Mobile IPv6에서 AAA를 이용한 이동노드와 홈 에이전트간의 최적화된 인증 방안

(An Optimized Authentication Method between Mobile Node and Home Agent using AAA in Mobile IPv6)

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

요 약 이동 노드가 여러 도메인에 걸쳐 서브넷들 간을 이동하는 경우 Mobile IPv6 서비스는 보안상 취약성을 드러낸다. AAA 인프라 구조는 ISP가 다른 도메인으로부터 온 이동 사용자를 인증할 필요가 있을 때 권고되는 기반 구조이다. AAA 서비스의 기본 요구사항 외에 이동 서비스 지속성을 위해서는 이동 환경에 적합하도록 인증 지연 및 AAA 메시지 부하가 최소화되어야 한다. 이 논문에서는 Mobile IPv6에서 AAA 인프라 구조를 지원하는 로밍 서비스를 고려하고 효율적인 방법으로 이동 노드를 인증할 수 있도록 하는 위임 기능을 고려한 인증 방법을 제안한다. 제안된 구조는 비용 분석을 통해 그 효율성을 검증하였는데 결론적으로 위임 기능이 동작하는 상황에서 이동 노드가 빠르게 로밍하는 경우 50% 이상의 성능 향상을 보였다.

키워드 : Mobile IPv6, AAA, 인증

Abstract A Mobile IPv6 services exposes its vulnerability when a mobile node is roaming the subnets belonging to the different domains. The AAA infrastructure is strongly recommended when the ISPs need to authenticate the mobile user comes from the different domains. In addition to the basic requirements for the AAA service, the authentication latency and AAA message overhead should be minimized for the continuity of the mobile service. This paper considers the roaming service with AAA infrastructure in Mobile IPv6 and proposes an authentication scheme using delegation to authenticate the mobile node with effective manner. The effectiveness of the proposed scheme is confirmed using the cost analysis. The result shows at least 50% of performance enhancement when the MN is roaming fast under the control of the delegation.

Key words : Mobile IPv6, AAA, Authentication

1. 서 론

본 논문은 이동 노드가 외부 망에 접근하기 위해서 수행해야 할 인증 절차에 대해서 기술한다. 이동 노드가 서로 다른 도메인 간을 이동하는 경우, AAA와 같은 글로벌 인증 인프라 구조를 안정적으로 제공하지 않는다면, 외부 링크의 자원 사용에 관한 권한을 얻지 못하므로 진행 중인 세션은 중단되고 서비스 이동성 제공은 불가능해진다. IETF 문서인 Mobile IP 기고서에서는 서로 다른 도메인 간에 이동 노드가 이동하는 경우에 대한 인증 방법에 관해서는 다루지 않고 있다[1]. 예를 들어, 802.11 무선 랜 망에서 이동 노드가 AP에 접속을 하는 경우 먼저 링크 사용에 관한 권한을 얻어야 한다[2]. 만일 이 과정이 실패하면, 이동 노드는 외부 링크를 사용할 수 없으며, 진행 중인 전송 세션은 모두 중단된다. 그러므로 외부 링크 상에서도 지속적인 이동 서비스를 가능하게 하려면 외부 링크 자원 사용에 관한 도메인 간 사전 로밍 협의 및 인증 방법을 제공해야 한다. 본 논문은 이동 노드가 동일한 도메인 내의 여러 서브넷을 빠르게 이동하고 있는 상황에서 인증 절차를 간소화함으로써 이동 노드가 진행 중인 세션에 대한 신속한 서비스 재개를 가능케 하기 위한 방법을 기술한다. 이

· 이 논문은 2002년도 학술진흥재단의 지원에 의하여 연구되었음 (KRF-2002-041-D00487)
† 정 회 원 : 숭실대학교 컴퓨터학과
mizero31@sunny.ssu.ac.kr
†† 종신회원 : 숭실대학교 컴퓨터학과 교수
mun@computing.ssu.ac.kr
논문접수 : 2003년 4월 17일
심사완료 : 2003년 8월 29일

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

2. AAA 인증 모델 및 엔티티

아래의 그림은 AAA(Diameter) 인증 구조[3]를 사용해서 이동 노드와 Attendant 간에 세션 키를 교환하고 이동 노드의 현재 위치 정보를 홈 에이전트로 등록하기 위한 AAA 기반의 통신 모델을 나타낸다.

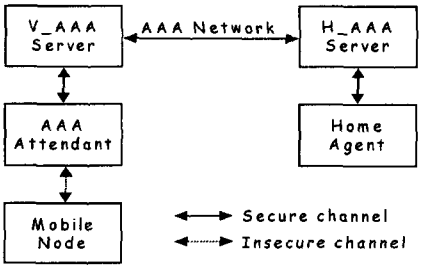

그림 1 AAA 인증 모델

바인딩 등록 절차를 정상적으로 수행하기 위해서, 인증 과정은 이동성 제공을 위한 다른 절차들보다 우선되어야 하며, 바인딩 키의 생성 및 분배는 H_AAA나 홈 에이전트에 의해서 수행될 수 있다[3]. AAA 인증 모델에서는 이동 노드(MN), 홈 에이전트(HA), Attendant, V_AAA 및 H_AAA 등 5개의 엔티티를 정의하고 있다. AAA 엔티티는 DIAMETER 고유의 인증 기능을 수행하며, 그 외의 엔티티는 이동 서비스를 위한 바인딩 등록 절차를 처리한다. 이동 노드와 홈 에이전트는 [1]에서 정의한 모든 기능을 만족한다. Attendant는 이동 노드가 외부 링크에서 가장 먼저 접속하게 되는 외부 엔티티로서 이동 노드가 전송하는 패킷에 대한 통과, 폐기, 보류 등의 정책을 수행할 수 있으며, AAA 서버를 통한 인증 성공시 패킷을 통과 시킬 수 있다. V_AAA는 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. H_AAA는 홈 도메인의 AAA 인증 서버로서, 이동 노드의 인증에 필요한 인증 정보들로 구성된 프로 파일을 관리하고 있다. 이동 노드가 보내온 인증 정보를 기반으로 이동 노드에 대한 인증 처리 과정을 진행하고 결과를 V_AAA로 전송한다. 만일 홈 망이 재구성된 경우(Network Renumbering) 동적인 홈 에이전트 발견[4] 절차를 수행할 수도 있다.

3. 최적화된 Mobile IPv6 인증 구조

3.1 관련 연구

[4]에서는 총 12 단계에 걸치는 Diameter 기반의 AAA 인증 방식에 관해 기술하고 있는데, 한 가지 위험 요소는 12 단계의 인증 메시지 처리와 더불어 바인딩 등록을 함께 처리하도록 하는 옵션인 '바인딩 내장(Embedded BU)' 옵션을 설정하는 것이다. 아직 이동 노드와 Attendant 간의 공유 키가 생성되지 않고, 인증이 완료되지 않은 상태에서 '바인딩' 정보가 내장된다면 이동 노드의 현재 위치 정보 및 홈 망의 정보가 공격자에게 쉽게 노출될 수 있기 때문이다[5]. [3]에서는 [4],[6]의 위험 요소인 '바인딩 내장' 옵션을 제거하고 각 단계별로 주고 받는 메시지의 옵션을 줄임으로써 보다 개선된 보안 기능을 제공하고 있다. 이동 노드가 바인딩 등록을 하기 전에 자신의 홈 도메인의 인증 서버 혹은 홈 에이전트를 통한 인증 기능이 수행되고 이동 노드와 Attendant에서 공유되어지는 세션 키 및 바인딩 갱신을 위한 바인딩 키가 분배 되어야 한다. 만일 이동 노드가 짧은 시간 동안에 여러 서브넷을 자주 이동한다면 이러한 12 단계는 매우 빈번하게 수행되므로, 이동 서비스의 지연이 많이 발생한다. 따라서 이동 노드의 이동 특성을 고려한 최적화된 인증 및 바인딩 등록 방법이 필요하다.

3.2 제안하는 위임 기능(delegation)을 갖는 AAA 구조

MN에 대한 키 재료 및 SA 문맥 관리를 V_AAA로 위임하기 위해 'delegation option'을 정의한다. 'delegation option'은 MN이 AReq 메시지를 통해 인증을 요청할 때 보내질 수 있다. 이동 노드가 다른 도메인에서 방문 링크를 접속한다면 공유 세션 키를 얻고 이동 노드의 현재 위치를 등록하기 위해서 [3],[4]에서 기술한 12 단계가 수행된다. 만일 이동 노드가 AReq 메시지에 'delegation option'을 추가해서 보낸다면, 이 메시지는 세션 키와 바인딩 키 재료들을 생성하고 분배하는 역할을 하는 H_AAA와 Home Agent 같은 엔티티에게 전달된다. 보안 문맥(security context)은 MN과 HA간의 SA에 대한 기능의 집합이다. 만일 AAA 엔티티가 MN과 HA 간의 SA와 동일한 보안 문맥을 가지고 있고, HA나 H_AAA가 V_AAA 엔티티로 SA 정보를 전송할 수 있다면, 보안 문맥 전송시 HA나 H_AAA에 의해서 설정된 라이프타임 값이 만료되기까지 인증 과정은 그 엔티티의 통제 하에 놓이게 된다. H_AAA가 키 재료를 관리할 권한을 가지고 있다면, MN을 인증하고 MN에 대한 세션 키를 생성하는데 사용되는 보안 문맥은 H_AAA가 m_AR에 대한 응답으로 h_AA를 보낼

때 전송된다. 보안 문맥을 포함하고 있는 메시지를 수신하게 되면, V_AAA는 보안 문맥(SAs, algorithms, hash functions, etc.)을 자신이 처리할 수 있는지의 여부를 판단하기 위해 자신의 처리 능력('capability')과 비교한다. 처리가 가능하다고 판단되면, V_AAA는 'delegation' 요청을 수락하고 처리하기 위해 자신의 'delegation' 항목 리스트에 MN에 대한 새로운 항목을 생성한다. V_AAA가 보안 문맥 처리를 위한 기능을 가지고 있지 않다면, delegation 요청은 무시되고, 메시지는 [3]과 [4]에서 정의한 대로 처리된다. 이동 노드의 이전 위치에서 같은 도메인 내의 다른 링크로 이동하는 경우, 'delegation' 요청 옵션이 설정되고, V_AAA는 이동 노드가 'delegation' 엔트리 리스트에 등록된 노드인지를 확인하게 된다. 만일 이동 노드에 대한 항목이 존재한다면 V_AAA는 이동 노드를 인증하고 보안 문맥에 따라서 세션 키를 생성한다. 'delegation' 절차가 완료된 후, V_AAA는 m_AR에 대한 응답으로, 세션 키, 키 재료 및 그 외의 보안 파라메터들을 포함하고 있는 h_AA 메시지를 전송한다. 'delegation entry'는 라이프 타임이 만료되기 전까지 V_AAA에 의해 유지되며 라이프타임이 만료되면, 'delegation' 항목은 'delegation' 항목 리스트에서 삭제된다. 처음 'delegation' 요청이 수락된 경우 사용된 V_AAA를 정확히 구별하고 선택하기 위해서, 본 논문에서는 '인증 경로'를 정의하고 있다. 인증 경로는 H_AAA와 V_AAA가 인증 요청 메시지에 대한 응답 시 포함하는 자신의 NAI로 구성되어 있으며, 외부 또는 홈 링크상에 하나 이상의 AAA 서버가 존재하는 경우 'delegation entry'를 유지하고 있는 인증 서버를 식별하기 위해 사용한다. 'delegation'이 사용되는 경우 이동 노드로부터 요청되는 인증 절차는 그림 2와 같이 수행된다.

단계 1에서 이동 노드는 다른 서브넷으로 이동 했을 때, AS 메시지를 보내서 Attendant를 찾는다. 만일

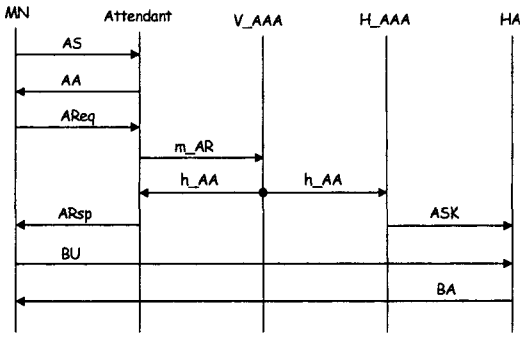

그림 2 제안된 위임 기능을 이용한 인증 메시지 처리 절차

Attendant로부터 응답이 없을때, 이 메시지는 이동 노드가 Attendant를 찾을 때까지 주기적으로 보낸다. 단계 2에서 Attendant가 AS 메시지를 수신하면, 인증이 완료될 때까지 사용될 로컬 챌린지를 포함하는 AA 응답을 이동 노드로 전송한다. 단계 3에서 이동 노드는 Attendant에게 세션 키 및 바인딩 키를 얻기 위해 AAA 프로토콜 동작 수행을 요청하는 AReq를 전송한다. 이 메시지에 포함되는 파라메터들로는 로컬 챌린지, MN 및 AAA 서버들에 대한 NAI(없으면 NULL), 넌스, MN의 홈주소, MN의 HA 주소, 메시지 인증 값, 위임 옵션 등이 포함된다. 단계 4에서 Attendant는 AReq 메시지로부터 데이타를 추출하고 데이타로부터 파라메터 집합(AVP)을 가지는 새로운 m_AR 메시지를 구성한다. V_AAA는 이 메시지를 받았을 때, 요청을 수락할지를 결정하기 위해 Attendant를 인증하고 메시지를 포워딩 할 H_AAA 서버를 찾기 위해 이동 노드의 NAI를 검증한다. 만일 이동 노드의 홈 도메인과 방문 도메인 간에 사전 로밍 계약이 체결되어 있지 않다면 인증 요청은 실패로 처리되고, V_AAA는 Action-AVP의 Result-Code-Option(NAI_ROAMING-INVALIDE)를 h_AA에 실어서 Attendant에게 보낸다. Attendant 인증 및 NAI 검증이 성공하고, 메시지에 'delegation-Option'을 가지는 Action AVP가 포함되어 있다면 V_AAA는 이동 노드의 엔트리가 존재 하는지를 알기 위해 'delegation entry'를 검색해야 한다. m_AR 메시지에는 Authentication-Path AVP(NAI-Option), Address AVP(Care-of-Address-Option, Home-Address-Option, Home-Agent-Address-Option), Security AVP(Authenticator-Option, Nonce-Option, Security-Parameter-Option), Action AVP(Delegation-Option) 등의 파라메터가 포함된다. 만일 엔트리가 존재하고 유효 시간이 아직 있다면, V_AAA는 세션 키를 아래와 같이 키 재료를 통해 계산할 수 있다.

session_key = prf(N_m | N_a, m_HoA, m_CoA, a_R), key_material = {Nonces(N_a, N_m), SPI, HASH,..} 여기서 N_a는 이동 노드의 홈 에이전트 또는 H_AAA 서버를 대신해서 V_AAA에 의해 생성된 넌스 값이다. a_R은 각각 요청 되어진 세션 키를 위한 V_AAA에 의해 생성된 랜덤 넘버이다. 랜덤 넘버와 넌스를 제외한 모든 파라메터는 이동 노드를 위한 'delegation list' 엔트리에서 보안 문맥(securiry context)으로부터 참조한다. 단계 5에서 V_AAA는 Attendant에게 키 재료와 세션 키를 생성하고 전달한다. 포함되는 파라메터로는 Security AVP(Authenticator-Option, Session-Key-Option, Key-Materials-Option, Nonce-Option, Ramdom-Number-Option), Action

AVP(Result-Code-Option) 등이 있다. 이 단계에서, V_AAA는 이동 노드의 H_AAA 또는 HA에게 바인딩 키를 복사해서 보내야만 한다. 이와 같은 경우에는 ASK 메시지가 이동 노드에 관한 세션 키와 추가적인 정보를 전달하는데 사용되며, Security AVP(Session-Key-Option), Address AVP(Home-Address-Option, Home-Agent-Address-Option) 등이 포함된다. 단계 6에서 Attendant가 이 메시지를 받았을 때, 이동 노드에 대한 키 생성 재료를 추출하고 로컬 스토리지에 바인딩 키를 저장한다. 이때 ARsp 메시지에 넌스, 키 생성 재료, 랜덤 번호, 인증자, 로컬 챌린지 등이 포함된다. 단계 7과 8은 생성된 바인딩 키를 기반으로 Mobile IP[3]에서 기술된 과정을 따라 바인딩 갱신/응답을 수행한다. 일반적인 흐름과 비교해 본다면, 그림 2의 단계 5,6,7,8은 'delegation' 후에 메시지 순서로부터 제거 되어지며 메시지 교환 횟수는 8 단계로 감소된다. 이동 노드가 한 도메인에 속한 도메인을 빠르게 로밍할 때, 이동 노드는 방문 링크의 통신 자원을 접근하기 위해 세션 키를 얻기를 시도한다. 이동 노드의 지역적인 이동성을 고려할 때, 'delegation' 모델은 이러한 경우에 적합하다. 만약 이동 노드가 다른 도메인으로 이동 하거나 'delegation' 요청이 실패하면, 3.1에서 기술된 일반적인 12 단계의 인증 절차를 따른다.

4. 성능 평가

4.1 시스템 모델

성능 평가 기준은 비용 함수를 도입했으며, 비용은 노드간의 거리와 각 노드에서의 처리 시간으로 구하였다. 그러나 노드간의 거리와 노드의 처리 시간에 대한 단위가 다르므로 노드에서의 처리 시간을 거리로 환산하여 비용 함수를 유도했다. 제안하는 구조에 포함된 여러 개의 엔티티 간의 거리는 그림 3에서와 같다. 시스템 모델은 서브 네트워크 간의 이동시 비용 분석을 위해 제안되었다. 논문에서는 비용 분석을 위해 [7],[8]에서 기술한 접근 방법을 참조하였다. CN은 λ 비율로 MN에게 데이타 패킷을 전송하고, MN은 μ 비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정한다. 본 논문에서는 MN이 이동 때마다 CN으로부터 수신되는 평균 패킷 수를 Packet to Mobility Ratio(PMR)이라고 정의한다. PMR은 $p=\lambda/\mu$라고 정의한다. 제어 패킷의 평균 길이를 l_c라 하고, 데이타 패킷의 평균 길이를 l_d라고 정의하며, 비율은 $l=l_d/l_c$라고 정의한다. 제어 패킷을 전송하는 비용은 송신자와 수신자의 거리에 의해 주어지며 데이타 패킷의 전송 비용은 제어 패킷에 비해 평균 l 배 크다고 정의한다. 그리고 한 호스트에서 제어 패킷을 처리하는 평균 비용은 r이라고 가정한다.

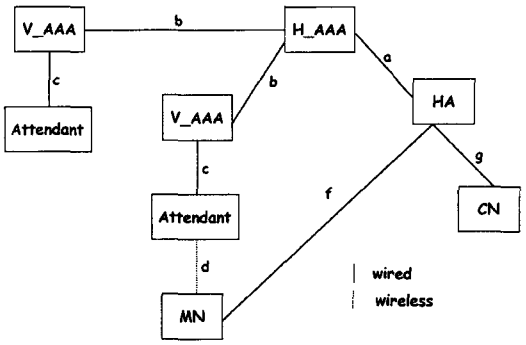

그림 3 비용 분석을 위한 시스템 모델

4.2 Mobile IPv6를 위한 AAA 인증 비용 분석

일반적인 인증 절차에서, MN이 한 도메인에서 서브 네트워크 사이를 이동하는 시간 동안에 발생하는 전체 비용은 (1)에 의해서 C_{auth-g}로 정의하며, 인증에 소요되는 비용과 인증 처리 동안 이전 도메인으로 송신되어 손실된 패킷을 재전송하는 비용의 합으로 나타낼 수 있다.

$$C_{auth-g} = C_{rg-g} + C_{oldFA-g} \quad (1)$$

새로운 호스트에서 MN을 인증하는 비용은 (2)에 의해서 C_{rg-g}로 정의하며, 그림 5의 구조에 따라 노드간 거리와 각 노드에서 처리하는 비용의 합이며 다음 식으로 표현할 수 있다.

$$C_{rg-g} = 2(a+b+c+d)+7r \quad (2)$$

한 개의 패킷이 CN에서 HA를 통해 MN까지 재전송되는 비용을 C_{dt}라고 두면, 인증 지연 동안에 이전 도메인으로 전달되는 데이타 패킷의 손실에 따른 재전송 비용은 인증에 소요되는 시간 동안 전송될 패킷에 대한 비용이므로 다음과 같이 표현 가능하다.

$$C_{oldFA-g} = \lambda \times t_{auth-g} \times C_{dt} \quad (3)$$

Mobile IP의 AAA에서 C_{dt}는 $l(g+f)+r$로 나타낼 수 있는데 이는 HA에서의 터널링을 통해 CN으로부터 MN으로 전달되는 단일 데이타 패킷의 비용을 의미한다. 인증 지연 시간은 그림 5의 시스템 모델에 따라 식 (4)와 같이 표현할 수 있다.

$$t_{auth-g} = 2(t_a+t_b+t_c+t_d)+9t_r \quad (4)$$

그러므로, 일반적인 인증인 경우의 전체 비용인 식 (1)을 다시 표현하면 다음과 같다.

$$C_{auth-g} = 2(a+b+c+d)+7r+\lambda \times t_{auth-g} \times C_{dt} \quad (5)$$

제안된 위임 기능을 가지는 인증 절차의 경우, MN이 한 도메인에서 서브 네트워크 사이를 이동할 때의 시간 간격 동안에 발생되는 전체 비용, C_{auth-d}은 일반적인 인증 절차의 경우와 마찬가지로 다음과 같이 표현할 수

있다.

$$C_{auth-d} = C_{rg-d} + C_{oldFA-d} \quad (6)$$

제안한 구조에서 새로운 서브 네트워크에서 MN의 인증 비용, C_{rg-d}은 해당 V_AAA에 등록하는 비용이므로 식(7)과 같이 표현할 수 있다.

$$C_{rg-d} = 2(c+d) + 5r \quad (7)$$

인증 지연 동안 이전 도메인으로 전달되어서 분실(또는 지연)되는 데이타 패킷의 재전송에 따른 비용은 일반적인 인증 절차의 경우와 마찬가지로 식 (8)에 의해 주어진다.

$$C_{oldFA-d} = \lambda \times t_{auth-d} \times C_{dt} \quad (8)$$

그리고 제안하는 구조에서 인증 지연 시간은 식(9)에 의해 나타낼 수 있다.

$$t_{auth-d} = 2(t_c + t_d) + 5t_r \quad (9)$$

그러므로, 제안하는 인증 경우의 전체 비용은 (10)에 의해 나타낼 수 있다.

$$C_{auth-d} = 2(c+d) + 5r + \lambda \times t_{auth-d} \times C_{dt} \quad (10)$$

4.1 절에서 이동성을 나타내는 p는 $\frac{\lambda}{\mu}$에 대한 정의를 이용하여 그림 5에 제시한 모델에 대한 성능 분석을 위해 일반적인 인증 절차에 대한 비용과 제안하는 인증 절차에 대한 비율을 (11)과 같이 정의하였다.

$$\frac{C_{auth-d}}{C_{auth-g}} = \frac{2(c+d)+5r+p\times\mu\times t_{auth-d}\times C_{dt}}{2(a+b+c+d)+7r+p\times\mu\times t_{auth-g}\times C_{dt}} \quad (11)$$

이동성을 나타내기 위해 [7]의 uniform fluid model을 적용하였으며, 이 모델에서 보행 속도는 $\mu = 0.01$이고 차량의 속도는 $\mu = 0.2$로 가정하였다[8].

성능 분석을 위해 C_{auth-d}/C_{auth-g} 비용 비율을 도입하여 설명할 수 있다. 다시 말하면, 제안된 구조의 비용은 일반적인 AAA 절차 비용에 대한 정규화로 볼 수 있다.

$$\lim_{p\to\infty}\frac{C_{auth-d}}{C_{auth-g}} = \lim_{p\to\infty}\frac{C_{rg-d}+p\times\mu\times t_{auth-d}\times C_{dt}}{C_{rg-g}+p\times\mu\times t_{auth-g}\times C_{dt}} = \frac{t_{auth-d}}{t_{auth-g}} \approx 0.34 \quad (12)$$

4.3 성능 평가

본 절에서는 앞 절에서 기술한 시스템 모델 및 비용 분석 결과를 기반으로 제안된 모델의 성능 평가 결과를 기술한다. 한 노드에서 메시지 처리 비용은 동일(r=1)하다고 가정한다. 또한 같은 도메인 안에서의 거리에 대한 비용은 1(a=c=d=1)이고 가까운 두 도메인 간의 거리에 대한 비용은 2(b=g=f=2)로 가정할 때 이동체와 보행자의 PMR 즉, p 값에 따르는 비용 비율인 식 (11)의 결과는 그림 4, 그림 5과 같이 구해진다. 그림 4는 이동 단말이 빠른 속도로 이동하는 이동체의 특성을 가지는 경우 PMR 값에 따른 인증 비용 비율(Cauth_d / Cauth_g) 변화를 보여 준다. 이동 속도가 빠르고 데이타 양이 많을수록 전체 인증 이동 비용 비율은 급격히 감소하며 PMR이 50인 지점을 지나면 전체 인증 비용 비율은 0.35를 유지한다. 즉, 이 경우 Cauth_g의 비용은 Cauth_d에 비해 대략 2.8배의 비용의 감소한다.

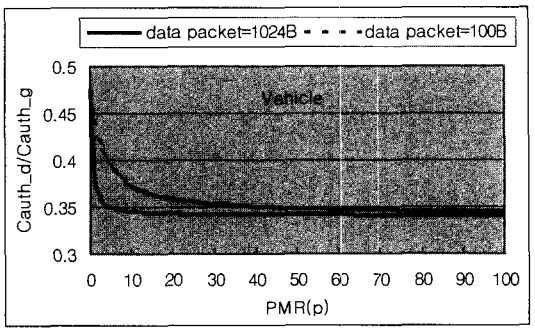

그림 4 빠른 이동체의 인증 비용 비율

그림 5는 이동 단말이 보행자의 속도로 이동하는 특성을 가지는 경우 PMR 값에 따른 인증 비용 비율(Cauth_d / Cauth_g) 변화를 보여 준다. 데이타 양이 많을수록 전체 인증 비용 비율은 급격히 감소하며 PMR 값이 클수록 전체 인증 비용 비율은 감소한다. PMR이 50인 지점에서 데이타 패킷이 1024 바이트인 경우 인증 비용 비용은 0.36 값을 가지며 데이타 패킷이 100 바이트인 경우 0.42 값을 가진다. 즉, 각각 2.5배와 2.3배의 비용 절감 효과를 기대할 수 있다.

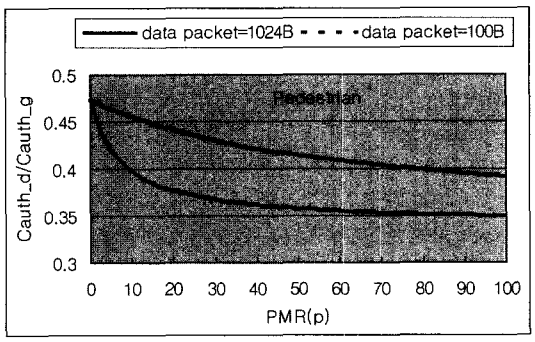

그림 5 보행자의 인증 비용 비율

5. 결 론

과거 몇 년간 이동 사용자에 대한 실시간 인증을 제공하기 위한 많은 주목할 만한 연구가 진행되어 왔다. 같은 사업자 도메인 내의 한 서브넷에서 다른 서브넷으로 빠르게 이동하는 상황하에서는 MN의 이동에 비례해

서 인증 메시지의 오버헤드가 증가하게 되므로 [1]과 [6]에 제안된 방법은 이 경우에 적합하지 않다. 효율적인 인증 절차를 제공하기 위해, 본 논문에서는 '위임(delegation)' 방법을 제안하고 있다. 제안된 방법에서, V_AAA는 MN에 대한 보안 문맥을 포함하고 있는 항목들을 관리한다. 그러나 이러한 항목에 대한 정보는 방문 도메인 내의 모든 AAA 서버가 공유하고 있을 필요는 없는데 이는 항목 갱신이나 삭제에 따르는 무결성을 유지하도록 관리하는 것이 매우 어렵기 때문이다.

본 논문에서는 비용 분석을 위한 시스템 모델을 제안하였으며, MN이 이동시 CN으로부터 수신하는 평균 패킷 수인 Packet to Mobility Ratio(PMR)을 정의하였다. 제안된 모델에 대한 일반적인 인증 비용 및 delegation 인증 비용에 대한 비용 비율을 계산하였으며, PMR 값의 증감 및 데이타 양에 따르는 비용을 분석하였다. 결과적으로 PMR 값이 증가하는 경우 delegation 인증 비용이 일반적인 인증 비용에 비해 낮아짐을 볼 수 있었다. 또한 도메인 간의 이동 확률 및 같은 도메인의 서브넷간 이동 확률을 고려한 비용 변이를 측정하였는데 동일한 도메인 내에서 이동 노드가 여러 서브넷을 빠른 속도로 이동할 확률이 높은 경우 일반적인 인증절차에 따른 비용에 비해 50% 이상의 비용 감소 효과를 기대할 수 있다.

참 고 문 헌

[1] Davied B. Johnson, Charles E. Perkins, Jari Arkko: Mobility Support in IPv6, draft-ietf-mobileip-ipv6-18.txt,Internet Draft, IETF, June, 2002.

[2] IEEE: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

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

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

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

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

[7] R. Jain, T. Raleigh, C. Graff and M. Beres-chinsky: Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers, in Proc. ICC'98 Conf., pp. 1690-1695, Atlanta.

[8] 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, Sep. 1988.

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

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

김 미 영

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

문 영 성

정보과학회논문지 : 정보통신
제 30 권 제 5 호 참조