MIPv6에서 빠른 이동성 서비스를 위한 효율적인 인증 방법☆

An Efficient Authentication Mechanism for Fast Mobility Services in MIPv6

이승연* 허의남**
Seung-Yeon Lee Eui-Nam Huh

요 약

홈 도메인을 벗어난 단말 노드가 이동성 서비스를 받을 수 있으려면 해당 노드에 대한 인증이 이루어 져야 한다. 이는 AAA 기반 구조와 연동을 통해 이루어 질 수 있는데 현재까지 제안된 방안들은 경우에 따라 오히려 이동 노드의 성능을 저하시킬 가능성이 존재하는 문제점을 가지고 있다. 본 연구에서는 AAA 인증 절차에 의해서 소요되는 지연을 줄이기 위한 방안으로 고속 핸드오프를 적용한 모델을 제안하여 AAA 인증 지연에 대한 성능을 향상 시킬 수 있는 방법에 대해 기술하고 효과적인 방법으로 이동 단말을 인증 할 수 있도록 하는 위임 기능을 고려한 인증 방법을 제안한다. 또한, 본 연구에서 제안된 Assertion 기능을 모바일 서비스에 추가하는 모델은 홈 에이전트와의 거리 혹은 지연시간이 멀어질 경우 V_AAA 간의 상호 위임 기능을 통해 인증 효율성을 높일 수 있는 방법이다. 제안된 방법은 비용 분석을 통해 그 효율성을 검증하였는데 결론적으로 Assertion 기능이 동작하는 상황에서 이동 단말이 홈 에이전트와의 거리가 멀어질수록 인증 비율이 높아지는 성능 향상을 볼 수 있었다.

Abstract

If a mobile node out of home domain asks to provide mobility service, the mobile should be permitted by the home domain. This can be accomplished by the usage of AAA but the recent studies have shown its weakness to fail the ability of mobile node. This study suggests Fast Handoff model which will shorten permission time by AAA and allow the mobility service to be more efficient. Our suggestion with Assertion function is a new approach to assist authentication capability through mutual authentication of each V_AAA when the distance between HA and itself gets far or its delay time becomes longer. Our suggestion verifies its efficiency by cost analysis

☞ Keyword : Mobile IPv6, AAA, Fast Handoff, Authentication, Assertion

1. 서 론

Mobile IPv6는 IPv6 주소를 가진 단말이 이동시에도 그 연결을 항상 보장하는데 필요한 기술이다. 따라서, 이동 노드(MN: Mobile Node)가 이동하는 상황에서도 서비스의 단절 없이 원활한 통신을 지원한다. Mobile IPv6는 특성상 다른 도메인에 속한 IP 계층의 로밍이 발생하므로 많은 보안상의 취약점을 가질 수 있다. 그러므로 이동 노드에게 서비스를 안전하게 제공하기 위해서는 여러 가지 기술적 문제점이 해결되어야 한다. 현재까지 다양한 보안 기법들이 연구되어 왔지만 지금까지 연구된 방안들은 경우에 따라 Mobile IPv6의 성능을 저하시킬 가능성이 존재하고 보안성이 낮다는 몇 가지 단점을 가지고 있다[1]. Mobile IPv6에서는 이동성으로 발생

* 준 회 원: 경희대학교 컴퓨터공학과 석사과정
seungyeon@khu.ac.kr
** 종신회원: 경희대학교 전자정보대학 컴퓨터 공학과 조교수
johnhuh@khu.ac.kr
[2005/11/09 투고 - 2005/11/20 심사 - 2006/02/07 심사완료]
☆ 이 연구는 2005년도 경희대학교 지원에 의한 결과임. (KHU-20051077)

하는 보안상의 취약점과 문제점을 극복하기 위해 홈 에이전트와 이동노드 사이의 보안 프로토콜로써 IPSec을 사용하고 있다. IPSec은 이동노드와 홈 도메인의 홈 에이전트 사이에 설정된 보안연계(SA:Security Association)를 통하여 바인딩 정보를 보호하고 메시지를 인증한다. 그러나 IPSec만을 사용하는 경우 홈 망에서 방문 망으로 이동한 이동 노드가 실제로 홈 망에서 인증된 노드인지를 판단할 수 없다는 단점을 가지고 있다. 따라서 보안상의 취약점을 극복하고 망 노드들 간의 인증을 제공하는 안전한 로밍 서비스 기술 즉, AAA(Authentication, Authorization, Accounting) 기술이 기본적으로 요구된다.

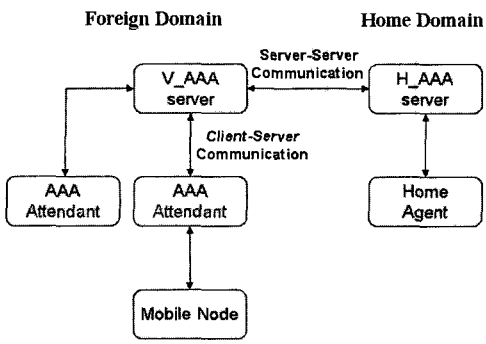
AAA는 홈 망을 벗어난 이동 노드가 로밍을 하는 경우, 즉 방문 망에서 이동 서비스를 받고자 하는 경우 이동 노드에게 다양한 유무선 서비스에 대한 인증, 권한검증, 과금 등의 기능을 수행한다. 그러나 다양한 네트워크와 프로토콜 상에서 안전하고 신뢰성 있는 이동 노드의 인증은 이동노드의 빈번한 이동 및 이로 인한 매번 새롭게 갱신되어야 하는 세션키 갱신 등의 문제점을 가지고 있다. 이러한 문제점을 해결하고자 본 논문에서는 이동 노드의 이동시 필요한 인증을 수행하기 위해 이동 노드와 멀리 떨어진 홈 에이전트와의 정보 교환이 이루어 질 때 인증 메시지의 오버헤드 증가로 인한 이동 노드의 처리 지연이 발생하는 문제점을 지적하고 Francis Dupont의 AAA 모델[2]을 기반으로 고속 핸드오프를 적용하여 인증 지연 시간과 패킷 손실을 줄이기 위한 방법을 기술한다. 아울러 이동 노드가 외부 망에 접근하기 위해서 수행해야 할 인증절차에 대해서 고찰한다.

본 제안 방식에서는 이동 노드가 동일한 도메인 내의 여러 서브넷을 빠르게 이동하고 있는 상황에서 인증 절차를 간소화함으로써 진행 중인 세션에 대한 신속한 서비스 재개를 가능케 하기 위한 방법을 검증한다. 본 논문의 구성은 2장에서 Mobile IPv6상에 AAA 인증 모델 및 엔티티를 정의하고 3장에서는 기존 방식의 대한 고찰을 한 후 4장에서 제안방식에 대한 설명 및 성능평가를 한다. 마지막으로 5장에서는 결론을 맺도록 한다.

2. 관련연구

2.1 AAA 인증 모델 및 엔티티

Mobile IPv6를 큰 규모의 여러 ISP들로 이루어진 상용망에 적용하기 위해서는 이동 노드가 서비스에 크게 지장 받지 않고 안전하게 인터넷 접점을 변경할 수 있도록 허용해야 한다. Diameter같은 AAA프로토콜은 이동 노드가 다른 망으로 로밍을 한 후에도 서비스를 지속적으로 제공받을 수 있도록 해준다[3,4]. 그러므로 Mobile IPv6를 상용망에 적용하기 위해서는 프로토콜에 AAA 지원기능이 있어야 한다. 아래의 그림 1은 Diameter AAA 인증구조를 사용해서 이동 노드와 Attendant 간에 세션 키를 교환하고 이동 노드의 현재 위치 정보를 홈 에이전트로 등록하기 위한 AAA 통신 모델을 나타낸다.



〈그림 1〉 AAA 프로토콜 모델 정의

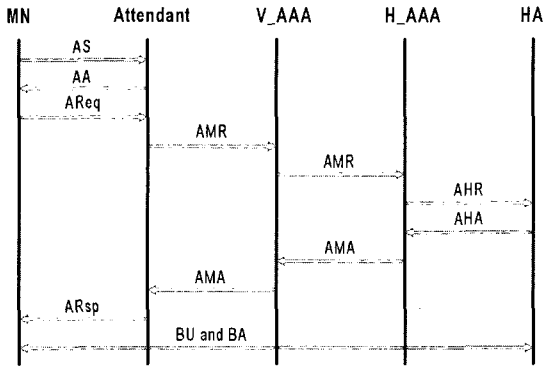
DIAMETER AAA는 고유의 인증 기능을 수행하며, 이동 서비스를 위한 바인딩 등록 절차를 처리한다. AAA는 이동 노드, Attendant, 홈 에이전트 (HA: Home agent), V_AAA (Visited

AAA Server), H_AAA(Home AAA Server)등 5개의 엔티티를 정의하고 있다. Attendant는 이동 노드가 방문 망에 가장 먼저 접속하게 되는 외부 엔티티로서 이동 노드에 전송하는 패킷에 대한 통과, 폐기, 보류 등의 정책을 수행할 수 있으며, AAA 서버를 통한 인증 성공시 패킷을 통과 시킬 수 있다. 홈 에이전트는 이동 노드의 홈 네트워크에 존재하는 라우터로써, 이동 노드의 HoA와 CoA에 대한 바인딩을 유지 및 관리한다. V_AAA는 방문 망에 AAA 인증 서버로서 이동 노드로부터 인증 요청을 수신하면 먼저 Attendant를 인증하고 이동 노드의 NAI(Network Access Identifier)나 홈 주소를 통해 이동 노드의 홈 망에 존재하는 AAA 인증 서버로 이동 노드로부터의 인증 요청 메시지를 전송한다. H_AAA는 홈 망의 AAA 인증 서버로서, 이동 노드의 인증에 필요한 인증 정보들을 관리하고 있다. H_AAA는 이동 노드가 보내온 인증 정보를 기반으로 이동 노드에 대한 인증처리 과정을 진행하고 그 결과를 V_AAA로 전송한다.

2.2 AAA 인증 및 바인딩 절차

본 절에서는 "AAA for Mobile IPv6" 문서를 통해 Francis Dupont이 제안한 AAA 인증 방법에 관해 논의한다[5]. Mobile IPv6 키 분배를 위한 프로토콜인 IKE(Internet Key Exchange) 성능이 무선 인터넷 환경에서 기대에 못 미치는 것으로 보고 됨에 따라 Dupont은 AAA 구조와의 결합된 방법을 통해 해결책을 제시하고 있다. 아래의 (그림 2)는 이동 노드를 위한 AAA 인증 및 바인딩 절차이다.

이동노드는 자신의 IPv6 주소를 설정하고 Attendant를 발견한 후 (AS : Attendant Solicitation), Attendant에게서 받은 Advertisement (AA : Attendant Advertisement)를 통하여 자신의 이동을 감지하고 홈 망으로의 인증을



〈그림 2〉 AAA인증 및 바인딩 절차

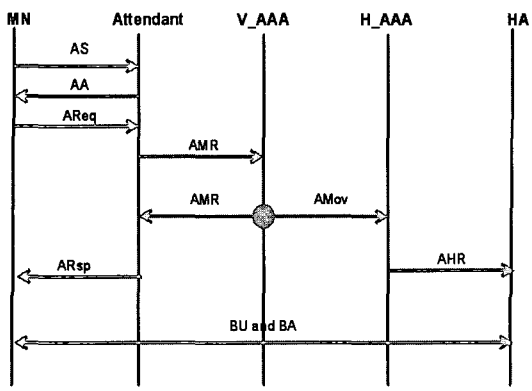
시도한다(AReq : Authentication Request). Attendant는 이동 노드로부터 인증 요청 메시지를 받으면 임시 바인딩 리스트에 이동 노드의 정보를 저장한 후 V_AAA 서버에 메시지를 전달한다(AMR : Authentication MN-Request). V_AAA 서버는 그 요청 메시지를 AAA 프로토콜로 변환해서 H_AAA 서버로 전달한다 H_AAA 서버는 엔티티들이 사용할 세션 키를 생성하고, 에이전트로 메시지를 전달(AHR : Authentication HA-Request)한다. 홈 에이전트는 H_AAA로부터 인증 요청 메시지를 받으면 이동 노드로부터 온 메시지임을 인증하고 이동 노드와 Attendant간에 사용될 세션키를 생성한 후 MN과 V_AAA간의 인증에 필요한 메시지를 포함한 인증 응답 메시지를 작성하여 H_AAA에게 돌려준다(AHA : Authentication HA-ACK). H_AAA 서버는 HA로부터 받은 인증 응답 메시지를 V_AAA로 전달(AMA : Authentication MN-ACK)하고 이 메시지를 받은 Attendant는 암호화된 세션키를 저장하고 이동 노드로 전송(ARsp : Authentication Response)한다. Attendant에게서 인증 응답 메시지를 받은 이동 노드는 자신의 바인딩 리스트를 갱신 후 홈 에이전트에게 위치 갱신(BU: Binding Update, BA: Binding Acknowledgement)을 한다.

3. 기존 모델

본 장에서는 2장에서의 관련 연구를 통한 분석을 기본으로 AAA 절차로 인한 인증 지연을 줄이기 위한 기존 모델의 메시지 교환 방법을 고찰한다[6,7].

3.1 위임기능을 갖는 AAA

Diameter AAA의 기본 모델에서는 이동 노드가 인증 요청을 할 때마다 AAA 엔티티들 간에 세션키를 공유하기 위해 메시지 교환이 이루어지게 된다. 이동 노드와 엔티티들 사이에서 공유되어지는 세션키 및 바인딩 갱신은 이동노드가 인증 요청을 할 때마다 빈번하게 수행되므로 이동 서비스의 지연이 많이 발생하게 된다. 따라서 이동 노드의 이동성을 고려한 인증 및 바인딩 등록 방법이 필요하다. 위임기능을 갖는 AAA는 이러한 문제점을 개선시키기 위해 이동 노드에 대한 인증 정보 및 세션키 생성 재료를 V_AAA로 위임한 인증 절차를 제공하고 있다. 위임기능을 갖는 AAA 모델은 인증 메시지 처리 절차와 더불어 'delegation' 옵션을 세션키에 내장하여 각 단계별로 주고받는 메시지 교환 절차를 줄임으로써 보다 더 개선된 보안 기능을 제공하고 있다. 아래의 그림 3은 'delegation' 옵션이 추가된 AAA 모델을 나타낸다.



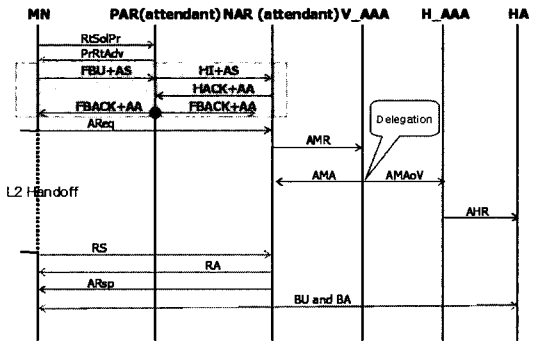
〈그림 3〉 위임기능을 갖는 AAA 모델

보안 문맥(SAs, algorithms, hash functions, etc.)을 포함하고 있는 'delegation' 옵션은 이동 노드의 이전 위치에서 같은 도메인 내의 다른 링크로 이동하는 경우 이동노드가 Areq 메시지를 통해 인증 요청을 할 때 보내질 수 있다.이 메시지를 수신한 V_AAA는 보안 문맥을 자신이 처리할 수 있는지의 여부를 판단하기 위해 자신의 처리능력(capability)과 비교한 후 처리가 가능하다고 판단되면, V_AAA는 'delegation' 요청을 수락하고 자신의 'delegation' 항목 리스트에 이동 노드에 대한 새로운 항목을 구성한다. V_AAA는 이동 노드가 'delegation' 엔트리 리스트에 등록된 노드인지를 확인하고 이동 노드에 대한 항목이 존재한다면 이동 노드를 인증하고 세션 키를 생성한다. V_AAA가 보안 문맥 처리를 위한 기능을 가지고 있지 않다면, delegation 요청은 무시되어, 인증 메시지는 2.2에서 정의한 대로 처리된다. 'delegation' 절차가 완료된 후, V_AAA는 AMR에 대한 응답으로, 세션키, 키 재료 및 그 외의 보안 파라미터들을 포함하고 있는 AMA, AMAoV(AMA : Authentication MN-ACK of V_AAA) 메시지를 전송한다.

3.2 고속 핸드오프를 적용한 위임기능을 갖는 AAA

고속 핸드오프를 적용한 위임 기능을 갖는 AAA는 인증 지연으로 인한 패킷 손실을 줄이기 위해 고속 핸드오프 동작 절차가 시작될 때 AAA 인증 절차도 수행할 수 있는 방식이다. Layer2 Handoff가 발생하기 전에 몇몇 AAA 인증 절차가 수행되기 때문에 이동 노드가 이동을 마치면 나머지 AAA 인증 절차만을 수행함으로써 인증 절차로 인한 지연시간을 줄일 수 있다[8][9]. 일반적인 흐름과 비교해본다면, 메시지 교환 횟수는 12단계에서 8 단계로 감소된다. 'delegation'이 내장된 옵션은 이동 노드 홈 망과 방문 망간에 사전 로밍 계약이 체결되어 있는 자원을 접근하는 경우에 적용된다. 사전 로밍

계약이 체결되어 있지 않다면 방문 망의 자원 사용에 관한 권한을 얻지 못하므로 'delegation' 요청이 실패로 처리되고, 2.2에서 기술된 일반적인 12 단계의 인증 절차를 따른다. 아래의 그림 4는 고속 핸드오프가 적용된 위임기능을 갖는 AAA 모델의 메시지 절차를 나타낸다.



〈그림 4〉 고속 핸드오프가 적용된 위임기능을 갖는 AAA

4. 제안모델

본 장에서는 3장에서의 기존 모델을 기반으로 하여, Mobile IP의 인증 효율과 유연성을 높이기 위한 Assertion이라는 새로운 모델을 제안한다.

4.1 Assertion 배경

Assertion의 개념은 SAML(Security Assertion Markup Language)이라는 인터넷 프로토콜에서 처음으로 정의되었다[10]. SAML은 인터넷 상에서 보안 정보 교환을 위한 XML 프레임웍을 뜻한다. 이것은 OASIS(the Organization for the Advancement of Structured Information Standards)에 의해 표준화 되었고, 표준적인 메시지 형식과 전송 프로토콜을 사용함으로써 플랫폼이나 솔루션 등에 독립적인 인증 및 속성 확인, 승인 등의 서비스를 제공하며 이는 XML 기반의 다른 보안 기술들과 통합되어 전체 보안 시스템을 구성하는 요소 기술로서 기능을 가진다. SAML 은 인증, 속성, 인가 결정 정보를 단언하는 Assertion과 인증 및 승인 등을 요청/수신하기 위한 프로토콜, 실제 인터넷 상의 네트워크와의 연동을 정의한 바인딩 및 프로파일로 구성된다. 이로부터 얻을 수 있는 장점은 각 엔터티 간에 SSO (Single Sign-On) 기능을 제공할 수 있어, 사용자는 한 사이트(혹은 도메인)에서 사용자 인증을 받은 후에 인증해준 사이트(혹은 도메인)과 서로 인증된 파트너 사이트를 따로 인증 받을 필요 없이 이용할 수 있다. Assertion 은 이처럼 보안의 취약 부분을 보다 강력하게 할 뿐만 아니라, 이를 AAA 프로토콜에 응용하여 메시지의 오버헤드를 보다 효율적으로 줄일 수 있는 방안을 마련할 수 있다.

4.2 Assertion AAA

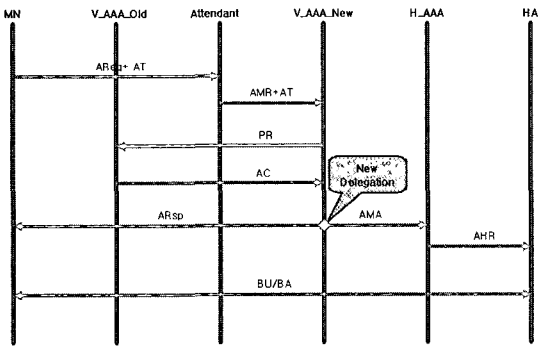
AAA를 이용한 이동 노드에 대한 기존에 인증 방식은 이동 노드가 새로운 망으로 이동할 때마다 매번 인증 과정을 거쳐야 하고 홈 망에 있는 인증 서버로부터 인증을 받아야 한다. 이동 노드가 다양한 방문 망을 통해서 인증 서버가 있는 홈 서버에게 까지 인증을 요청하는 방식은 방문 망에서 홈 망까지의 빈번한 인증 절차로 인해 대량의 트래픽을 유발하게 된다. 이때 이동 노드와 홈 망간의 거리가 길어질수록 인증을 위한 시간이 커지게 되고 많은 양의 시그널링 처리를 위한 상당한 통신 지연 및 불필요한 오버헤드가 생기게 된다. 인증 처리 시간의 지연은 이동성 서비스의 지연을 유발시키고 민감한 실시간 처리를 필요로 하는 서비스에 대하여 치명적인 문제점을 발생 시키게 된다. 이러한 인증 지연 시간을 줄이기 위해 본 논문에서는 'Assertion' 옵션을 AAA 모델에 도입하여 AAA 인증 지연을 최소화 하는 효율적인 인증 방식을 제공한다. 본 방식은 홈 인증 서버로부터의 인증 받는 방식을 그대로 이용하면서 홈 망에 인증 서버의 역할을 방문 망에 인증 서버가

대행하는 위임 기능을 갖는 AAA 모델을 기반으로 연동된다.

제안하는 모델은 방문 망에 이동노드의 Lifetime이 남아있는 채 새로운 망으로 이동 노드가 이동했을 경우와 이동 노드와 홈 망의 사전 로밍 계약이 이루어져 있지 않은 경우를 가정한다.

이동 노드가 방문 망에서 다른 방문 망으로 서로 다른 두 개의 외부 방문 망을 걸쳐 이동하는 경우 이동 노드는 이동에 따른 홈 망에 서버로부터의 인증을 받아 오는 것이 필요하다. 이동 노드의 인증 요청이 시작되면 홈 에이전트와의 보안 연계가 새롭게 설정되어야 하며 이동 노드와 홈 에이전트와의 거리가 멀어 질수록 등록을 위한 지연 시간은 증가하게 된다.

'Assertion' 옵션을 적용한 AAA는 인증 지연을 최소화하기 위해 현재 이동 노드가 속한 방문 망 인증 서버에 'Assertion' 메시지를 세션 키에 내장하여 전달하므로 써 이동 노드의 인증 절차를 간소화 한다. 'Assertion' 옵션 방식은 방문 망에 인증 정보를 활용하여 인증에 대한 검증을 제공하므로 AAA 메시지의 전체적인 양과 홈 에이전트의 오버헤드 및 처리 지연을 줄일 수 있는 방법이다. 아래 (그림 5)는 'Assertion' 옵션의 메시지 처리 절차를 나타낸다. 본 모델은 Single Sign-On으로 확장되어 이동 환경에서의 인증 절차를 효율적으로 수행 할 수 있는 방안이 될 것이다.



〈그림 5〉 Assertion 기능을 갖는 AAA 모델

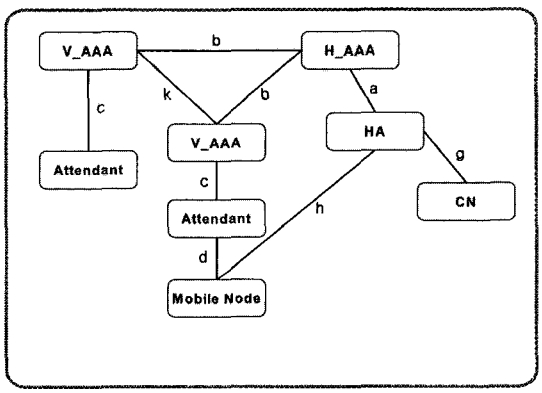
이동 노드가 새로운 망으로 이동 시, MN은 ARep메시지, 가장 최근의 delegation 된 V_AAA_Old 정보와 AT(Assertion Trigger) 메시지를 V_AAA_New 에게 전송한다. MN은 이전의 바인딩 갱신 소요된 시간의 변화를 기록하므로 현재의 이동이 홈 에이전트에 근접하는지의 여부를 판단하여 이동노드와 홈 에이전트의 거리가 멀어지는 경우에 아래와 같은 프로토콜로 V_AAA_New에게 AT를 전송한다. V_AAA_New는 PR(Proxy Request) 메시지를 V_AAA_Old에 보내어 아직 유효한 이동 노드의 identity를 검사하고 만일 이동 노드가 적합하다면 이에 대한 응답으로 V_AAA_Old는 AC(Assertion Conformation) 메시를 V_AAA_New에 전달한다. V_AAA_New는 이동 노드를 인증하고 보안 문맥에 따라서 세션 키를 생성한다. 'Assertion' 절차가 완료된 후, V_AAA_New는 AMA, AHR 메시지를 H_AAA와 홈 에이전트에게 전송한다. 이동 노드에 대한 인증 절차가 끝나면 바인딩 갱신 메시지를 보냄으로써 홈 에이전트의 바인딩을 갱신할 수 있다.

5. 성능 평가

5.1 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. 본 논문에서는 [11][12]에 기술된 접근 방법을 참조 하였다. 제안하는 구조에 포함된 여러 개의 엔티티 간의 거리는 (그림 6)에서와 같다. 시스템 모델은 서브네트워크 간의 이동시 비용 분석을 위해 제안되었다. CN은 λ비율로 MN에게 데이터 패킷을 전송하고, MN은 μ비율로 한 서브넷에서 다른 서브넷으로 이동한다고 가정하며, MN이 이동 때마다 CN으로부

터 수신되는 평균 패킷 수를 Packet to Mobility Ratio (PMR) 이라고 정의한다[13]. PMR은 $p = \lambda / \mu$ 라고 정의한다. 제어 패킷의 평균 길이를 l_c 라하고, 데이터 패킷의 평균 길이를 l_d 비율은 $l = l_d / l_c$라고 정의한다. 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 r이라고 가정한다.



〈그림 6〉 비용분석을 위한 시스템 모델

5.2 Mobile IPv6를 위한 AAA 인증 비용 분석

일반적인 인증 절차에서, MN이 한 도메인에서 서브네트워크 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 6의 구조에 따라 노드간 거리와 각 노드에서 처리하는 비용의 합이며 다음 식으로 표현할 수 있다.

$$C_{rg-g} = 2(a+b+c+d) + 3h + 12d + 20r \quad (2)$$

한 개의 패킷이 CN에서 HA를 통해 MN까지 재전송되는 비용을 C_{dt}라고 두면, 인증 지연 동안에 이전 도메인으로 전달되는 데이터 패킷의 손실에 따른 재전송 비용은 인증에 소요되는 시간동안 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 데이터 패킷의 비용을 의미한다. 인증 지연 시간은 그림 6의 시스템 모델에 따라 식 (4)와 같이 표현할 수 있다.

$$t_{auth-g} = 2(t_a + t_b + t_c + t_d) + 3t_h + 12t_d + 20t_r \quad (4)$$

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

$$C_{auth-g} = 2(a+b+c+d) + 3h + 12d + 20r \quad (5)$$
$$+ (\lambda \times t_{auth-g} \times C_{dt})$$

제안된 위임 기능을 가지는 인증 절차의 경우, MN이 한 도메인에서 서브네트워크 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 서브네트워크에서 MN의 인증 비용, C_{rg-d}은 해당 V_AAA에 등록하는

비용이므로 식 (7)과 같이 표현할 수 있다.

$$C_{rg-a} = 2(a+b+c+d)+3h+10d+18r \quad (7)$$

인증 지연 동안 이전 도메인으로 전달되어서 분실(또는 지연)되는 데이터 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.

$$t_{auth-a} = 2(t_a + t_b + t_c + t_d) + 3t_h + 10t_d + 18t_r \quad (9)$$

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

$$C_{auth-a} = 2(a+b+c+d)+3h+10d+18r \quad (10)$$
$$+(\lambda \times t_{auth-a} \times C_{dt})$$

일반적인 모델의 전체 비용은 (11)에 의해 나타낼 수 있다.

$$I_{auth-a} = C_{auth-g} - C_{auth-a} = 2d+2r+ \quad (11)$$
$$((\lambda \times t_{auth-g} \times C_{dt}) - (\lambda \times t_{auth-g} \times C_{dt}))$$

고속 핸드오프를 적용한 위임기능을 갖는 AAA 구조의 제안한 모델에서 한 도메인에서 서브네트워크 사이를 이동하는 시간 동안에 발생하는 전체 비용은

$$C_{auth-d} = C_{rg-d} + C_{oldFA-d} \quad (12)$$

새로운 호스트에서 MN을 인증하는 비용은 (2)에 의해서 C_{rg-d}로 정의하며, 그림 6의 구조에 따라 노드간 거리와 각 노드에서 처리하는 비용의 합이며 다음 식으로 표현할 수 있다.

$$C_{rg-d} = a+b+2(c+d)+3h+9d+15r \quad (13)$$

인증 지연 동안에 이전 도메인으로 전달되는 데이터 패킷의 손실에 따른 재전송 비용은 인증에 소요되는 시간동안 전송될 패킷에 대한 비용은

$$C_{oldFA-d} = \lambda \times t_{auth-d} \times C_{dt} \quad (14)$$

제안된 모델에서의 인증 지연 비용은 다음과 같이 계산된다.

$$t_{auth-d} = t_a + t_b + 2(t_c + t_e) \quad (15)$$
$$+ 3t_h + 9t_d + 15t_r$$

그러므로 제안된 모델의 전체 비용의 합은 (16)과 같이 나타낼 수 있다.

$$C_{auth-d} = a+b+2(c+d)+3h \quad (16)$$
$$+9d+15r+(\lambda \times t_{auth-d} \times C_{dt})$$

제안된 모델의 전체 비용의 합은 다음식과 같이 나타낼 수 있다.

$$I_{auth-d} = C_{auth-g} - C_{auth-d} = a+b+3d+5r+ \quad (17)$$
$$((\lambda \times t_{auth-g} \times C_{dt}) - (\lambda \times t_{auth-d} \times C_{dt}))$$

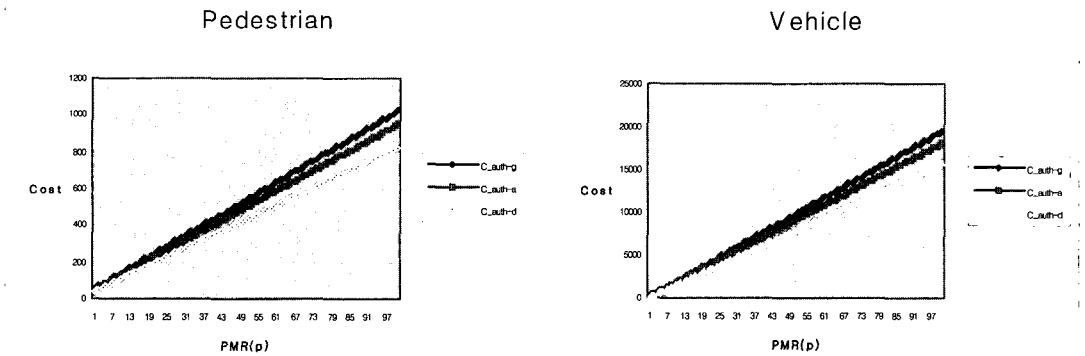
그러므로 delegation 구조를 갖는 모델의 전체 비용은 (18)과 같이 나타낼 수 있다.

$$L_{total} = C_{auth-d} - C_{auth-a} = a+b+d+3r- \quad (18)$$
$$((\lambda \times t_{auth-d} \times C_{dt}) + (\lambda \times t_{auth-a} \times C_{dt}))$$

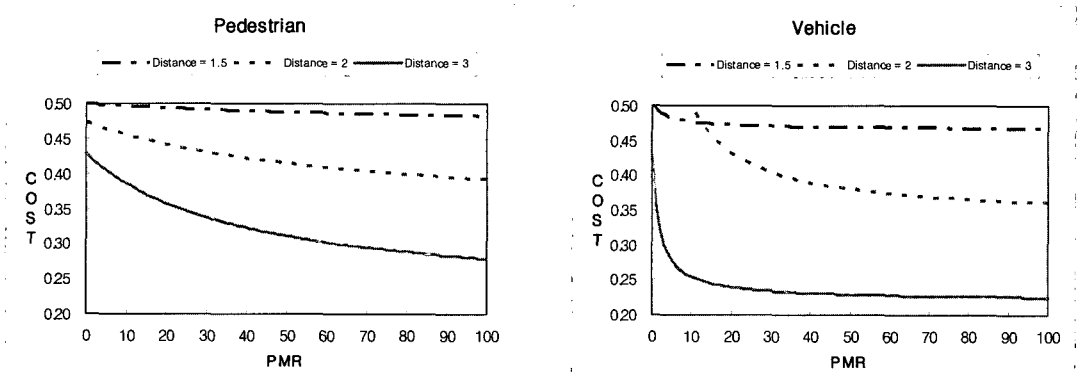
5.3 성능 평가

본 연구에서는 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 데이터양에 따르는 비용을 분석하였다. 결과적으로 PMR 값이 증가하는 경우 delegation 인증 비용이 일반적인 인증 비용에 비해 낮아짐을 볼 수 있었다. 또한 도메인간의 이동 확률 및 같은 도메인의 서브넷간 이동 확률을 고려한 비용 변화를 측정하였는데 동일한 도메인 내에서 이동 노드가 여러 서브넷을 빠른 속도로 이동할 확률이 높은 경우 일반적인 인증절차에 따른 비용에 비해 20% 이상의 비용 감소 효과를 확인할 수 있었다.

Assertion을 이용한 V_AAA간의 위임모델은 PMR 값의 변동을 기준으로 V_AAA 간에 거리의 변화에 따른 변동을 그래프로 나타내었다. 본 실험은 거리에 따른 V_AAA 간의 delegation 얼마나 효율적인 것인가 보여주는 것으로 방문 네트워크와 홈 네트워크의 delay time에 근거해서 1.5, 2, 3배까지의 delay time을 두고 delegation 인증 비용에 대한 비용 비율을 계산



〈그림 7〉 빠른 이동체와 보행자의 인증 비용 비율 분석



〈그림 8〉 Assertion을 이용한 모델의 인증비용 비율 분석

하였다. 예상과 같이 제안한 모델에서 이동 노드와 홈 에이전트와의 거리가 멀수록 인증 비용 비율이 증가함을 볼 수 있었다. Assertion을 이용한 제안 모델은 이동 노드가 홈 에이전트와의 거리가 먼 특성을 가질수록 이동 노드의 인증의 효율성을 높일 수 있는 효과를 기대할 수 있다.

6. 결 론

본 연구에서는 Mobile IPv6에서의 보안 강도를 높이기 위해서 AAA 인증 기법을 이용한 모델을 적용하였고, 이러한 AAA 인증으로 인한 지연을 줄이기 위해서 고속 핸드오프를 적용한 방안을 제안 하였다. 제안된 모델은 시그널링 비용과 패킷 전송 비용을 계산하여 성능 평가를 통해 비용이 절감 되는 것을 확인 하였다. 본 연구의 결과에 의해서 제안된 모델은 이동 노드가 이동 했을 때 인증으로 인한 지연을 줄일 수 있고, 또한 고속 핸드오프를 적용함으로써 일반적인 MIPv6에서 핸드오프시 발생했던 패킷 손실을 크게 줄일 수 있었다. 같은 도메인 내의 한 서브넷에서 다른 서브넷으로 빠르게 이동하는 상황에서는 MN의 이동에 비례해서 인증 메시지의 오버헤드가 증가하게 되므로 효율적인 인증 절차를 제공하기 위해 Assertion 방법을 제안하여 보다 효율적인 인증 방법을 연구하였다.

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] Charles E. Perkins and Thomas Eklund, "AAA for IPv6 Network Access", Internet Draft, draft-perkins-aaav6-06, May 2003.

[3] Charles E. Perkins, "Diameter Mobile IPv6 Application", IETF Internet Draft, draft-le-aaa-diameter-mobileipv6-03, Oct 2003

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

[6] 김창남,문영성,허의남 "Mobile IPv6에서 Fast Handoff 기법을 이용한 AAA 인증 성능 향상 방안",정보과학회 제31권 6호

[7] 김미영,문영성,"Mobile IPv6에서 AAA를 이용한 이동 노드와 홈 에이전트간의 최적화된 인증 방안", 정보과학회 제30권 6호

[8] Miyoung Kim and Youngsung Mun, "Localized Key Management for AAA in Mobile IPv6", Internet Draft, draft-mun-aaa-localkm-mobileipv6-01, May 2003.

[9] Seung-Yeon Lee and Eui-Nam huh, An Efficient Performance Enhancement Scheme for Fast Mobility Service in MIPv6, LNCS Volume 3480/2005

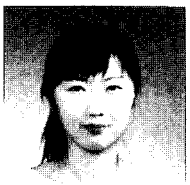
[10] 허의남,황준,"웹 서비스 상의 상호 인증을 위한 SAML 보안 취약성 분석" , 인터넷정보학회 춘계학술대회 2004.

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

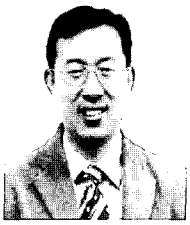
[12] P. Calhoun, C.Perkins: Mobile IP Network Access Identifier Extension for IPv4, RFC 2794, IETF, March, 2000

[13] Sangheon Pack and Yanghee choi, "Performance Analysis of Fast Handover in Mobile IPv6 Networks", in proc. IFIP PWC 2003, Venice, Italy, September 2003.

◐ 저 자 소 개 ◑



이 승 연 (Seung-Yeon Lee)
2004년 서울여자대학교 컴퓨터 공학과 (공학사)
2005년 ~현재 경희대학교 컴퓨터공학과 석사과정
관심분야: Mobile IPv6, Security, Telemetics
e-mail : seungyeon@khu.ac.kr



허 의 남 (Eui-Nam Huh)
1985년 부산대학교 전산통계 (학사)
1995년 University of Texas, 전산학 (석사)
2000년 The Ohio University, 전산공학 (박사)
2002년 삼육대학교
2003년 서울여자대학교 컴퓨터공학과 조교수
2005년 ~현재 경희대학교 컴퓨터공학과 조교수
관심분야 : Telemetics, Grid, Ubiquitous, embedded
E-mail : johnhuh@khu.ac.krr