되면 감소하게 된다. 즉, 노드의 이동 노드의 수가 적은 경우 상대적으로 보행 및 차량 이동 노드의 이동 확률은 높지만 전체 이동 노드의 수가 많아지게 되면 낮아지게 된다. 이는 이동 노드가 다른 도메인으로 이동하기보다 해당 도메인에서 이동하는 경우가 빈번해짐을 의미한다. 도메인간의 이동이 발생하는 경우 본 논문에서 제안하는 방식에 따라 로컬

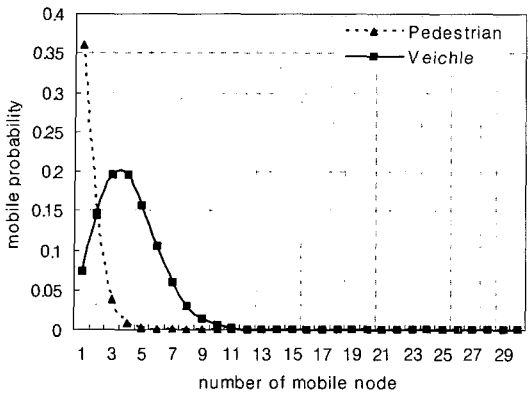

그림 7 이동 노드 수에 대한 보행자 및 차량 이동 노드의 도메인 간 이동 확률

도메인에 존재하는 AAA와 이동 노드의 홈 도메인에 존재하는 AAA 엔티티를 통한 노드 인증 및 키(재료)의 분배 과정이 수행된다. 이동 노드가 다른 도메인으로 이동한 경우, AAA 인프라를 통한 인증을 완료하고 VPN을 경유해서 자신의 인트라넷 안에 존재하는 상대노드와의 통신을 완료한 후 다른 도메인으로 이동하기까지의 전체 시간을 이동 노드의 서비스 시간으로 간주한다면, 노드의 서비스 시간은 지수 분포를 따르므로 다음과 같은 식으로 표현할 수 있다.

$$f(t) = \sigma e^{-\sigma t} \quad (4)$$

여기서 σ는 평균 서비스 시간을 나타내며, 이는 이동 노드의 현재 위치 탐지에 소요되는 시간(t_{LOC}), 이동 노드의 평균 인증시간(t_{AAA}), VPN 통과를 위한 키(재료)를 얻는 평균 시간(t_{IKE}), 바인딩 등록 처리에 소요되는 평균 시간(t_{BU}) 및 인트라넷에 존재하는 상대 노드와의 평균 통신 시간(t_{CN})를 합으로 나타낼 수 있다. 먼저 모델에 의한 위치 탐지 시간은 다음과 같다. 먼저 이동 노드는 현재 위치 탐지를 위해 x-HA와 i-HA로 각각 바인딩 등록 메시지를 전송하는데, 이때 이동 노드와 Attendant와는 무선 구간이므로 최대 11Mbps의 속도를 가정한다면, 현재 Attendant가 서비스하고 있는 평균 이동 노드의 수는 45개 이므로 무선 링크의 평균 서비스 속도는 $(11Mbps/45) = 0.244Mbps$로 정리할 수 있고, Attendant가 메시지를 받아서 Layer2 처리를 완료한 후 로컬 서브넷의 라우터로 메시지를 포워딩하므로 물리층 및 MAC층의 처리 오버헤드($338\mu s \approx 0.34ms$)가 추가된다. Attendant와 라우터간은 유선링크로서 메시지 포워딩 속도는 10Mbps이며 라우터에서 x-HA까지는 80ms의 전송 지연이 발생한다. 이에 따라 구간별 소요되는 전송 및 처리시간을 계산하면 다음과 같다.

표 2 각 구간별 단일 패킷에 대한 전송 시간

모델	전송시간
t_a	$80ms - \frac{(lc*8bit)/1Mbit}{100Mbps} = 79.9ms$
t_b	$\frac{(l*8bit)/1Mbit}{10Mbps} + 0.34ms = 0.418ms(l=l_c), 1.14ms(l=l_d)$
t_c	$\frac{(l*8bit)/1Mbit}{0.244Mbps} = 3.2ms(l=l_c), 32.78ms(l=l_d)$
t_d	$\frac{(l_c*8bit)/1Mbit}{0.244Mbps} + 0.34ms + \frac{(l_c*8bit)/1Mbit}{10Mbps} + 80ms = 83.62ms$
t_e	$80ms$
t_f	$\frac{(l*8bit)/1Mbps}{100Mbps} = 0.0078ms(l=l_c), 0.08ms(l=l_d)$
t_g	$\frac{(l*8bit)/1Mbps}{10Mbps} = 0.078ms(l=l_c), 0.8ms(l=l_d)$
t_h	$\frac{(l*8bit)/1Mbps}{10Mbps} = 0.078ms(l=l_c), 0.8ms(l=l_d)$
t_i	$t_c + t(※endant \leftrightarrow router) + 80ms = \frac{(l*8bit)/1Mbit}{0.244Mbps} + 0.34ms + \frac{(l*8bit)/1Mbit}{10Mbps} + 80ms$ $= 83.62ms(l=l_c), 113.92ms(l=l_d)$
t_j	$t_c + t(※endant \leftrightarrow router) + 80ms = \frac{(l*8bit)/1Mbit}{0.244Mbps} + 0.34ms + \frac{(l*8bit)/1Mbit}{10Mbps} + 80ms$ $= 83.62ms(l=l_c), 113.92ms(l=l_d)$

$$t(MN \leftrightarrow x-HA) = \frac{(l_c*8bit)/1Mbit}{0.244Mbps} + 0.34ms + \frac{(l_c*8bit)/1Mbit}{10Mbps} + 80ms \quad (5)$$

본 논문에서 제어패킷의 평균 길이 $l_c = 100$ 바이트이므로 이동 노드가 바인딩 등록 메시지를 x-HA로 전송하는데 걸리는 평균 시간은 $t(x-HA) = 83.62ms$가 된다. 즉, 모델에서 $t_d = 83.62ms$이다. 같은 방식으로 모델의 각 구간별 단일 패킷에 대한 전송 시간을 구하면 다음과 같다.

4.2.2 비용 분석

전체 패킷 분실 비용은 'Location Detection', 'AAA Authentication + IKE Negotiation' 및 'Binding Registration' 처리 시간 동안에 발생하는 총 분실 패킷 수의 합으로 표시할 수 있다. 그러므로 이동 노드가 인트라넷 외부에서 AAA 인증 및 VPN 게이트웨이를 통한 홈 바인딩 등록을 완료하기까지의 시간 동안 발생하는 패킷 분실 비용(C_{loss})는 수식 (6)과 같이 나타낼 수 있다.

$$C_{loss} = C_{loss-detection} + C_{loss-\max(AAA,IKE)} + C_{loss-BU} \quad (6)$$

각 단계에서 발생하는 loss는 해당 단계를 처리하는데 걸리는 시간, 평균 데이타 패킷 수신율을 곱한 것으로서 $C_{loss-detection} = \lambda * t_{detection}$로 나타낸다. 따라서 수식 (6)를 정리하면 수식 (7)과 같다.

$$C_{loss} = \lambda*(t_{detection} + \max(t_{AAA}, t_{IKE}) + t_{BU}) \quad (7)$$

여기서 이동 노드의 현재 위치(인트라넷 내부 또는 외부)를 파악하기 위해 BU를 x-HA와 i-HA로 보내는데 이때 양쪽 HA로 동시에 보내며 이동 노드가 외부에 있는 경우 x-HA로부터 응답(BA)를 수신한다. 따라서 $t_{detection} = 2t_d + 3t_r$로 나타낼 수 있다. 여기서 t_r은 물리층에서 전송 층 오버헤드를 모두 더한 값이 되므로 0.44ms이다. 따라서 $t_{detection} = 2*38.62ms + 3*0.44ms = 78.56ms$가 된다. $\max(t_{AAA}, t_{IKE})$는 AAA 인증을 완료하기까지의 기간과 IKE 키를 얻어 오는데 걸리는 시간 중 긴 시간을 취하기 위한 함수이다. 그러나 본 연구에서 IKE 메시지는 AAA 메시지와 동시에 전송되며 메시지 전송 시간은 홉 간의 거리에 의존하고 각 노드에서 처리하는 시간 r은 작은 값이므로 그림 6에 주어진 모델에 따른 링크 가중치를 기반으로 $\max(t_{AAA}, t_{IKE}) \equiv t_{AAA}$로 정의한다. 이때 $t_{AAA} = 2(t_a + t_b + 2t_c + t_f + t_g) + 13t_r = 179.32ms$이다. t_{BU} 는 인증이 완료되고 IKE 키를 얻은 후 페이로드를 IKE 키로 암호화한 후 VPN 게이트웨이를 통해 i-HA로 홈 등록을 수행하는데 걸리는 시간으로서 AnT를 통해 VPN 게이트웨이에 접근하므로 $t_{BU} = 2(t_i + t_f + t_g) + 7t_r = 170.48ms$로 나타낼 수 있다. 따라서 수식 (7)을 정리하면 수식 (8)과 같다.

$$C_{loss} = \lambda*(4(t_c + t_f + t_g) + 2(t_a + t_b + t_d + t_i) + 23t_r) = \lambda*428.36ms \quad (8)$$

여기서 보행시($\mu = 0.01$) 평균 0.8개 및 차량 이동시($\mu = 0.2$) 평균 4개의 노드가 다른 서브넷으로 이동하고 이때 λ값은 110.5Kbyte/s이므로 각각 $C_{loss} \approx 37.86Kbyte$와 $C_{loss} \approx 189.32Kbyte$가 된다.

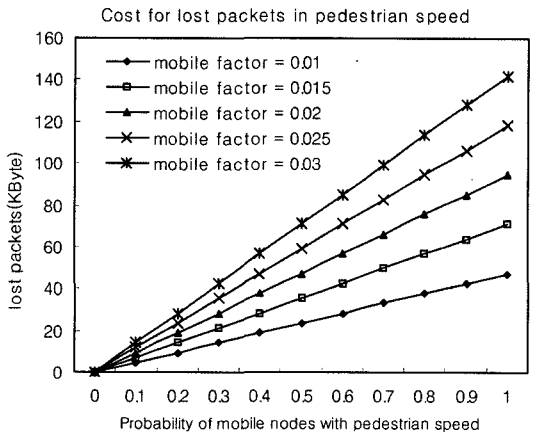

그림 8 보행 이동시 이동 특성에 따른 패킷 분실 비용 증가

이 그림은 전체 이동 노드 중에서 보행 특성을 가지는 이동 노드의 수 및 이동 노드의 이동 특성에 따르는 패킷 분실 비용을 보여준다. 이동 노드의 수가 많아지고, 이동 특성이 증가할수록 이동 발생시 생기는 패킷 분실이 커지게 된다. C_{CN}은 이동 노드의 인증 및 바인딩 등록을 완료한 후 상대 노드(CN)와의 통신을 재개하고 다른 서브넷으로 이동하기 전까지 해당 서브넷에 머무는 동안 발생하는 트래픽에 대한 처리 비용으로서 이동 노드의 특성에 따라 각각 보행 및 차량 이동시 한 서브넷에 머무는 전체 시간 동안 수신하는 패킷에 대한 처리량으로 나타낼 수 있다. 이동 노드가 상대 노드로 보내는 패킷은 AnT에서 IP-in-IP 터널링 되고 AnT와 VPN 게이트웨이 간에는 ESP 처리가 필요하므로, 이동 노드와 AnT간의 평균 데이타 패킷의 길이는 1044바이트이고 AnT와 VPN 게이트웨이간의 평균 데이타 패킷 길이는 1052바이트이다. VPN게이트웨이에서 상대노드로 보내는 데이타 패킷은 터널링 및 암호화 처리를 모두 마쳤으므로 1024바이트이다. 그러므로 전 구간에 대한 데이타 패킷의 평균 길이는 1040바이트이다.

$$C_{CN} = \lambda*2(t_i + t_f + t_g) = \lambda*2(114.45ms + 0.08ms + 0.81ms) = \lambda*230.68ms \quad (9)$$

여기서 보행 시($\mu = 0.01$) 평균 0.8개 및 차량 이동시

($\mu=0.2$) 평균 4개의 노드가 다른 서브넷으로 이동하고 이때 λ값은 110.5Kbyte/s이므로 이를 반영하여 구한 값에 보행 및 차량 이동시 한 서브넷에 머무는 시간을 곱하면 된다. 보행 속도로 이동하는 경우 한 서브넷에 머무는 평균 시간은 12분이고 차량 보행 속도의 경우 3분이므로 각각 $C_{CN} \approx 14.68Mbyte$와 $C_{CN} \approx 18.35Mbyte$가 된다. 여기서 한 서브넷에 머무는 동안 수신하는 트래픽의 비율인 TMR(Traffic to Mobile Ratio)를 정의할 수 있다.

$$TMR(\tau) = \omega * p(\gamma) * f(t) = \omega * (\frac{e^{-\eta}\eta^{x}}{x!}) * (\sigma e^{-\sigma t}) \quad (10)$$

노드가 포아송 도착률에 따라 서브넷으로 이동하고 서브넷에서 인증 및 바인딩 등록을 완료한 후 다음 서브넷으로 이동하기까지 발생하는 트래픽으로서 서브넷에 머무는 시간은 지수 분포를 따르므로 해당 시간동안의 트래픽을 나타내 준다. 여기서 ω는 트래픽 특성을 나타낸 것으로서 이동 노드가 상대 노드와 유지하고 있는 평균 세션의 개수 및 세션 트래픽 평균값을 반영한 것으로서, 이동 노드가 전체 세션을 통해 송수신하는 초당 패킷 바이트에 대한 평균값으로 정의할 수 있다.

4.3 성능 분석

4.3.1 PMR 값에 따른 성능 분석

먼저 PMR 값의 변동을 기준으로 이동 노드와 상대 노드간의 트래픽 특성을 고려하여 성능을 분석하였다. 이동 노드가 외부에서 로밍 하는 중에 상대 노드와 교환하는 데이타 트래픽의 평균 길이를 각각 1024 바이트와 100 바이트를 기준으로 PMR 변화량에 따른 비용 증가를 그래프로 나타내었다.

먼저 이동 노드가 보행자 속도로 이동하는 비율을 따를 때 데이타 패킷의 평균 길이의 변동은 전체 비용 증가에 크게 영향을 주지 않지만, 차량의 이동 속도로 이동하는 특성을 가질 때 데이타 패킷의 평균 길이는 전체 비용 증가에 크게 관여하게 된다. 1024 바이트의 평균 데이타 트래픽 특성을 가지는 경우 PMR 값이 증가함에 따라 인증 및 홈 바인딩 등록비용은 급격히 증가한다. 이는 빈번한 이동 발생 시 데이타 길이가 비용에 크게 영향을 줌을 알 수 있다. 또한 다음 그래프는 차량의 속도로 이동하는 경우와 보행자의 속도로 이동하는 경우 데이타 패킷의 평균 길이를 고려한 PMR 증가에 따른 비용 정규화(Normalization) 변화율을 보여 준다. 보행자 속도로 이동하는 경우 PMR 증가에 완만하게 비용율이 증가하는 반면 차량의 이동 속도로 이동하는 특성을 가지는 경우 PMR 값이 증가하면 초기에 급격한 비용율 변화를 보여준다. 또한 PMR 값이 큰 경우 (>100)인 경우 두 가지 이동 특성에 따른 비용 변화율은 비슷한 값을 보이게 된다.

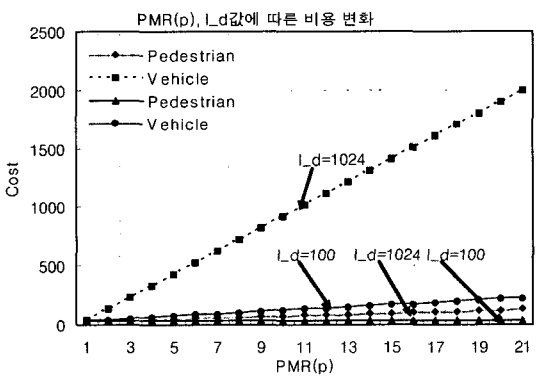

그림 9 데이타 트래픽 및 PMR 변화에 따른 비용 증가

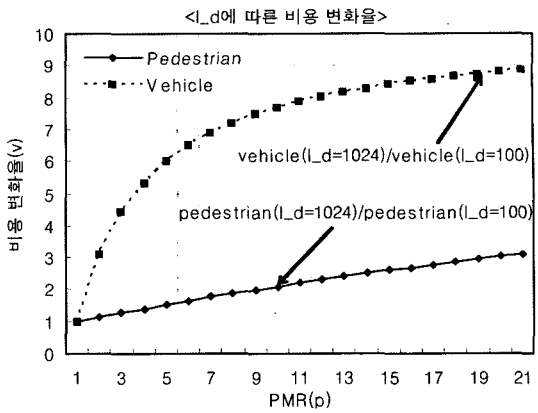

그림 10 보행자와 차량 이동 속도 특성을 가지는 경우 비용 변화율

4.3.2 보행 이동시($\mu=0.01$) 및 차량 이동시($\mu=0.2$) 패킷 분실 비용 분석

수식 (8)에서 구한 바와 같이 본 논문에서 제시하는 방식에 따른 패킷 분실 비용을 구할 수 있다. 동일한 조건하에서 기존 제안 방식에 따르는 'cvc' 및 'fvc' 모드에 대한 패킷 분실 비용을 구해서 비교하였다. 이동 노드는 평균 5개의 세션을 유지하고 있고, 전체 세션에 대한 트래픽은 초당 110.5KByte/s 라고 동일하게 가정하였다.

그림에서와 같이, 한 서브넷에 존재하는 전체 이동 노드의 수를 100으로 가정하였을 때 보행 및 차량 속도로 움직이는 이동 노드의 수가 증가할수록 한 서브넷에서 분실되는 패킷의 크기도 증가한다. 그래프에서 기존의 제안 방식인 'cvc'와 'fvc'의 경우 비슷한 분실 비용을 나타내고 있으며, 본 연구에서 제안한 방식은 기존 제안 방식에 비해 50% 정도의 비용 절감 효과가 있음을 보여 주고 있다.

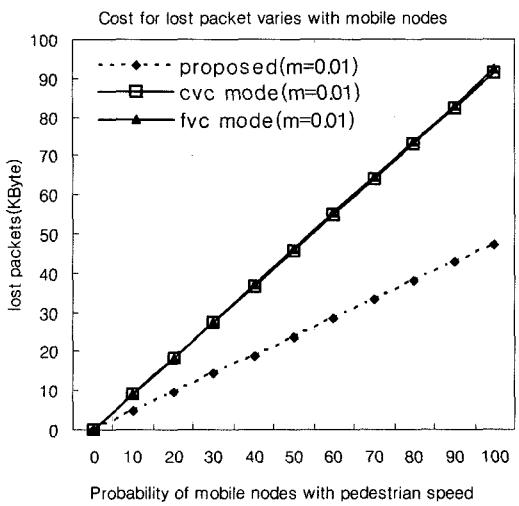

그림 11 보행 이동시 패킷 분실 비용

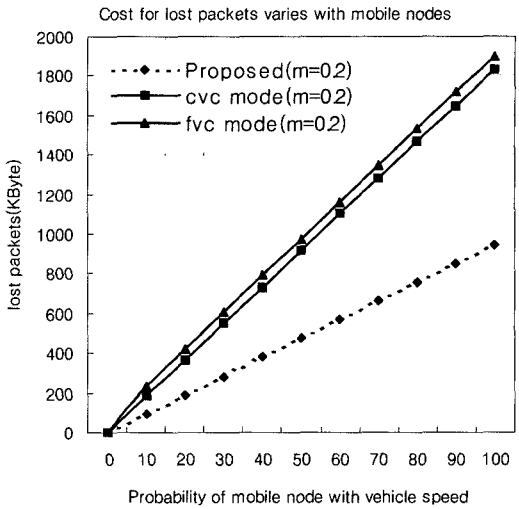

그림 12 차량 이동시 패킷 분실 비용

5. 결 론

본 연구에서는 기존에 유선 서비스 환경 하에서 성공적으로 적용된 대표적인 AAA 기술인 DIAMETER 프로토콜을 사용해서 안전하게 이동 노드를 인증하는 방법을 제안하였고, 제안된 방법에 따른 패킷 분실 비용을 계산하였으며 이동 노드의 트래픽 특성 및 PMR 값의 변화에 따른 성능을 분석하였다. 연구를 통해 보행 및 차량 이동 특성에 따라 인증 및 홈 등록 기간 동안 분실되는 패킷 비용이 달라지며, 서브넷의 크기, Attendant의 처리 용량, 데이타 및 제어 패킷의 평균 길이, 이동 노드의 전체 세션에 대한 트래픽 등에 따라 비용이 변화하는 것을 살펴볼 수 있었다. 특히 이동 노드가 상대 노드와 많은 세션을 가지고 있고, 주로 실시간 대량 전송 트래픽 패턴을 가지며, 상대적으로 자주 이동하는 특성을 가지는 경우 기존 방식에 비해 비용 절감 효과가 높다는 것을 보여 준다. 본 연구는 Mobile IP와 VPN 서비스를 효과적으로 통합할 수 있는 기본 구조를 제공하며 향후 유사한 서비스 도입 시 제공될 수 있는 보안 인프라 구조로서 활용될 것으로 기대된다.

참 고 문 헌

[1] F. Adrange, M. Kulkarni: Problem Statement Mobile IPv4 Traversal of VPN Gateways, draft-ietf-mobileip-vpn-problem-statement-req-01.txt, Internet Draft, IETF, Jan, 2003.

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

[3] Pat R. Calhoun, Erik Guttman, Jari Arkko: Diameter Base Protocol, RFC 3588, IETF, Sept, 2003.

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

[5] Davied B. Johnson, Charles E. Perkins, Jari Arkko: Mobility Support in IPv6, RFC3775, IETF, June, 2002.

[6] S. Vaarala: Mobile IPv4 Traversal Across IPsec-based VPN Gateways, draft-ietf-mobileip-vpn-problem-solution-03, Internet Draft, IETF, Sept, 2003.

[7] Franck Le, Basavaraj Patil, Charles E. Perkins : Diameter Mobile IPv6 Application, draft-le-aaa-DIAMETER-mobileipv6-01.txt, Internet Draft, IETF, November, 2001.

[8] Pat R. Calhoun, Charles E. Perkins: Diameter Mobile IPv4 Application, Internet draft, Internet Engineer Task Force, November 2001.

[9] R. Jain, T. Raleigh, C. Graff 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, Atlanta.

[10] A.Hess, G.Schafer: Performance Evaluation of AAA/Mobile IP Authentication, Proc. 2nd Polish-German Teletraffic Symposium(PGTS'02), Gdansk, Poland, Sep. 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). 2006년 3월~현재 숭실대학교 정보미디어연구소 전임연구원. 관심분야는 Mobile IP, AAA, Network Security, P2P Network

문 영 성

정보과학회논문지 : 정보통신
제 33 권 제 2 호 참조