韓國 컴퓨터情報學會 論文誌
第11卷 第2號, 2006. 5.

2006-11-2-2-3

휴대인터넷 환경에서 모바일 IPv6을 이용한 인터 도메인간 인증

정윤수*, 우성희**, 이상호*

Inter-domain Authentication Mechanism using MIPv6 in Portable Internet Environments

Yoon-Su Jeong*, Sung-Hee Woo**, Sang-Ho Lee*

요 약

휴대 인터넷은 high-speed 무선 인터넷 서비스를 제공하는 새로운 서비스이다. high-speed 무선 인터넷 서비스는 터미널 이동성을 제공한다. 휴대인터넷은 2006년에 상업화될 것으로 예상된다. 네트워크 확장과 터미널 이동성은 효율적 소개와 분산 이동 인터넷 서비스를 위해서 보장되어야 한다. 따라서 이 논문에서는 휴대 인터넷의 이동성과 호가장성을 보장하기 위해서 이동 IPv6 기술과 휴대 인터넷의 이동성을 적용한 메커니즘을 제안한다. 제안된 메커니즘은 보안성을 향상시키기 위해서 인터 도메인에서 다이어미터 프로토콜을 적용한다. 또한, 제안된 메커니즘은 데이터 보안성을 제공하기 위해 최소의 시그널 수로 데이터를 안전하게 전송한다.

Abstract

Portable Internet is a new service providing a high-speed wireless Internet service. The high-speed wireless Internet service guarantees terminal mobility. Portable Internet is expected to commercialize in 2006. Network expansion and terminal mobility should be guaranteed in order to efficiently introduce and distribute portable Internet service. Accordingly, the thesis suggests a mechanism which applies mobile IPv6 technology and supports inter-domain authorization In order to guarantee expansion and mobility of portable Internet. The suggested mechanism applies diameter protocol to the mobile IPv6 to improve securities. Also, The suggested mechanism safely transmits data at the minimal signal number, to guarantee the data secrecy.

▸ Keyword : 휴대인터넷(Portable Internet), 모바일 IPv6, 인터 도메인 인증(Inter domain authentication)

• 제1저자 : 정윤수, 교신저자 : 이상호
• 접수일 : 2006.01.25, 심사완료일 : 2006.05.13
* 충북대학교 전기전자컴퓨터공학부
** 충주대학교 전기전자 및 정보공학부

Ⅰ. 서 론

국내 초고속 인터넷 및 이동 통신 시장은 성숙기에 접어들어 양적인 팽창을 통한 통신산업 발전을 이루는 데에는 한계에 도달하고 있다. 이러한 한계를 극복하기 위한 새로운 수익원의 하나로 무선인터넷이 예상되고 있으며, 경쟁력 있는 무선인터넷 제공을 위한 솔루션의 하나로 휴대인터넷이 최근 주목 받고 있다.

휴대인터넷에서 사용되고 있는 휴대용 컴퓨터나 PDA등의 이동 단말들의 이동성을 보장하기 위해 최근 IETF에서는 차세대 인터넷 프로토콜인 IPv6를 이용한 모바일 IPv6에 대한 표준화 작업을 활발히 진행 중이다. 표준화 작업에서 언급된 것처럼 모바일 IPv6는 자신의 관리 도메인 안에서 이동 단말의 이동성을 적용하는데 사용되지만 이동 단말의 인증과 권한을 검증하기 위한 외부 도메인의 도메인간 인증은 정의되어 있지 않고 있다. 현재 표준화 작업에서 가장 중요시되고 있는 것은 외부 도메인에서 모바일을 액세스하는 것과 지역 보안정책이 적당한 보안 레벨을 유지하면서 외부 도메인을 안전하게 인식하는 것이다[1,2].

이러한 인터 도메인 보안 문제를 풀기 위해서, 인증, 권한, 과금을 위한 AAA 개념이 IETF에 의해서 정의됐고, 현재 AAA는 연구가 활발하게 진행되고 있지만 모바일 IPv6에 다이어미터(Diameter) 프로토콜을 적용하여 서로 다른 도메인간에 이동 노드가 이동하는 경우에 대한 인증 방법에 관해서는 다루어 지지 않고 있다.

따라서, 이 논문에서는 휴대인터넷 환경에서 인터 도메인간 인증을 지원하기 위해 모바일 IPv6에 다이어미터 프로토콜을 적용하여 보안성을 증대시키고, 데이터의 기밀성을 최소의 시그널 수로 안전하게 전송할 수 있는 효율적인 메커니즘을 제안한다.

이 메커니즘은 무선매체의 공개성 등으로 인해 보안상 많은 결함을 가지고 있는 기존 메커니즘의 문제점을 특별한 보호 장치 없이 네트워크 스니핑, 데이터 변조 등의 공격에 대하여 데이터 기밀성을 보장할 수 있도록 AAA프로토콜을 확장하여 적용하였다.

이 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 휴대인터넷, 모바일 IPv6 그리고 다이어미터등을 분석하고, 3 장에서는 휴대인터넷 환경에서 인터 도메인간 모바일 인증을 제공하기 위한 인증 메커니즘을 제안한다. 4장에서는 제안된 인증 메커니즘의 성능 및 보안 측면을 평가한다. 마지막으로 5장에서 결론을 내린다.

Ⅱ. 관련 연구

2.1 휴대인터넷

휴대인터넷 서비스는 휴대인터넷 단말을 이용하여, 정지 및 이동 중에도 언제, 어디서나 고속으로 무선 인터넷 접속이 가능한 서비스로 정의된다. 이는 정지 및 보행, 그리고 중속(최대 시속 60km/h)의 이동시에도, 실내외에서 휴대형 단말을 이용하여 끊김없는 무선인터넷 접속 환경을 언제나 지원할 수 있는 서비스이다. 특히, 다양한 초고속 무선 멀티미디어 서비스를 원활히 제공할 수 있는 1Mbps 이상의 전송속도를 제공하고, 헤드셋, 노드북, PDA 또는 스마트폰 등의 다양한 멀티미디어 단말을 지원할 수 있어야한다. 휴대인터넷 서비스는 비디오 스트리밍, 오디오 스트리밍, 인터렉티브 게임 등과 같이 전송 지연 조건을 요구하며 해당 서비스 동안 자원을 보장받는 실시간 서비스, 파일 전송, 멀티미디어 메일, 채팅, 이-커머스 등과 같이 전송 지연을 허용하는 비실시간 서비스, 그리고 웹 브라우징과 이-메일 등과 같이 전송 지연을 허용하면서 해당 서비스 동안 자원을 보장받지 않는 최선형 서비스로 분류된다.

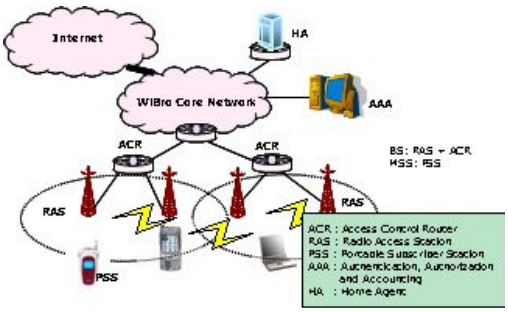

그림 1 휴대인터넷 망 구조
Fig 1 Portable Internet Network Architecture

[그림 1]은 휴대인터넷 네트워크의 망구조를 보여준다[3]. PSS(Portable Subscriber Station)는 휴대인터넷을 위한 단말기를 말하며, RAS(Radio Access Station)는 휴대용 단말기에게 직접적인 인터페이스를 제공하는 기지국의 역할을 담당한다. ACR(Access Control router)은 IP의 라우팅 및 이동성을 관리하고 ACR내의 RAS간 이동성을 제어한다.

2.2 모바일 IPv6

IPv6의 등장에 따라 모바일 IPv6가 제안되었다[4]. 모바일 IPv4와 달리 모바일 IPv6에는 MN이 HA와 직접통신을 하므로 FA가 필요하지 않고, 또한 보안이 필요한 모든 메시지들에 IPSec을 기본적으로 이용한다.

모바일 IPv6에서 MN의 이동에 따른 처리 과정은 [그림 2]와 같다. IPv6에서 라우터는 해당 네트워크의 prefix 값을 전송하고 이를 수신한 IPv6노드가 자신의 인터페이스 주소와 결합하여 IPv6주소를 만든다[5]. 따라서 MN은 이 prefix를 이용해서 자신의 인터페이스 주소와 결합하여 자신이 이용할 COA를 스스로 만든다. COA는 실제로 CN에서 MN으로 패킷을 전송할 때 수신되는 주소이다. COA를 얻은 후, MN은 HA로 바인딩 업데이트 목적지 옵션을 포함한 패킷을 보내서 HA에게 자신의 바인딩을 등록한다. 바인딩 업데이트를 처리한 HA는 바인딩 승인을 MN으로 전송한다.

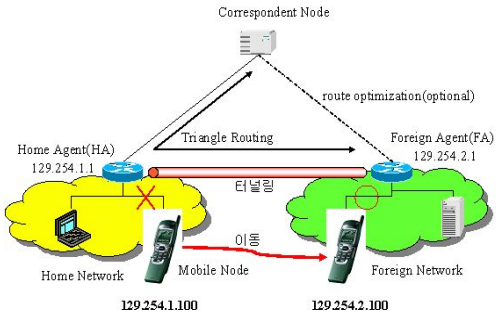

그림 2 Mobile IPv6에서 MN 이동 후 처리 과정
Fig 2 Process Procedure after Move MN to Mobile IPv6

HA에게 자신의 바인딩 정보인 COA를 등록한 MN은 COA를 IPv6 헤더의 소스 주소로 하는 패킷을 CN에게 전송할 수 있다. 패킷을 수신한 CN은 COA를 이용하는 소스 주소와 옵션으로 포함된 홈 주소를 이용하여 MN의 바인딩 정보를 등록하게 된다. 그러나, COA는 수명이 있으며, 만약 MN과 CN이 통신하는 동안에 바인딩 정보 중 COA의 수명이 거의 완료되어 간다면, CN은 MN으로 새로운 바인딩 정보를 보낼 것을 요청하는 바인딩 요청 메시지를 보낸다.

2.3 다이어미터

다이어미터는 PPP(Point-to-Point Protocol), 로밍(Roaming), 이동(Mobile) IP와 같은 기존 기술과, 새롭게 요구되는 기술에 대한 AAA 서비스를 제공하기 위한 가볍고 확장성이 있는 peer 기반의 AAA 프로토콜이다[6,7]. 다이어미터는 AVP(Attribute/Value Pair)와 프록시를 지원한다는 점에서 레디어스와 비슷하나 AVP의 사용 범위에 있어서는 큰 차이를 보인다. 레디어스 주소 공간은 256쌍으로 제한되어 있지만 다이어미터는 32bit의 AVP 주소 공간으로 수백만 쌍 이상을 지원할 수 있다. 이와 같은 강력한 AVP 주소 공간 특성은 이동 사용자나 전용 사용자들을 서비스하기에도 충분하다[8]. 다이어미터 프로토콜은 서버가 NAS(Network Application Support)에게 NAS가 처리할 수 있을 만큼의 메시지를 전송하는 것을 허용하는 신뢰성 있는 윈도우 통신 기반의 전송을 지원한다. 레디어스 서버는 사용자가 요구하지 않으면 메시지를 보낼 수 없는 반면 다이어미터는 가능하며, 이는 서버가 NAS에게 특별한 과금 기능이나 연결 종료 같은 오퍼레이션 수행을 알릴 때에 유용하게 사용된다. 또한 다이어미터는 재전송과 장애 복구 기능을 개선하여 초보적이고 느린 레디어스에 비해 향상된 망 회복력을 제공한다. 마지막으로, 다이어미터는 레디어스가 제공하지 않는 종단간 보안 기법을 제공한다[9].

다이어미터는 로밍과 Mobile IP 망을 지원하기 위해 처음 설계되었다. [그림 3]은 다이어미터 브로커가 방문망에 접속하여 홈망의 자원을 이용하고자 하는 로밍 및 Mobile IP 사용자에 대해 AAA 서비스를 어떻게 제공하는지를 보여준다. 이 경우 방문망 ISP에 있는 다이어미터 서버는 AAA 기능을 수행하기 위해 브로커에 대한 peer로 동작한다.

다이어미터 서버와 브로커 사이의 통신은 브로커가 CA(Certificate Authority)의 역할을 하므로 안전한 연결 상태에서 동작한다. 서버에 대해 인증서를 분배하는 것은 모든 서버가 공유 비밀키를 가지는 것보다도 확장성이 있으면서도 효과적인 방법이다.

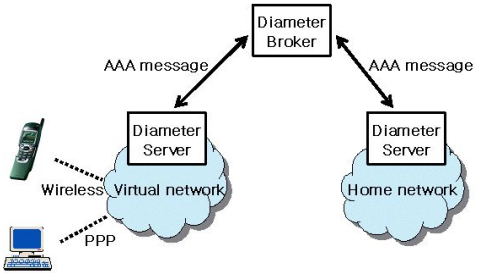

그림 3 로밍을 지원하는 다이어미터 구조
Fig 3 Diameter Architecture with Loaming

다이어미터 기본 프로토콜은 그 자체 그대로 사용되기보다 대게 특별한 애플리케이션을 위해 확장되는 형태로 사용되고, 다음과 같은 IETF WG들에 의해 확대되어 개발되고 있다[10,11].

① ROAMOPS(Roaming Operations) : ISP들 사이에서 사용자의 로밍을 지원하도록 메커니즘, 절차, 프로토콜을 개발 중에 있다.
② NASREQ(Network Access Server Requirements) : 간단한 다이얼 업 사용에서부터 VPN 지원, 스마트 인증 방법, 로밍까지 지원하기 위한 NAS의 디자인이 이루어진다.
③ Mobile IP(IP Routing for Wireless/Mobile Hosts) : IPv4나 IPv6를 사용하는 IP 노드들이 IP 서브넷과 매체 종류들 사이에 로밍을 지원하도록 라우팅 기술 개발 중에 있다.
④ AAA(Authentication, Authorication, Account) : 과금, 전송, 보안, 프록시를 지원하는 다이어미터 관련 프로토콜들을 개발하고 있다.

III. 인터 도메인간 모바일 IPv6을 이용한 인증 메커니즘

3.1 가정

① 이동노드는 유일한 방법으로 네트워크 액세스 식별자(NAI: Network Access Identifier)에 의해 식별된다. IPv6 모바일 노드는 유일한 방법으로MN-NAI에 의해 식별되고 IPv6 모바일 노드는 외부 도메인으로 로밍할 때 AAA 인프라구조에 의해 인증과 권한을 얻어 홈 주소 대신 NAI를 사용할 수 있다.

② 이동노드와 AAAh는 long-term 키를 공유한다. Long-term 키는 네트워크 인증과 사용자 인증을 제공한다. 또한 세션키와 지역 보안 연상을 유추하는데 사용된다.

③ AAAv와 AAAh 사이의 통신은 안전하다. AAA 보안 연상은 홈과 방문 도메인이 서로 신뢰하고 인증과 예방 방법의 정보를 교환하도록 한다.

3.2 파라미터

이 절에서는 제안 메커니즘에서 사용하고 있는 파라미터들을 [표 1]처럼 정의하고 있다.

표 1. 파라미터 정의
Table 1. Parameter Definition

항 목	내 용
BA	바인딩 업데이트에 대한 Mobile IPv6인식
BU	모바일 IPv6 바인딩 업데이트
CR	MN의 인증을 위해 AAAH에서 사용되는 MN의 인증서
H@	HOR/HOA와 ARR/ARA에 존재하는 MN의 홈주소
HA@	HOR/HOA와 ARR/ARA에 존재하는 HA의 주소
HC	MN에 의해 이슈화된 호스트 챌린지(Host Challenge)
Key-infor	MN/attendant, MN/HA사이의 keying material을 설립하기 위한 특정 keying material 초기 정보
LC	Attendant에 의해 이슈화된 Local challenge
NAI	MN의 인식자

3.3 모바일 IPv6을 이용한 인증 메커니즘

IPv6 기능을 가진 이동 노드는 사전 구성된 홈 주소와 홈 에이전트 정보를 가진다. 그러나 제안 메커니즘에서의 이동 노드는 방문 네트워크에서 동적으로 홈 에이전트와 홈 주소를 할당 받아 사전에 홈 주소와 홈 에이전트를 구성하지 않는다. 그리고, 제안 메커니즘에서의 인증 처리는 모바일 IPv6-Feature-Vector AVP를 통해 처리한다.

제안 메커니즘에서 기본적으로 제공되는 기능(키분배, 바인딩 최적화, 홈 네트워크에서의 동적 홈 에이전트 할당)들은 Mobile IPv6 기본 모델과 동일하며, 홈 에이전트만이 방문 네트워크에 추가로 할당되어 홈 도메인과 방문 도메인

사이에서 홈 주소를 동적으로 할당한다. 제안 메커니즘에서 제안하고 있는 메커니즘의 세부적인 단계별 처리절차는 [그림 4]와 같다

● 단계 1 :MN에서 정보 생성

MN은 홈 주소 존재유무에 따라 Mobile-Node-Home-Domain flag와 Home-Agent-only-in-Home-Domain flag의 MIP Feature 데이터를 포함한다.

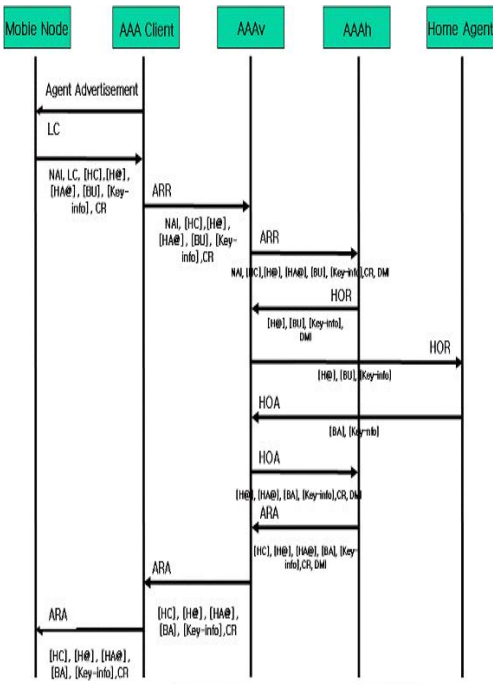

그림 4 제안 메커니즘의 세부 처리절차
Fig 4 Detail Process Procedure of Proposed Mechanism

● 단계 2: Mobile Node ← AAA Client [LC]

AAA 클라이언트로부터 수신된 LC(Local Challenge)를 이용하여 네트워크를 인증하고, 홈 바인딩 Acknowledgement의 소스 IP로부터 홈 에이전트 주소를 얻는다. 홈 에이전트를 얻은 MN은 keying material를 이용하여 보안 협상을 생성한다.

● 단계 3: MN Node → AAA Client

NAI, LC, [HC],[H@], [HA@], [BU], [Key-info], CR

이 단계는 이동 노드가 인증/권한 기능을 수행하기 위해 AAA Client와 상호작용하는 단계이다. 이 과정에서 AAA 클라이언트는 인증 기능과 Mobile IP의 일부 기능을 수행한다. 또한 이중 주소 탐지를 수행하여 LC의 최신성을 검증하고 Diameter ARR 메시지를 생성한다.

● 단계 4: AAA Client → AAAv

NAI, [HC],[H@], [HA@], [BU], [Key-info],CR

이 단계는 AAAv가 AAA 클라이언트로부터 수신된 메시지를 검증하고, Mobile IPv6 특정 벡터 AVP를 체크한다.

● 단계 5: AAAh 동작

NAI, [HC],[H@], [HA@], [BU], [Key-info],CR, DMI

AAAh는 AAAv로부터 전달받은 ARR 메시지를 검증하고 난 후 NAI를 이용하여 사용자를 인증한다. 그리고, 호스트 챌린지와 인증 알고리즘에 적용된 다른 정보 등을 기반으로 네트워크 인증 데이터를 계산한다. 또한, AAAh는 EAP 데이터를 변환할 수 있도록 ARA 명령에 인증 정보와 키 분배를 위한 메시지를 생성하고, 모바일 IPv6-home-agent-address AVP를 체크하여 AAAh가 정확히 홈 에이전트인지를 검증한다.

● 단계 6: AAAh → AAAv

[H@], [BU], [Key-info], DMI

AAAh는 HOR 메시지 안에 모바일 IPv6-mobile-Node-Address AVP나 모바일 IPv6-Home-Agent-Address AVP 포함하여 AAAv에게 보낸다. 그 후, AAAv는 동적 홈 에이전트 할당을 통해 키 분배를 수행한다. AAAh는 선택된 키 분배 메커니즘에 의존하는 바인딩 업데이트를 인증하기 위해 MN과 홈 에이전트 사이의 keying material을 AAAv에게 보낸다.

● 단계 7: AAAv → HA

[H@], [BU], [Key-info]

AAAv는 HOR 메시지에 바인딩 업데이트를 생성하여 HA에게 보내고 홈 에이전트를 할당한다. AAAv는 MN에 대한 IP주소를 할당하고모바일 IPv6-Mobile-Node-Address AVP를 추가한 HOR 메시지를 홈 에이전트에게 전달한다. AAAv는 MN과 홈 에이전트 사이에 보안 협상을 위한 Keying material을 홈 에이전트에게 알린다.

● 단계 8: HA → AAAv

[BA], [Key-nfo]

홈 에이전트가 MN에 대한 바인딩 캐쉬를 생성하거나 요청한다면 홈 IP주소를 할당한다. 홈 에이전트는 적당한 메커니즘에 보안 협상을 생성하고 MN에게 보호된 것을 보내기 위한 바인딩 Acknowledgement를 생성한다. 홈 에이전트는 상태정보를 알리기 위해 AAAv에게 HOA를 돌려보낸다.

● 단계 9: AAAv → AAAh
[H@], [HA@], [BA], [Key-info],CR, DMI

AAAv는 AAAh로 보낸 HOA 메시지 안에 할당된 홈 IP 주소와 홈 에이전트 주소를 포함한다.

● 단계 10: AAAh → AAAv
[HC], [H@], [HA@], [BA], [Key-info],CR, DMI

AAAh는 홈 IP 주소, 홈 에이전트 IP 주소, keying material 정보등을 포함하고 있는 ARA를 AAAv에게 전달한다.

● 단계 11~12: AAAv → Mobile Node
[HC], [H@], [HA@], [BA], [Key-info],CR

AAAv로부터 ARA 메시지를 수신한 AAA 클라이언트는 MN에서 동작할 수 있도록 메시지를 변환한다. 이 메시지는 다음과 같은 기능이 수행된다.

- 인증 데이터
- 바인딩 인식
- keying material 생성

Ⅳ. 성능평가

이 절에서는 제안 메커니즘을 보안 측면과 효율적 측면으로 나누어 성능을 평가한다.

4.1 보안 평가

이 논문에서 제안된 기법은 휴대인터넷 환경에서 인터도메인간 MN의 취약한 보안 측면을 보강하기 위한 방법이다. 따라서 휴대 인터넷에서 많은 보안 문제를 야기하고 있는 재전송 공격, 인증 및 기밀성 등을 중심으로 평가 한다.

① 재전송 공격

AAA 클라이언트와 AAAh 사이에서 발생하는 재전송 공격을 예방하기 위해 타임스탬프(Timestamp)와 random challenge를 사용하고, 또한 AAA구조에서 MN의 인증과 권한 기능을 원활하게 수행할 수 있도록 타임스탬프(Timestamp)와 random challenge가 사용된다. 제안기법에서 재전송 공격을 예방하기 위한 구체적 과정을 기술하면 다음과 같다. 첫째 AAA 수신자는 동기화된 클럭을 요구하고 지역 클럭에 대하여 수신된 메시지의 타임스탬프를 체크하도록 구성된다. 둘째, AAAh와 MN은 캐쉬안에 replay 예방 인식자 HC를 유지한다. 마지막으로 Attendant는 이전에 보낸 LC에 대한 요청에서 지역적으로 LC를 체크함으로써 request 메시지의 응답에 대한 재전송 공격을 예방한다.

② 인증

제안기법에서 MN을 인식하고 인증하기 위해 NAI와 CR(credential)을 사용하고 있다. 초기 인증 설정과 단계 3에서는 MN을 인식하기 위해 NAI를 이용하고, 홈 주소(H@)를 AAAh에서 인증하기 위해 요청 메시지에 CR을 포함시킨 디지털 시그너처를 이용한다. 신뢰적인 보안은 MN의 요청에 의해 AAA 데이터를 바인딩하고 안전한 방법으로 repay 공격을 예방할 수 있도록 서비스를 제공한다. 다이어미터 메시지의 Keying material은 MN과 attendant, MN과 HA 사이에서 keying material을 설립하기 위해 정보를 초기화한 후 최종적으로 MN을 인증작업을 수행하는 AAAh는 키 분배 메커니즘에 의존하는 바인딩 업데이틀 NAI와 Keying material을 이용하여 인증한다.

③ 기밀성

[그림 4]에서 처럼 보안 파라미터의 기밀성을 보장해 주기 위해 이 논문에서는 keying material을 사용하고 있다. keying material을 사용하는 목적은 MN과 AAAh 사이에서 기밀성 있는 데이터를 교환하는 역할과 MN과 HA사이의 바인딩 업데이트를 인증하는데 사용된다. 특히, 바인딩 업데이트를 인증하는 HA는 MN에 대한 일정 크기의 목록을 유지하고, 목록에 저장되지 않은 MN의 바인딩 갱신은 무시한다. 또한, 바인딩 갱신의 송신자가 자격이 있는 MN인지를 확인하여 공격자의 악의적인 redirect 및 DoS공격을 방지할 수 있다.

4.2 효율성 평가

제안 메커니즘의 효율성 평가는 비용함수를 이용하여 노드간의 거리와 각 노드에서의 처리 시간으로 구하였다. 노드간의 거리와 노드의 처리 시간에 대한 단위가 다르므로 노드에서의 처리 시간을 거리로 환산하여 비용 함수를 유도하였다. 실험에 사용된 기본 모델은 [그림 4]의 모델을 사용하였으며, 비용 분석을 위해 [12,13]에서 기술한 접근 방법을 참조하였다. [12,13]에서 기술한 시스템 모델 및 비용 분석 결과를 기반으로 제안된 모델을 성능평가 한다. 제안 모델은 이동성을 나타내기 위해 [12]의 uniform fluid model을 적용하였으며, 이 모델에서 이동 노드의 속도는 μ=0.2로 가정하였다[13].

같은 도메인 안에서의 거리에 대한 비용은 1이고 가까운 두 도메인간의 거리에 대한 비용은 2로 가정할 때 빠른 이동 노드의 인증 비용 비율 PMR 즉, ρ 값에 따르는 비용 비율인 식 (1)의 결과로 구해진다.

$$p = \frac{M_d}{M_g} \quad \cdots\cdots (1)$$

M_d : MN이 도메인간 이동할때 발생되는 전체 비용

M_g : 전체 인증 비용

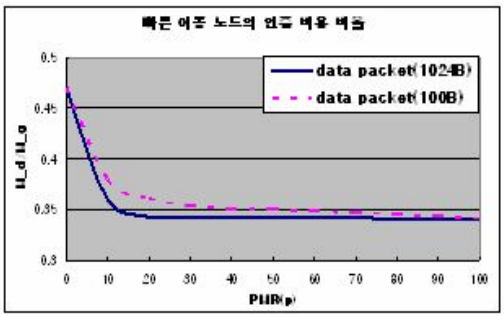

그림 5 빠른 이동 노드의 인증 비용 비율
Fig 5 Authenticaion Cost Ratio of Speedly Move Node

[그림 5]는 이동 단말이 빠른 속도로 이동하는 이동체의 특성을 가지는 경우 PMR값에 따른 인증 비용 비율(M_d/M_g)변화를 보여주고 있다. 이동 속도가 빠르고 데이터 양이 많을수록 전체 인증 이동 비용 비율은 급격히 감소하며 PMR이 50인 지점을 지나면 전체 인증 비용 비율은 0.345를 유지한다. 즉 이 경우 M_g 의 비용은 M_d 에 비해 2.5배 비용 비율이 감소함을 알수 있다.

V. 결론

모바일 IPv6에서 MN이 새로운 도메인으로 이동한 후에 수행하는 인증과정은 경로 최적화를 통한 패킷 전송의 효율성을 높이는 중요한 기능이다. IPSEC을 통한 강한 보안 연관을 갖는 MN과 HA사이의 경로와 달리 도메인간 MN사이의 보안 연관 규정이 없어 보안에 취약하다.

따라서, 이 논문에서는 휴대인터넷 환경에서 인터 도메인간 인증을 지원하기 위해 Mobile IPv6에 다이어미터 프로토콜을 적용하여 보안성을 증대시키고, 데이터의 기밀성을 최소의 시그널 수로 안전하게 전송할 수 있는 효율적인 메커니즘을 제안하였다.

특히, 무선매체의 공개성 등으로 인해 보안상 많은 결함을 가지고 있는 기존 메커니즘의 문제점을 특별한 보호 장치 없이 네트워크 스니핑, 데이터 변조 등의 공격에 데이터 기밀성을 보장할 수 있도록 AAA프로토콜을 확장하여 제안 메커니즘에 적용하고 있다. 또한 도메인간 이동 노드의 이동 확률을 고려한 비용 분석을 PMR 값의 증감 및 데이터 양에 따라 비용을 분석하였다. 향후 연구에서는 모바일 IPv6의 실용화 단계에 적용할 수 있는 인증과 정보 교환을 위한 다양한 응용 연구를 수행할 것이다.

참고문헌

[1] 김홍섭, 이상호, “USN 상호인증을 위한 개선된 신용 모델 설계”, 한국컴퓨터정보학회, 2005. 10. 6.

[2] 이상렬, “실시간 상호인증 지원을 위한 무선랜 보안시스템에 관한 연구”, 한국컴퓨터정보학회, 2005. 10. 6.

[3] "2.3GHz 휴대인터넷 네트워크 참조모델", 정보통신기술보고서 TTAR-0018, 2004년 8월

[4] C. E. Perkins, "IP Mobility Support," Internet RFC 2002, October, 1996.

[5] S. Deering and R. Hinden, "Internet Protocol Version 6(IPv6) Specification", RFC 2460, December 1998.

[6] P. Calhoun, C. Perkins, "Diameter Mobile IPv4 Application", IETF work in progress, 2002

[7] P. R. Calhoun, "Diameter Base Protocol," IETF Internet-Draft, draft-ietf-aaa-diameter-08.txt, work in progress, Nov. 2001.

[8] Diameter extends remote authentication, http://www.nwfusion.com/news/tech/0131tech.html#diagram

[9] Christopher Metz, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," Cisco Systems, http://www.computer.org/internet/v3n6/w6onwire.htm

[10] C.E. Perkins and David B.Johnson. "mobility support in IPv6," in ACM Mobi;com '96, November 1996.

[11] Diameter, http://www.linkionary.com/d/diameter.html

[12] 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.

[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 Sern., paper 9.4, Copenhagen, Denmark, Sep. 1988.

저 자 소 개

정윤수

2000년 2월: 충북대학교 전자계산학과 이학석사

2003~ 현재 : 충북대학교 컴퓨터전공 박사수료

우성희

1999년 2월 : 충북대학교 전자계산학 이학박사

1995년 9월~2006년 2월: 청주과학대학 컴퓨터과학과 부교수

2006년 3월 ~ 현재 : 충주대학교 전기전자및정보공학부 부교수

이상호

1989년 2월 : 숭실대학교 컴퓨터네트워크학과 공학박사

1981년~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수