Mobile IPv4에서 VPN 게이트웨이 통과를 위한 AAA 기반의 인증 방법

정회원 김 미 영*, 문 영 성**

Authentication Method based on AAA to Traverse the VPN Gateway in Mobile IPv4

Miyoung Kim*, Youngsong Mun** *Regular Members*

요 약

이동 노드가 홈 망을 벗어나 이동하는 경우 현재 위치 정보를 홈 에이전트로 등록해야 한다, 그러나 이동 노드의 홈 에이전트가 홈 망의 VPN 게이트웨이에 의해 보호되고 외부로부터의 비 인가된 엑세스가 차단되는 경우 이동 노드는 등록 절차를 성공적으로 실행할 수 없는데 이는 이동 노드가 외부 망으로부터 얻은 임시 주소(CoA)와 홈 망의 보안 정책간의 보안 협약(SA)의 부재로 인해 바인딩 등록 메시지는 VPN(Virtual Private Network) 게이트웨이에 의해 차단되기 때문이다. 이 논문은 인터넷에 존재하는 Mobile IPv4 사용자가 VPN 게이트웨이에 의해 보호되는 인트라넷을 엑세스할 수 있도록 AAA 인프라 구조를 사용한 인증 및 키 교환 방법을 제시한다. 각 에이전트나 릴레이 엔티티를 위한 인증 및 터널 처리를 정의함으로써 이동 중인 노드가 안전한 방법으로 VPN 내부의 홈 에이전트로의 바인딩 등록 절차를 하였고, 이동 및 트래픽 특성에 따른 인증 비용 항목에 대해 일반적인 방식과 제안 방식을 비교하였는데 최대 40% 성능향상을 보였다.

Key Words : Authentication, AAA, Mobile IPv4, VPN, Security

ABSTRACT

Mobile node has to register its current location to Home Agent when it moves to another network while away from home. However, the registration procedure cannot be completed successfully when Home Agent is protected by the VPN gateway which guards MN's home network and discards the unauthorized packets incoming from outside as a lack of security association(SA) between the Care-of address and security policy of the home network so that the binding registration message without SA is discarded smoothly by the VPN gateway. This paper presents the authentication and key exchange scheme using the AAA infrastructure for a user in Internet to access the home network behind the VPN gateway. By defining the role of authentication and tunnel processing for each agent or relay entity, this paper presents the procedure to register the current location to its Home Agent with secure manner. Performance result shows cost improvement up to 40% comparing with existing scheme in terms of the packet loss cost, the property of mobility and traffic.

Ⅰ. 서 론

Mobile IPv4와 같은 새로운 이동 서비스의 성공 여부는 기존의 서비스를 추가 부담 없이 그대로 사용할 수 있느냐에 달려 있다. 802.11b/g의 핫스폿 서비스와 셀룰러 폰, PDA등의 단말 장치가 대중화

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2006-C1090-0603-0040).
* 숭실대학교 정보미디어기술연구소(mizero@hanafos.com), ** 숭실대학교 컴퓨터학부 교수(mun@computing.ssu.ac.kr)
논문번호 : KICS2007-03-101, 접수일자 : 2007년 3월 6일, 최종논문접수일자 : 2007년 4월 10일

되면서 유무선 서비스 타입에 관계없이 다양한 종류의 서비스 이용이 가능해야 하는 필요가 증가하고 있다. 따라서, 기존 IPv4 망에서 널리 사용된 여러 서비스를 그대로 제공해야 하며 이동 환경에 적합하도록 설계된 새로운 서비스가 제공되어야 한다. 이에 대표적인 인터넷 서비스 중 하나인 VPN을 이동 환경에서 그대로 사용할 수 있도록 하는 연구가 진행되어 왔다. 예를 들면, 홈 에이전트를 인터넷과 인트라넷간의 게이트웨이로서 활용하는 방안이 있다[1,2].

VPN 이동 사용자가 인트라넷 내부에서 외부로 이동 할 때 VPN의 보안 정책을 만족하는 동시에 이동 노드의 홈 에이전트로 현재 위치를 등록할 수 있도록 하는 메커니즘이 제공되어야 한다. VPN 게이트웨이는 사전에 SA(Security Association) 관계가 설정된 노드로부터의 접근을 허용하고 나머지는 차단하거나 제한된 엑세스를 제공한다. 이동 노드가 외부 이동 중 외부 에이전트(FA)로부터 구성한 CoA(Care-of-Address) 주소는 VPN 게이트웨이와 사전 SA 관계성을 가지지 않으므로 이동 노드가 보내는 바인딩 등록 메시지는 VPN 게이트웨이에 의해 차단되거나 홈 에이전트에 대한 엑세스가 제한된다. 사전에 FA와 SA를 설정하고 FA가 관리하는 주소를 허용하도록 VPN 게이트웨이 설정이 가능하지만 이동 노드의 이동 경로 예측이 어렵고, 추가적인 보안 위협이 발생한다. 인터넷에서 홈 영역으로 들어올 때, 이동 노드는 홈 망의 자원을 엑세스할 수 있는 권한을 얻기 위해 인증 절차를 우선적으로 수행해야 한다. 안전한 방법으로 이동 환경을 위해 최적화된 확장 구조를 제공하므로 써 권한, 검증, 과금 및 견고한 인증 서비스를 제공하기 위해 본 논문에서는 Diameter 인증 방식[3]을 사용한다.

이 논문에서, 우리는 외부로부터 인트라넷으로의 엑세스를 위한 AAA 인증 및 키 분배를 제안하기 위해 Mobile IPv4에서 AAA 인증구조를 사용하는 인증 모델과 엔티티를 정의하고 외부 이동 중인 VPN 사용자가 인트라넷에 접근하기 위한 인증 시나리오를 제시한다.

Ⅱ. VPN 환경에서의 AAA 인증 모델과 엔티티

그림 1은 이동 노드(MN)가 인트라넷 내부에서 외부로 이동한 경우, 이동 노드와 외부 에이전트(FA)간의 상호 인증, 인트라넷 내부의 홈 에이전트(HA)로의 성공적인 바인딩 등록, 상대 노드와의 통신 재개를 위한 서비스 모델과 역할에 따른 엔티티를 보여 준다.

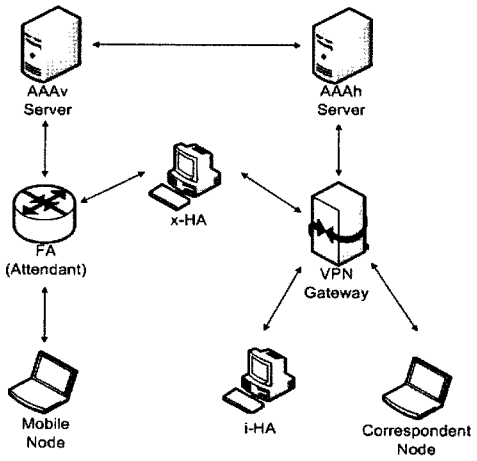

그림 1. VPN 환경에서 AAA 인증 모델

이동 노드는 MIPv4에서 정의한 이동 노드의 기능을 가지는 노드로서 외부로의 이동 시 외부 링크 및 노드 인증을 위해 NAI(Network Access Identifier)[4], 홈 주소 등의 인증 정보를 제공하며 Mobile IPv4에서 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. AAAv는 외부 링크 사용을 위한 인증 서버로서 이동 노드가 이동 후 외부 망의 자원의 사용 여부를 결정하는 엔티티이다. 이동 노드로부터 인증 요청을 수신하면 먼저 Attendant를 인증하고 메시지의 NAI나 홈 주소를 통해 이동 노드의 홈 도메인에 존재하는 AAA 인증 서버로 전송한다. i-HA와 x-HA는 각각 VPN 인트라넷 내부와 외부에 존재하는 홈 에이전트로서 이동 노드의 현재 위치 탐지 및 바인딩 등록을 처리한다. VPN 게이트웨이와 x-HA간에는 사전 SA를 설정한다.

Ⅲ. 이동 노드 인증 및 홈 등록

Mobile IPv4 기술 사양에는 CoA에 대한 SA를 사전에 설정하기 위한 방법이 존재하지 않는데 이는 CoA가 임시적으로 사용되며 망을 이동할 때 FA(Foreign Agent)로 반납되기 때문이다. 이 논문은 이동 노드를 인증하고 홈 에이전트로 바인딩 등록을 위한 방법을 제시한다. 이동 노드가 보내는 패킷이 VPN 게이트웨이를 경유해 홈 에이전트로 전

송되도록 하기 위해 패킷을 직접 VPN 게이트웨이로 보내는 것은 의미가 없는데 이는 수신되는 패킷의 IP 주소와 이동 노드의 CoA간에 SA가 설정되지 않기 때문이다.

3.1 관련

이동 노드의 위치에 따른 접근 모드는 참고문헌[5]에 정의되는데 이동 노드가 인트라넷 외부에 존재하는 동안 외부 에이전트나 DHCP(Dynamic Host Configuration Protocol) 서버로부터 CoA를 구성하는 각 경우에 대한 엑세스 시나리오인 'fvc'와 'cvc' 모드를 기술하고 있다. 이동 노드의 현재 위치를 알아내기 위해 이동 노드는 바인딩 등록 메시지를 x-HA로 보내고 응답을 확인한다. 만일 방문 망의 외부 에이전트로부터 CoA를 구성한 경우, 'fvc' 모드를 처리하기 위해 다른 절차가 실행된다[5][6]. 그러나 이 방법은 인증을 제공하지 않는다. 따라서 안정된 방법으로 인증을 제공하기 위해 이 논문에서는 AAA 인프라 구조인 Diameter를 모델에 통합시킨다.

3.2 VPN에서 AAA를 사용한 이동노드 인증 및 홈 등록

제안된 인증 방법에서는 그림 2와 같은 메시지 교환 절차가 발생한다.

그림 2에서 AnT(AAAh+Tunneling)는 이동 노드의 홈 AAA 서버로서 인터넷 상에 존재하며 VPN 게이트웨이와의 사전에 정의된 IPsec-ESP 터널을 갖는다. FA(Attendant)와 x-HA간에는 동적인 터널링 관계성이 존재하고, x-HA와 VPN 게이트웨간에 SA가 사전에 구성된다. x-HA와 i-HA는 위치 파악을 위한 기준점으로서 각각 인터넷과 인트라넷 에 존재 한다.

AnT는 사전에 협의된 로밍 계약에 따라 AAAv의 인증 요청을 처리하고, 노드 인증 확인 응답을 해 준다. 또한 인트라넷으로의 진입을 위한 엔티티로서 노드가 이동 시 매번 IKEv1/IKEv2 교환을 통해 IPsec-ESP 협상을 수행할 필요 없이 AnT 엔티티가 사전에 미리 구성한 IPsec-ESP 협상키를 제공함으로써, 이동 시 발생하는 빈번한 키 협상 오버헤드를 줄이며, 안전하게 패킷을 암호화할 수 있도록 해준다. 이동노드가 다른 망으로 이동한 경우, 자신의 현재 위치를 파악할 필요가 있다. 이는 인트라넷 내부와 인트라넷 외부의 존재 여부에 따라 홈 망의 자원에 대한 엑세스 방식이 달라지기 때문이다. 이동 노드는 이동 시 x-HA로 바인딩 갱신을 시도하며, 성공하는 경우 노드의 현 위치는 인터넷 상으로

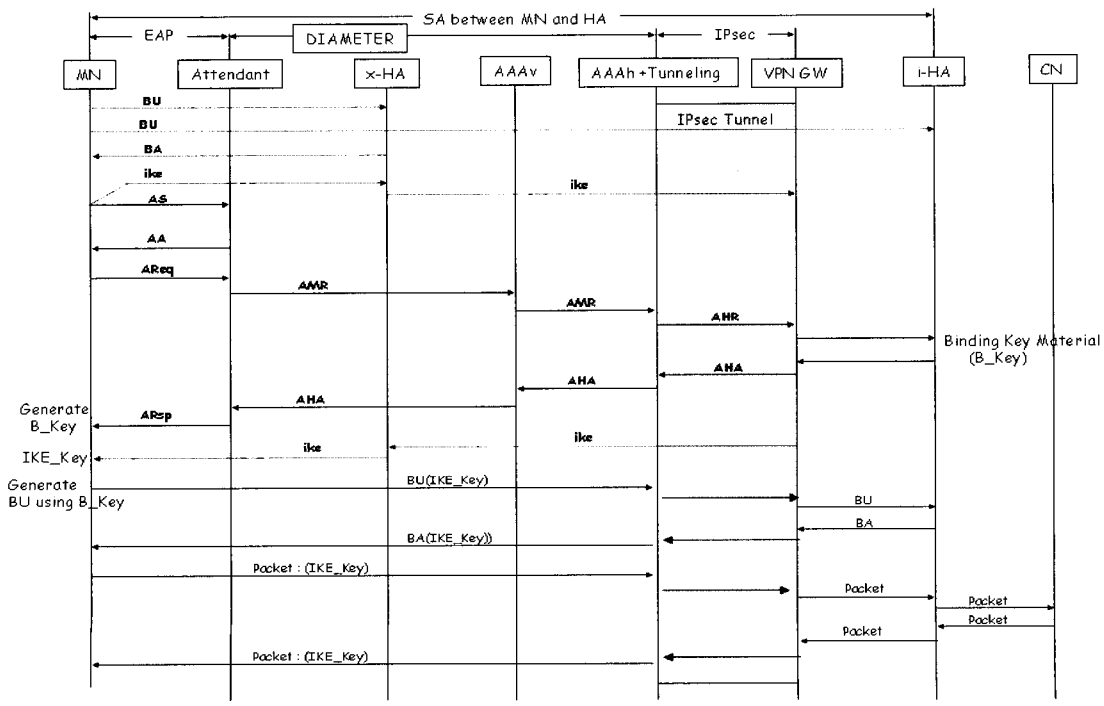

그림 2. 제안된 인증 모델에 대한 메시지 교환 절차

결정된다. 만일 실패한다면 이동 노드는 인트라넷 내부에 존재하게 된다.

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-HA는 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. 상대노드(CN)는 이동 노드와 세션을 유지하고 있는 노드로서 인트라넷 내부의 노드이거나 인터넷 상의 노드일 수 있다.

AnT 엔티티는 MN을 인증하고 VPN 게이트웨이를 통해 인트라넷 내부로 접근할 수 있는 경로 제공 역할을 수행하는 복합 엔티티이다. AnT는 VPN 게이트웨이를 항상 알고 있으며 설정된 SA가 아직 유효한지 여부를 검사하기 위해 메시지를 교환함으로써 SA의 일관성을 유지한다. AnT와 VPN 게이트웨이간의 모든 트래픽은 수동 또는 자동으로 구성되는 SA에 의해 보호된다. AnT의 또 다른 역할은 AAA 기능을 수행하는 것이다. AnT는 접근하려 하는 이동 노드의 메시지를 인증하고 VPN 게이트웨이를 통해 인트라넷으로 전송되는 바인딩 등록 메시지의 pass-thru 정보를 포함하는 SA 설정 정보를 이동 노드로 제공한다. 키 생성 재료를 얻기 위해 이동 노드는 인트라넷을 엑세스할 때 우선 AnT에 의해 인증되어야 한다. 이동 노드는 i-HA와 x-HA로 동시에 바인딩 등록 메시지를 전송함으로써 현재 위치를 알 수 있다. 만일 i-HA로부터 응답이 수신되는 경우, 현재 위치는 인트라넷으로 결정되고 아닌 경우 인터넷상의 임의의 지점으로 결정된다. 위치를 알아낸 후 이동 노드는 VPN 게이트웨이와 AnT 간에 설정된 IPsec-ESP 터널의 키 재료를 획득하기 위해 AnT로 IKE 메시지를 전송한다. 인증은 Diameter 프로토콜의 메시지 교환 작업에 의해 제공된다. 먼저 이동 노드는 인증 요청(AReq) 메시지를 외부 에이전트(Attendant)로 보내는데 여기에는 로컬 챌런지, 이동 노드의 NAI, 재실행 방지 식별값(RPI: Replay Protection Indicator), 이동 노드의 홈 주소, 이동 노드의 CoA, 홈 에이전트 주소, 보안 파라메터(SecureParam_I), Credentials, 키 요청 페이로드가 포함된다. 인증 완료 후 이동 노드는 인증 응답 메시지(ARsp)를 수신하는데 여기에는 로컬 챌런지, 재실행 방지 식별 값, 이동 노드의 홈 주소, 홈 에이전트 주소, 보안 파라메터(SecureParam_R), Credentials와 키 응답 페이로드가 포함된다. 이동 노드는 수신된 Secure Param_R과 IKE 키로부터 키 생성 재료를 얻고 이를 통해 내부 홈 에이전트에 대한 바인딩 키를 생성한다.

Ⅳ. 성능평가

4.1 비용 분석 모델

비용 분석은 VPN 환경에서 AnT 엔티티를 경유한 인증 및 등록 비용계산을 근거로 하며 각 노드에서의 처리에 따른 지연 시간과 분실 패킷 비용이 포함된다. 제안된 모델에서 엔티티 간의 거리는 그림 3에 표시된 바와 같다. 비용 계산을 위해 참고문헌 [7]의 접근 방법을 적용한다. 상대노드(CN)는 λ의 비율로 이동 노드로 패킷을 전송하고 이동 노드는 μ의 비율로 다른 서브넷으로 이동한다고 가정한다. 이 논문에서 제어패킷과 데이터 패킷의 길이를 각각 l_c 와 l_d 로 정의하고 엔티티에서의 제어 패킷 처리 비용을 r 로 정의한다.

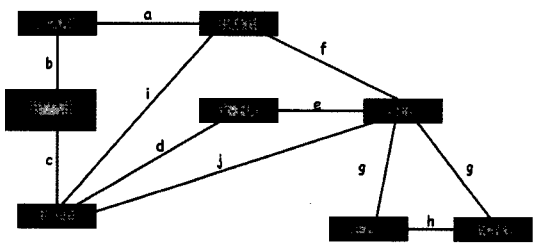

그림 3. VPN 환경에서 AAA인증 및 홈 등록 모델

논문에서는 인터넷을 통해 연결되는 상대적으로 큰 거리 값을 가지는 외부 링크와 로컬 서브넷이나 도메인 영역 내부에서 연결되는 작은 거리 값을 가지는 내부링크로 구분하는데 이는 링크 가중치 값이 링크의 타입에 의해 달라짐을 나타낸다. 같은 서브넷이나 도메인에 존재하는 내부링크의 가중치 값은 2로 주어지는데 이는 전송 오버헤드는 거리와 미디어 타입에 의해 결정됨을 말해 준다. 긴 거리를 가지는 외부링크의 가중치는 6으로 주어진다.

4.1.1 트래픽 모델

비용 측면에서 모델을 설명하기 위해 다음과 같은 트래픽 특성을 정의한다.

특성 1) 방문 도메인에 존재하는 로컬 AAA 서버는 20개의 서브넷(셀)을 처리할 수 있고 반경은 최대 1km라고 가정한다. 한 서브넷에 존재할 수 있는 노드의 총 개수는 200이며 이중 100은 고정 노드이고 나머지 100은 이동 노드로 가정한다. 이때 이동 노드의 80 퍼센트는 보행 속도로 이동하고 나머지 20퍼센트는 차량을 타고 이동한다고 가정한다.

특성 2) 한 서브넷에서 다른 서브넷으로 보행 이동하는 평균 비율은 0.01이고 차량의 경우 0.2로 정의된다[3]. 보행 이동 자는 가우스 분포에 따라 시간당 5km를 이동하고 차량의 경우 20km를 이동한다[8].

특성 3) 위의 가정에 의해, 이동 노드가 한 서브넷에 머무는 평균시간은 보행 속도로 이동하는 경우와 차량 속도로 이동하는 각각의 경우에 대해 12분과 3분으로 계산된다. 마찬가지로, 이동 노드가 도메인에 머무는 평균시간은 각각 240분과 60분으로 계산된다.

특성 4) 이동 노드와 상대노드간의 활성화된 세션의 평균 개수를 5로 정의하고 데이터 패킷과 제어 패킷의 평균 길이를 각각 1024바이트와 100바이트로 정의한다. 첫 번째와 두 번째 세션은 93$Kbyte$/sec 속도의 평균 전송량을 가지는 파일 전송 세션이고, 세 번째와 네 번째는 182$Kbyte$/sec의 전송량을 가지는 멀티미디어 트래픽 세션이며 마지막 세션은 그룹웨어 세션으로서 2.5$Kbyte$/sec의 전송량을 가진다고 정의한다. 가정에 의해 이동 노드는 초당 110.5 $Kbyte$의 패킷을 수신하고 한 서브넷에 머무는 동안 수신하는 패킷의 양은 이동 노드가 보행 속도로 움직이는 경우와 차량 이동 하는 각 경우에 대해 79.56 $Mbyte$와 19.89$Mbyte$로 계산된다.

특성 5) 한 Attendant에 의해 서비스되는 평균 노드 수를 45라고 정의하고 노드는 최대 11$Mbps$로 동작하는 Attendant(AP)와의 무선 링크 대역을 공유한다.

특성 6) Attendant와 라우터간의 유선 링크는 10 $Mbps$로 동작한다.

특성 7) 라우터와 로컬 AAA 서버간의 유선 링크 속도는 100$Mbps$이다.

특성 8) 라우터와 x-HA간, x-HA와 VPN 게이트웨이간, AnT와 VPN 게이트웨이간의 종단 간 지연은 약 80ms라고 가정한다.

특성 9) AnT와 VPN 게이트웨이는 같은 도메인에 소속되므로 이들 간의 유선 링크는 100$Mbps$로 동작한다고 가정한다.

특성 10) VPN 게이트웨이와 i-HA간, i-HA와 상대 노드(CN)간의 링크 속도는 10$Mbps$로 가정한다.

다양한 파라메터와 처리 시간에 따른 각 프로토콜 계층별 패킷 오버헤드의 길이는 참고문헌 [9]에 기술되어 있다. 논문에서는 한 엔티티로부터 다른 엔티티로의 전송 및 처리 시간을 측정하기 위해 참고문헌 [9]의 계산 결과를 인용하는데 물리층, MAC층, IP층 및 UDP층 처리에 대해 각각, 192μs, 136μs, 80μs 및 32μs의 처리 오버헤드를 가진다.

4.1.2 AAA 인증과 바인딩 등록 비용 분석

C_{total}은 전체 비용으로서 인증 및 홈 등록이 진행되는 동안 분실되는 패킷 비용과 홈 등록 후에 상대 노드와의 트래픽 송수신 비용의 합으로써 수식 1과 같이 나타낼 수 있다.

$$C_{total} = C_{loss} + C_{CN} \tag{1}$$

1) 패킷 전송 오버헤드

현재 위치를 판단하기 위해 이동 노드는 i-HA와 x-HA로 동시에 바인딩 등록 메시지를 보내는데 여기서 이동 노드와 Attendant간의 무선 링크는 한 개의 Attendant가 서비스 하는 평균 이동 노드의 수를 45로 가정했으므로 0.244$Mbps$ (11$Mbps$/45)의 속도를 제공한다. 또한, 물리 층과 MAC 계층의 처리 오버헤드($\approx 0.34ms$)가 추가되는데 이는 2계층 처리를 한 후 로컬 라우터로 메시지를 포워딩하기 때문이다. "트래픽 모델"의 정의에 의해 Attendant와 라우터간의 링크는 10$Mbps$의 속도를 제공하고 라우터에서 x-HA로의 전송은 80ms만큼 지연된다. 따라서 전송 및 처리 시간은 수식 2와 같이 구해진다.

$$t(MN \Leftrightarrow x - HA) = \frac{(l_c * 8bit)/1Mbit}{0.244Mbps} + 0.34ms + \frac{(l_c * 8bit)/1Mbit}{100Mbps} + 80ms \tag{2}$$

제어패킷이 100 바이트의 길이를 갖는다고 가정했으므로, 이동 노드가 x-HA로 바인딩 등록 메시지를 보내는데 걸리는 평균 시간은 $t(x-HA)=t_d=83.62ms$ 이다. 마찬가지로, 패킷을 전송하는 각 링크에 대한 시간은 다음과 같이 계산된다.

표 1. 링크에 대한 계산 시간

Link	Time
t_a	$79.9ms$
t_b	$0.418ms(l=l_c), 1.14ms(l=l_d)$
t_c	$3.2ms(l=l_c), 32.78ms(l=l_d)$
t_d	$83.62ms$
t_e	$80ms$
t_f	$0.0078ms(l=l_c), 0.08(l=l_d)$
t_g	$0.078ms(l=l_c), 0.8ms(l=l_d)$
t_h	$0.078ms(l=l_c), 0.8ms(l=l_d)$
t_i	$83.62ms(l=l_c), 113.92ms(l=l_d)$
t_j	$83.62ms(l=l_c), 113.92ms(l=l_d)$

2) 비용 분석

C_{loss}는 위치 발견, AAA 인증 및 바인딩 등록 처리 시간 동안 분실되는 패킷 비용의 합으로서 다음 수식과 같이 나타낼 수 있다.

$$C_{loss}=C_{loss-detection}+C_{loss-\max(AAA,IKE)}+C_{loss-BU} \quad (3)$$

각 단계에 대한 분실 비용은 수식 4와 같이 단계 처리를 위한 시간과 평균 패킷 처리 비율을 곱으로 얻어질 수 있다.

$$C_{loss}=\lambda^*(t_{detection}+\max(t_{AAA},t_{IKE})+t_{BU}) \quad (4)$$

현재 위치를 파악하기 위해 이동 노드는 i-HA와 x-HA로 바인딩 등록 메시지를 보내고 만일 인트라넷 외부에 존재하는 경우 이동 노드는 x-HA로부터 응답을 수신한다. 그러므로 위치 파악 시간은 $t_{detection}=2t_d+3t_r$로 표현할 수 있는데 여기서 t_r 은 물리 층에서 전송 층 오버헤드를 모두 더한 값이므로 $0.44ms$ 이다. 그러므로 이동 노드의 현재 위치를 파악하기 위해 소요된 시간은$t_{detection}=2*38.62ms+3*0.44ms=78.56ms$ 이다. t_{AAA}은 $2(t_a+t_b+t_c+t_f+t_g)+13t_r=179.32ms$로 얻어진다. t_{BU}는 홈 등록 기간 동안 소요된 시간으로서 $t_{BU}=2(t_i+t_f+t_g)+7t_r=170.48ms$이다.

정리하면 전체 분실 패킷의 비용은 수식 5와 같다.

$$C_{loss}=\lambda^*(4(t_c+t_f+t_g)+2(t_a+t_b+t_d+t_i)+23t_r)=\lambda^*428.36ms \quad (5)$$

트래픽 모델에 의해 이동 노드의 평균 보행 및 차량 이동에 대해 각각 0.8(μ=0.01)와 4(μ=0.2) 노드가 이동하고 λ는 110.5$Kbytes/s$ 이므로, C_{loss}는 보행 이동시 37.86$Kbyte$, 차량 이동시 189.32$Kbyte$가 된다. C_{CN}은 서브넷에 머무는 동안 수신 패킷을 처리하는 비용으로서 수식 6과 같다.

$$C_{CN}=\lambda^*2(t_l+t_f+t_g)=\lambda^*2(114.45ms+0.08ms+0.81ms)=\lambda^*230.68ms \quad (6)$$

3) 보행 및 차량 이동 노드에 대한 분실 패킷 비용

기존 방식의 'cvc'와 'fvc' 모드에 대해 동일한 가정과 트래픽 모델을 적용했을 때 분실 패킷의 비용은 수식 5에 의해 계산된다. 그림 4는 이동 노드가 보행 속도로 움직이는 이동 특성을 가질 때 기존 방법과 제안된 방법들 간의 비용 변화 차이를 보여 준다.

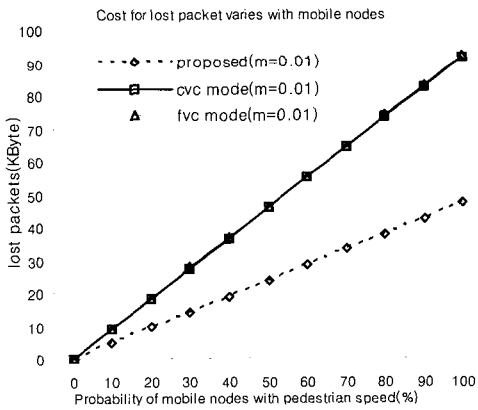

그림 4. 보행 이동 노드에 대한 패킷 분실 비용 변화

그림 5는 이동 노드가 차량 속도로 움직이는 특성을 가질 때 기존의 'cvc','fvc' 모드와의 비용 변화를 보여 준다.

그림 5에서 나타낸 바와 같이, 분실 패킷의 수는 이동 노드의 수를 100으로 가정했을 때 한 서브넷에서 다른 서브넷으로 이동하는 노드수에 비례하여 증가한다. 'cvc'와 'fvc' 모드는 거의 동일한 비용 변화량을 보이지만 제안된 방법의 경우 기존 방법과 비교할 비용 면에서 보다 경제적임을 알 수 있다.

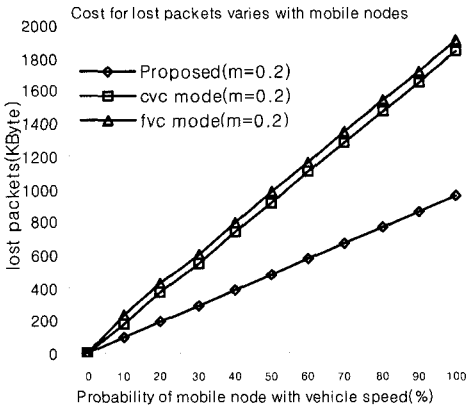

그림 5. 차량 이동 노드에 대한 패킷 분실 비용 변화

4) PMR에 따른 비용

PMR(Packet to Mobile Ratio)는 이동 노드의 트래픽으로서 이동당 송수신되는 패킷의 수로 정의하며 $PMR(\rho)=\lambda/\mu$로 정의할 수 있다. 여기서 λ는 평균 패킷 양을 의미한다. 가정에 의해 이동 노드는 평균 5개의 세션을 유지하고 있고, 이때 데이터 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. 이동 노드가 한 서브넷에 도착할 확률은 포아송 분포를 따르며[10] 다음 수식과 같다.

$$P(\gamma)=\frac{e^{-\eta}\eta^{x}}{x!} \qquad (7)$$

여기서 x는 이동 노드의 수, η은 다른 서브넷으로의 평균 이동 비율로서 보행자 및 차량속도의 이동 노드에 대한 이동 사건 발생에 대한 기댓값이다. 가정에서 한 서브넷에 존재할 수 있는 최대 노드의 개수는 200이며, 이중에 이동특성을 가지는 노드는 100개이다.(보행 이동 노드=80, 차량 이동 노드=20) 이때, 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.

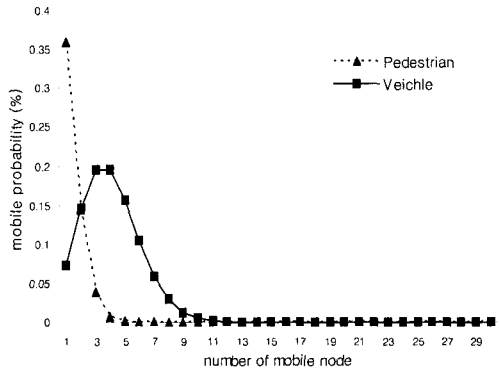

그림 6. 보행/차량 속도에 따른 이동 확률

그림 6은 한 도메인에 존재하는 이동 노드의 수에 따른 보행 및 차량 속도의 이동 노드에 대한 도착 확률을 보여 준다. 전체 이동 노드의 수가 증가하면 보행이동 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.

PMR 값의 변동을 기준으로 이동 노드와 상대 노드간의 트래픽 특성을 고려하여 성능을 분석하였다. 이동 노드가 외부에서 이동하는 중에 상대 노드와 교환하는 데이터 트래픽의 평균 길이를 각각 1024 바이트와 100 바이트를 기준으로 PMR 변화량에 따른 비용 증가를 그림 7과 같이 그래프로 나타내었다.

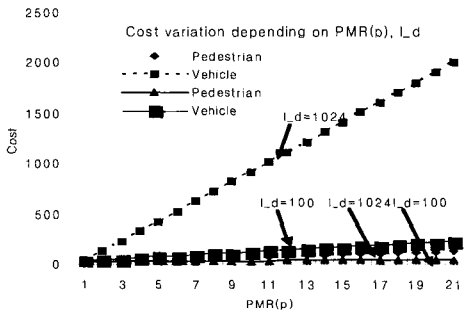

그림 7. 트래픽 및 PMR 변화에 따른 비용 변화

먼저 이동 노드가 보행자 속도로 이동하는 비율을 따를 때 데이터 패킷의 평균 길이의 변동은 전체 비용 증가에 크게 영향을 주지 않지만, 차량의 이동 속도로 이동하는 특성을 가질 때 데이터 패킷의 평균 길이는 전체 비용 증가에 크게 관여하게 된다. 1024 바이트의 평균 데이터 트래픽 특성을 가지는 경우 PMR 값이 증가함에 따라 인증 및 홈 바인딩 등록비용은 급격히 증가한다. 이는 빈번한 이동 발생 시 데이터 길이가 비용에 크게 영향을 줌을 알 수 있다. 그림 7의 그래프는 차량의 속도로 이동하는 경우와 보행자의 속도로 이동하는 경우 데이터 패킷의 평균 길이를 고려한 PMR 증가에 따른 비용 정규화(Normalization) 변화율을 보여 준다. 보행자 속도로 이동하는 경우 PMR 증가에 완만하게 비용 율이 증가하는 반면 차량의 이동 속도로 이동하는 특성을 가지는 경우 PMR 값이 증가하면 초기에 급격한 비용 율 변화를 보여준다. 또한 PMR 값이 큰 경우 두 가지 이동 특성에 따른 비용 변화율은 비슷한 값을 보이게 된다.

V. 결 론

이 논문에서는 VPN과 Mobile IPv4가 공존할 때 VPN 게이트웨이 에 의해 보호되는 인트라넷으로의 접근 방법을 제안하였다. 문제점을 분석하기 위해 이동 노드의 현재 위치에 따라 'cvc', 'fvc'등 서로 다른 엑세스 모드를 제공하는 기존 방법을 기술하였는데 문제점은 이동성 제공에 있어 가장 먼저 수행되어야 할 인증 기능을 제공하지 않는다는 점이다.

본 논문에서는 인증 및 경로 제공의 다중 역할을 담당하는 복합 엔티티인 AnT를 제안하였다. 이동 노드가 인트라넷 내부와 외부 망을 자주 이동하는 경우 생기는 주요 장애물은 매번 이동 시 마다 자신의 현재 위치를 i-HA에 등록해야 한다는 것이다. 그러나 VPN 게이트웨이는 이동 노드의 CoA와 SA가 존재하지 않고 이로 인해 이동 노드가 전송하는 패킷은 폐기되고 서비스는 중단된다. AnT와 VPN 게이트웨이간의 SA는 AnT에 이상이 발생한 경우 관리자에 의한 수동적 변경, 라이프타임 만료에 따른 재 갱신 등을 제외하고는 변경되지 않는데 이는 AnT는 고정 노드이고 사전에 VPN 게이트웨이와 미리 정의된 SA 관계성을 유지하기 때문이다. AnT는 이동 노드가 보내는 패킷이 VPN 게이트웨이를 통해 인트라넷 내부로 안전하게 전달될 수 있도록 VPN을 경유하는 경로 제공자 역할을 수행한다. 따라서 이동 노드가 매번 이동할 때 마다 IKEv2등의 방법으로 SA를 재설정하는데 드는 오버헤드를 제거할 수 있다.

본 논문에서는 분실 패킷 비용을 분석하고 보행 또는 차량 이동 특성, 이동 노드가 한 서브넷에 머무는 시간, 서브넷의 규모, Attendant의 처리량, 데이터 및 제어 패킷의 길이, 이동 중에 이동 노드가 유지하고 있는 세션의 개수, 이동 노드가 상대 노드로부터 수신하는 트래픽 등 다양한 요소에 따른 비용 변화를 분석하였는데 분석결과, 본 제안 방법은 기존 방법과 비교했을 때 약 40% 가까이 비용 절감 효과를 얻을 수 있었다.

참 고 문 헌

[1] F. Adrangi, K. Leung, "Mobile IPv4 Traversal Across IPsec-based VPN Gateways. draft-adrangi-mobieip- vpn-traversal-02.txt," Internet draft, IETF, Jul. 2002.

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

[3] A.Bosselaers, "Fast Implementations of Cryptographic Algorithms on the Pentium, "http://www.esat.kuleuven.ac.be/~bosselae/fast.html.

[4] A. Hess, G.Shafer, "Performance Evaluation of AAA/Mobile IP Authentication," Proc. Of 2nd PGTS, Sep. 2002.

[5] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann, "Diameter Mobile IPv4 Application," RFC4004, Aug. 2005.

[6] P. Calhoun, C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4," RFC2794, Mar. 2000.

[7] S. Vaarala, "Mobile IPv4 Traversal Across IPsec-based VPN Gateways. draft-ietf-mobileip-vpn-problem-solution-02.txt," Internet draft, IETF, Jun 2003.

[8] H. Ohnishi, K.Suzuki, "Mobile IPv6 VPN using Gateway Home Agent. draft-ohnish-mobileip-v6vpngateway-01.txt," Internet draft, IETF, Oct. 2002.

[9] R. Jain, T. Raleigh, C. Graff, "Mobile Internet

Access and QoS Guaranttes using Mobile IP and RSVP with Location Registers," in Proc. 3rd Nordic Sem., paper 9.4, Corpenhagen, Denmark. Sep. 1998.

[10] L. Kleinrock, Queueing Systems, Volume1: Theory, John Wiley&Sons, 1975.

김 미 영 (Miyoung Kim) 정회원

1992년 : 전주우석대학교 전산학과 졸업(학사)

1995년 : 광운대학교 대학원 전산학과 졸업(석사)

1995년~1997년 : (주)필컴시스템 개발부 근무

2000년~2005 : 숭실대학교 대학원 컴퓨터학과 졸업(박사)

2005년~현재 : 숭실대학교 정보미디어기술연구소

<관심분야> IPv6, Mobile IP, 네트워크 보안

문 영 성 (Youngsong Mun) 정회원

1993년 : 연세대학교 전자공학과 졸업(학사)

1986년 : Univ. of Alberta 전자공학과 졸업(석사)

1993년 : Univ. of Texas, Arlington 전산학과 졸업(박사)

1994년~현재 숭실대학교 컴퓨터학부 교수

<관심분야> IPv6, Mobile IP, 보안, 그리드