(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0122053
(43) 공개일자 2007년12월28일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 12/28 (2006.01)
(21) 출원번호 10-2006-0057037
(22) 출원일자 2006년06월23일
심사청구일자 2006년06월23일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 수원캠퍼스내
제주대학교 산학협력단
제주특별자치도 제주시 아라1동 1번지 제주대학교
(72) 발명자
허의남
경기 수원시 영통구 매탄동 주공 그린빌 301-1606
이승연
서울 노원구 상계동 389-419
(74) 대리인
특허법인 신성

전체 청구항 수 : 총 3 항

(54) 모바일 ＩＰｖ６ 기반 이동 노드의 로밍 인증 시스템 및 그방법

(57) 요 약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템 및 그 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, AAA 인증 클라이언트를 통해 이동 노드로부터 개인키가 삽입된 AAA 인증 요청메시지(AAA 키 요청 메시지)를 전달받음에 따라 인증 보증서(Assertion) 요청 세션 키를 생성한 후 상기 전달받은 AAA 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서(assertion key material)를 이용하여 이동 노드의 로밍을 인증하기 위한, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템 및 그 방법을 제공하는데 그 목적이 있음.

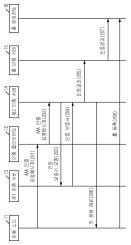
3. 발명의 해결방법의 요지

본 발명은, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템에 있어서, 이동 노드로부터 개인키가 삽입된 인증 요청메시지를 전송받음에 따라 제 2 인증 서버로 상기 인증 요청메시지를 전달하여 상기 이동 노드의 인증을 요청하기 위한 인증 클라이언트; 상기 인증 클라이언트로부터 인증 요청메시지를 전달받음에 따라 인증 보증서 요청 세션 키를 생성한 후 상기 전달받은 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서를 이용하여 상기 이동 노드를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버로 전달하며, 키 생성 재료를 이동 노드로 전송하기 위한 제 2 인증 서버; 및 상기 제 2 인증 서버로부터 전달받은 개인키를 이용하여 해당 이동 노드의 인증 보증서를 생성한 후, 다이어미터(DIAMETER) 프로토콜을 통해 제 2 인증 서버로 전송하기 위한 상기 제 1 인증 서버를 포함함.

4. 발명의 중요한 용도

본 발명은 이동 노드의 인증 등에 이용됨.

대표도 - 도2



특허청구의 범위

청구항 1

모바일 IPv6 기반 이동 노드의 로밍 인증 시스템에 있어서,

이동 노드로부터 개인키가 삽입된 인증 요청메시지를 전송받음에 따라 제 2 인증 서버로 상기 인증 요청메시지를 전달하여 상기 이동 노드의 인증을 요청하기 위한 인증 클라이언트;

상기 인증 클라이언트로부터 인증 요청메시지를 전달받음에 따라 인증 보증서 요청 세션 키를 생성한 후 상기 전달받은 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서를 이용하여 상기 이동 노드를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버로 전달하며, 키 생성 재료를 이동 노드로 전송하기 위한 제 2 인증 서버; 및

상기 제 2 인증 서버로부터 전달받은 개인키를 이용하여 해당 이동 노드의 인증 보증서를 생성한 후, 다이어미터(DIAMETER) 프로토콜을 통해 제 2 인증 서버로 전송하기 위한 상기 제 1 인증 서버

를 포함하는 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템.

청구항 2

제 1 항에 있어서,

상기 제 1 인증 서버 및 제 2 인증 서버는,

DIAMETER 프로토콜에 기반을 둔 AAA(Authentication Authorization Accounting) 서버로서, SAML(Security Assertions Markup Language)의 인증 보증서(Assertions)를 통해 이동 노드의 로밍을 인증하는 것을 특징으로 하는 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템.

청구항 3

모바일 IPv6 기반 이동 노드의 로밍 인증 방법에 있어서,

이동 노드로부터 개인키가 삽입된 인증 요청메시지를 전송받음에 따라 제 2 인증 서버로 상기 인증 요청메시지를 전달하여 상기 이동 노드의 인증을 요청하는 단계;

상기 인증 클라이언트로부터 인증 요청메시지를 전달받음에 따라 인증 보증서 요청 세션 키를 생성한 후 상기 전달받은 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하는 단계;

상기 제 1 인증 서버로부터 전송받은 인증 보증서를 이용하여 상기 이동 노드를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버로 전달하고, 키 생성 재료를 이동 노드로 전송하는 단계; 및

상기 제 2 인증 서버로부터 전달받은 개인키를 이용하여 해당 이동 노드의 인증 보증서를 생성한 후, 다이어미터(DIAMETER) 프로토콜을 통해 제 2 인증 서버로 전송하는 단계

를 포함하는 모바일 IPv6 기반 이동 노드의 로밍 인증 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<7> 본 발명은 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 DIAMETER 프로토콜에 기반을 둔 AAA(Authentication Authorization Accounting) 시스템에서 MIPv6(Mobile Internet Protocol version 6) 기반 이동 노드의 로밍을 효율적으로 인증하기 위한, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템 및 그 방법에 관한 것이다.

<8> 일반적으로, 보안 보장 생성 언어(Security Assertions Markup Language, 이하 SAML)는, 인터넷상에서 확장성

생성 언어(XML) 기반의 비즈니스 보안 정보 교환 표준으로서, 다른 시스템 간 보안 서비스의 상호 운용이 가능한 XML로 된 정보를 기술하는 공통 언어를 말한다.

<9> 이러한 SAML은 인증 보증서(assertion) 제공 기능을 가지는데, 여기서 인증 보증서란, 한 사이트에서 인증을 받은 후 다른 사이트에 방문할 시에 사용자가 이미 인증되었음을 보장해주는 수단이다. 즉, 사용자가 A 사이트에서 인증을 하면, A 사이트는 사용자에게 인증이 성공적으로 이루어졌음을 보장하는 보증서를 발급하고, 사용자가 B 사이트에 방문할 시에 이 보증서를 제공하면 B 사이트는 A 사이트가 발급한 인증 보증서인지를 판단하여, 유효한 보증서이면 추가 인증 작업 없이 B 사이트를 사용할 수 있게 한다.

<10> 또한, MIPv6(Mobile Internet Protocol version 6)는, IPv6 주소를 사용하는 이동 단말을 인증하는데 사용되는 IETF(Internet Engineering Task Force) 이동 IP(Internet Protocol) 표준으로서, 기존 IPv6에 이동성 헤더를 추가하여 바인딩 관련 메시지를 전송하며, 외부 에이전트(FA) 없이 모바일 노드(MN)가 외부 에이전트 기능을 수행한다.

<11> 한편, 다이어미터(이하, DIAMETER) 프로토콜은 차세대 휴대인터넷 및 로밍 네트워크용으로 개발된 인터넷국제표준화기구(IETF)의 표준 프로토콜로서, 공중 무선랜, 휴대인터넷, 광대역통합망(BcN) 등 차세대 네트워크 환경의 인증 시스템 개발에 폭넓게 활용되고 있다.

<12> 이러한 DIAMETER 프로토콜은 기존 IEEE802.1x 라디우스(RADIUS) 프로토콜보다 확장성과 보안성 등의 기술적인 한계를 개선하여, 라디우스 프로토콜이 256 바이트까지 메시지를 송수신할 수 있었는데 반해, DIAMETER 프로토콜은 2의 32승 바이트까지 메시지를 송수신할 수 있다.

<13> 실제 와이브로 서비스를 위해서 단말 수를 결정하는 IP 자원, 접속망의 데이터 전송 속도, 가정 내 제공되는 장치 종류, 각종 미디어 및 서비스에 대한 접속 제한 방식 등을 구현해야 하는데, 이를 위해 가장 중요한 것이 접속 제어와 인증이다.

<14> 이하, DIAMETER 프로토콜에 대해 좀 더 상세히 살펴보기로 한다.

<15> DIAMETER 프로토콜은 크게 메시지 생성 및 전송, 보안, 장애 과금 기능을 포함한 기반 기술(base protocol)과 응용 기술로 분류할 수 있다.

<16> 현재까지 정의된 응용은 라우터에서 액세스를 위해 사용될 확장된 라디우스(RADIUS) 응용(Diameter NASreq Application), MIPv4 응용(Diameter Mobile IPv4 Application), 노드 간 인증을 위한 응용(Diameter CMS Security)이 있으며, 확장성 보장 기능을 통해 새로운 서비스가 출현하면 새로운 보안 응용을 추가할 수 있다.

<17> 이 외에 하부 프로토콜에서 필요한 요구사항을 별도로 정의하고 있다. 즉, DIAMETER 하부 프로토콜은 전송 계층 보안 프로토콜인 TLS(Transport Layer Security) 또는 IPsec(IP Security)을 적용하며, TLS 하부에는 TCP 및 UDP(User Datagram Protocol)가 제공하지 못하는 전송 계층에서의 확실성(Reliability)을 제공하기 위해 SCTP(Stream Control Transmission Protocol)를 적용한다.

<18> 따라서, TLS(Transport Layer Security) 및 IPSec(IP Security)를 이용하여 전송 계층의 Hop-by-Hop 보안을 제공하고, 전송계층의 피어(Peer) 관리 기능을 통하여 전송계층의 실패(Failure)에 대한 검출(Detection) 및 복구(Failover) 기능을 제공하며, 복구 시 프록시(Proxy) 서버가 자동으로 메시지를 다음 홉(Next-Hop)의 피어(Peer)로 재전송하기 때문에 프록시 분산 환경에 아주 적합하다. 이때, DIAMETER 서버는 반드시 TLS와 IPsec을 모두 지원해야 하지만, DIAMETER 클라이언트는 IPsec을 반드시 지원해야 하나 TLS는 옵션 사항이다.

<19> MIPv6 응용의 예를 들면, DIAMETER 서버들은 방문 망 또는, 브로커 망, 또는 홈 망의 AAA 서버들이 되며, DIAMETER 클라이언트는 MIP(Mobile Internet Protocol)의 FA(Foreign Agent) 또는 HA(Home Agent)가 된다.

<20> 한편, DIAMETER 프로토콜은 새로운 정책과 PPP(Point to Point Protocol)같은 기존 기술과 로밍, 이동(Mobile) IP 같은 새로운 기술에 대한 AAA 서비스를 제공하기 위한 가벼우면서도 확장 가능한 피어 기반의 AAA 프로토콜로 정의할 수 있다.

<21> DIAMETER 프로토콜은 AVPs(Attribute Value Pairs)와 프록시를 지원한다는 점에서 RADIUS 프로토콜과 닮았지만, RADIUS 프로토콜의 "Attribute Value"가 255바이트를 넘지 못하는 것과, RADIUS 프로토콜이 확인 메시지를 받기 전에 255개의 메시지만을 유지할 수 있었던 문제를 해결하였다.

<22> 즉, DIAMETER 프로토콜은 더 큰 "Attribute Value" 길이를 지원하기 때문에, DIAMETER 서버는 NAS(Network Access Server)가 처리할 수 있을 만큼의 메시지를 보낼 수 있으며, 장애에 대비할 수 있는 신뢰성 있는 윈도우

통신 기반의 트랜스포트를 지원한다.

<23> 게다가, RADIUS 서버는 클라이언트가 요구하지 않으면 메시지를 보낼 수 없지만, DIAMETER 서버는 NAS로 과금이나 연결 종료를 알려 주어야 할 경우 자체적으로 메시지를 보낼 수도 있다.

<24> 또한, DIAMETER 프로토콜은 재전송과 장애 복구 기능을 개선하여, 약하고 느린 RADIUS 프로토콜보다도 망 회복력이 뛰어나며, RADIUS 프로토콜이 지원하지 않는 종단 간 보안(End-to-End Security) 기법을 제공한다.

<25> 한편, 통신 사업자들은 단순히 모뎀 포트를 제공하는 것에서 그치는 것이 아니라, 불법적으로 서비스를 사용하는 것을 방지해야 하고, 가입자의 권한 레벨을 부여하고 검증해야 하며, 과금 및 자원 계획을 수립하기 위해 네트워크 사용에 대한 측정을 하여야 하기 때문에, 이러한 요구사항을 만족시키는 AAA 서버는 ISP(Internet Service Provider)나 상업 망 제공 사업자에게 매우 중요한 장치이다.

<26> 일반적인 AAA(Authentication Authorization Accounting) 처리 절차는 다음과 같은 단계로 요약할 수 있다.

<27> 1. 각 사용자는 관문장치에 연결하여 망에 대한 접근을 요청한다.

<28> 2. NAS AAA 클라이언트 기능은 사용자의 인증 정보를 받아서 AAA 서버로 전달한다.

<29> 3. AAA 서버는 수신한 데이터를 처리하고 AAA 클라이언트에게 허용 또는 거절과 함께 다른 관련 데이터를 보낸다.

<30> 4. NAS의 AAA 클라이언트는 사용자에게 특정한 자원에 대한 접근이 허용되었는지 또는 거절되었는지를 통지한다.

<31> 이러한 종래의 DIAMETER 프로토콜 기반의 AAA 시스템은 모바일 노드(MN)-홈 에이전트(HA) 간 대칭 키(Symmetric Key) 사용에 있어서 보안이 잘 이루어지지 않고, 방문 망에 홈 에이전트(HA)가 할당될 경우 H_AAA(홈 AAA) 서버와 홈 에이전트 간의 보안 설정(SA: Security Association)이 어려우며, 특히 802.1x/802.11i 등의 링크계층(Link Layer)에서 사용되는 키(Key) 관련 AVPs(AVPs 코드 및 AVPs 이름 등)과 EAP(Extensible Authentication Protocol)의 재시동(Restart) 관련 재인증을 신속하게 처리하지 못하는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<32> 본 발명은 상기 문제점을 해결하기 위하여 제안된 것으로, AAA 인증 클라이언트를 통해 이동 노드로부터 개인키가 삽입된 AAA 인증 요청메시지(AAA 키 요청 메시지)를 전달받음에 따라 인증 보증서(Assertion) 요청 세션 키를 생성한 후 상기 전달받은 AAA 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서(assertion key material)를 이용하여 이동 노드의 로밍을 인증하기 위한, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템 및 그 방법을 제공하는데 그 목적이 있다.

<33> 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

발명의 구성 및 작용

<34> 상기 목적을 달성하기 위한 본 발명의 장치는, 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템에 있어서, 이동 노드로부터 개인키가 삽입된 인증 요청메시지를 전송받음에 따라 제 2 인증 서버로 상기 인증 요청메시지를 전달하여 상기 이동 노드의 인증을 요청하기 위한 인증 클라이언트; 상기 인증 클라이언트로부터 인증 요청메시지를 전달받음에 따라 인증 보증서 요청 세션 키를 생성한 후 상기 전달받은 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서를 이용하여 상기 이동 노드를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버로 전달하며, 키 생성 재료를 이동 노드로 전송하기 위한 제 2 인증 서버; 및 상기 제 2 인증 서버로부터 전달받은 개인키를 이용하여 해당 이동 노드의 인증 보증서를 생성한 후, 다이어미터(DIAMETER) 프로토콜을 통해 제 2 인증 서버로 전송하기 위한 상기 제 1 인증 서버를 포함하는 것을 특징으로 한다.

<35> 한편, 본 발명의 방법은, 모바일 IPv6 기반 이동 노드의 로밍 인증 방법에 있어서, 이동 노드로부터 개인키가 삽입된 인증 요청메시지를 전송받음에 따라 제 2 인증 서버로 상기 인증 요청메시지를 전달하여 상기 이동 노드의 인증을 요청하는 단계; 상기 인증 클라이언트로부터 인증 요청메시지를 전달받음에 따라 인증 보증서 요청 세션 키를 생성한 후 상기 전달받은 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하는 단계; 상

기 제 1 인증 서버로부터 전송받은 인증 보증서를 이용하여 상기 이동 노드를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버로 전달하고, 키 생성 재료를 이동 노드로 전송하는 단계; 및 상기 제 2 인증 서버로부터 전달받은 개인키를 이용하여 해당 이동 노드의 인증 보증서를 생성한 후, 다이어미터(DIAMETER) 프로토콜을 통해 제 2 인증 서버로 전송하는 단계를 포함하는 것을 특징으로 한다.

<36> 또한, 본 발명은 SAML(Seucity Assertion Marup Langue)의 "Assertion" 기술을 DIAMETER 프로토콜에 적용하여 세션 키 교환 방식을 정의한다.

<37> 즉, 본 발명은 MIPv6 Assertion 발생 (Assertion trigger), Assertion 요청 및 응답 (Assertion Request, Assertion Response)의 메시지를 추가하고 Diameter AVPs(Attribute Value Pairs)에 Assertion AVPs를 추가한다.

<38> 또한, 본 발명은 DIAMETER 프로토콜에 기반을 둔 AAA 시스템에서 기존에 Diameter 프로토콜에 정의되어 있지 않은 인증 메시지의 교환 방식을 SAML assertion의 메시지 교환방식에 따라 DIAMETER 프로토콜에 정의하고, AAA 인증서버가 "assertion" 메시지를 통해 이동 노드에 대한 신속하고 효과적인 인증을 제공하여 Diameter 엔티티 간의 메시지 처리 절차를 감소시켜 이동 노드의 효율적인 인증 방식을 제공한다.

<39> 또한, 본 발명은 DIAMETER AAA 프로토콜의 효율성 및 신뢰성의 문제점을 보완하고 DIMAETER 엔티티 간의 메시지 이동 빈도를 최소화한다.

<40> 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명하기로 한다.

<41> 도 1 은 본 발명에 따른 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템의 일실시예 구성도이다.

<42> 도 1에 도시된 바와 같이, 본 발명에 따른 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템은, 이동 노드(11)로부터 개인키가 삽입된 AAA 인증 요청메시지(AAA 키 요청 메시지)를 전송받음에 따라 제 2 인증 서버(14)로 상기 AAA 인증 요청메시지를 전달하여 상기 이동 노드(11)의 인증을 요청하기 위한 인증 클라이언트(AAA 인증 클라이언트)(12), 상기 인증 클라이언트(12)로부터 AAA 인증 요청메시지를 전달받음에 따라 인증 보증서(Assertion) 요청 세션 키를 생성한 후 상기 전달받은 AAA 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버(13)로 전송하고, 상기 제 1 인증 서버(13)로부터 전송받은 인증 보증서(assertion key material)를 이용하여 이동 노드(11)를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버(15)로 전달하며, 키 생성 재료를 이동 노드(11)로 전송하기 위한 제 2 인증 서버(14), 및 제 2 인증 서버(14)로부터 전달받은 개인키를 이용하여 해당 이동 노드(11)의 인증 보증서(assertion key material)를 생성한 후, DIAMETER 프로토콜을 통해 제 2 인증 서버(14)로 전송하기 위한 제 1 인증 서버(13)를 포함한다.

<43> 여기서, 상기 제 1 인증 서버(13)와 제 2 인증 서버(14)는 DSA(Diameter Security Association)을 통해 상호 인증 및 기밀성 제공의 기반을 마련한다.

<44> 또한, 상기 제 1 인증 서버(13)와 제 2 인증 서버(14)는 사용자에게 AAA 서비스를 제공하는 DIAMETER 서버 및 각 서버 사이에 AAA 메시지를 중개하는 프록시(Proxy)서버, 그리고 주소 반환 서비스를 제공하는 리다이렉트(Redirect) 서버를 더 포함할 수도 있다.

<45> 또한, MIPv6를 위한 DIMAETER 기반 AAA 시스템은 방문 네트워크(Visited Networks), 중개 네트워크(Broker Network), 홈 네트워크(Home Network)로 구성된다.

<46> 도 2 는 본 발명에 따른 모바일 IPv6 기반 이동 노드의 로밍 인증 방법에 대한 일실시예 흐름도이다.

<47> 먼저, 이동 노드(11)가 제 1 인증 서버(13)를 통해 일 네트워크에 접속하고 있다.

<48> 이후, 이동 노드(11)가 타 네트워크로 이동(로밍)하기 위해 개인키를 이용하여 인증 데이터를 생성한 후 AAA 인증 요청메시지(AAA 키 요청 메시지)에 삽입하여 인증 클라이언트(AAA 인증 클라이언트)(12)로 전송한다(AReq: Authentication Request)(201).

<49> 그러면, 인증 클라이언트(12)는 타 네트워크상의 제 2 인증 서버(14)로 AAA 인증 요청메시지를 전달하여 이동 노드(11)의 인증을 요청한다(AMR : Authentication MN-Request)(202).

<50> 이후, 제 2 인증 서버(14)는 인증 클라이언트(12)로부터 AAA 인증 요청메시지를 전달받음에 따라 인증 보증서(Assertion) 요청 세션 키를 생성한 후 상기 전달받은 AAA 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버(13)로 전송한다(AAR : Authentication Assertion Request)(203).

<51> 이때, AAA 인증 요청 메시지는 이동 노드(11)의 이전 접속 네트워크상의 인증 서버 정보를 포함하고 있다. 또한, 제 1 인증 서버(13)와 제 2 인증 서버(14) 사이에는 사전 협의에 의한 로밍 계약이 체결되어 있어야 한다.

<52> 이후, 제 1 인증 서버(13)는 제 2 인증 서버(14)로부터 전달받은 개인키를 이용하여 해당 이동 노드(11)의 인증 보증서(assertion key material)를 생성한 후, DIAMETER 프로토콜을 통해 제 2 인증 서버(14)로 전송한다(Authentication Assertion Request)(204). 이때, 제 1 인증 서버(13)는 추가적으로 AVPs(Attribute Value Pairs) 데이터를 추가/수정할 수도 있다.

<53> 이후, 제 2 인증 서버(14)는 제 1 인증 서버(13)로부터 전송받은 인증 보증서(assertion key material)를 통해 이동 노드(11)를 인증한 후 인증 결과를 담은 응답 메시지를 홈 인증 서버(15)로 전달한다(AMA : Authentication MN-ACK)(205).

<54> 이때, 제 2 인증 서버(14)는 이동 노드(11)가 제 1 인증 서버(13)로부터 전달받은 추가 및 수정된 AVPs 메시지 중 인증 보증서를 포함하는 메시지를 수신할 경우에 이동 노드(11)를 정상적으로 인증할 수도 있다.

<55> 그리고, 제 2 인증 서버(14)는 키 생성 재료를 이동 노드(11)로 전송한다(ARsp : Authentication Response)(206).

<56> 이후, 홈 인증 서버(15)는 제 2 인증 서버(14)로부터 전달받은 인증 결과를 홈 에이전트(16)로 전달한다(207).

<57> 이후, 이동 노드(11)는 홈 에이전트에 등록(BU : Binding Update / BA : Binding Acknowledgement)한다.

<58> 이러한 절차를 통해 이동 노드(11)는 신속하고 안정적으로 로밍할 수 있다.

<59> 본 발명은 제 1 인증 서버(13)와 제 2 인증 서버(14) 간의 통신 및 상호 인증을 위한 기반을 제공한다.

<60> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

<61> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

발명의 효과

<62> 상기와 같은 본 발명은, AAA 인증 클라이언트를 통해 이동 노드로부터 개인키가 삽입된 AAA 인증 요청메시지(AAA 키 요청 메시지)를 전달받음에 따라 인증 보증서(Assertion) 요청 세션 키를 생성한 후 상기 전달받은 AAA 인증 요청 메시지 상의 개인키와 함께 제 1 인증 서버로 전송하고, 상기 제 1 인증 서버로부터 전송받은 인증 보증서(assertion key material)를 이용하여 이동 노드의 로밍을 신속하게 인증할 수 있는 효과가 있다.

<63> 또한, 본 발명은 키 분배 및 생성 과정에서 효율성을 보장하고 방문 AAA 서버 간의 세션 키를 방문 AAA 서버가 직접 발급함으로써, DIAMETER 노드 간의 메시지 빈도 및 통신량을 감소시키는 효과가 있다.

<64> 또한, 본 발명은 "assertion" 세션 키가 위조되거나 노출당하더라도 일회성 데이터이기 때문에 인증 및 무결성을 보장할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 도 1 은 본 발명에 따른 모바일 IPv6 기반 이동 노드의 로밍 인증 시스템의 일실시예 구성도,

<2> 도 2 는 본 발명에 따른 모바일 IPv6 기반 이동 노드의 로밍 인증 방법에 대한 일실시예 흐름도이다.

<3> * 도면의 주요 부분에 대한 부호의 설명

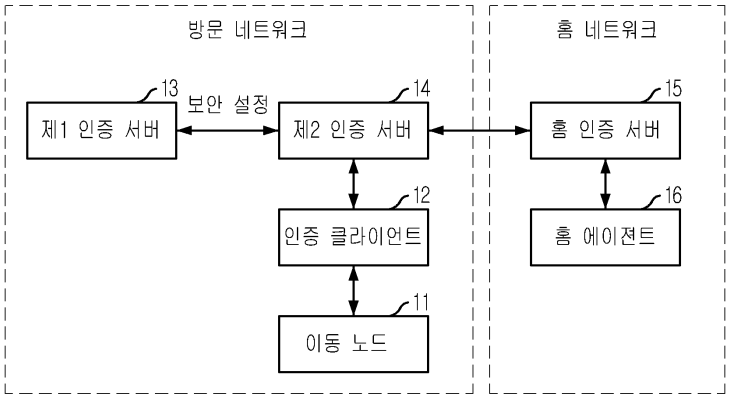
<4> 11 : 이동 노드 12 : 인증 클라이언트

<5> 13 : 제 1 인증 서버 14 : 제 2 인증 서버

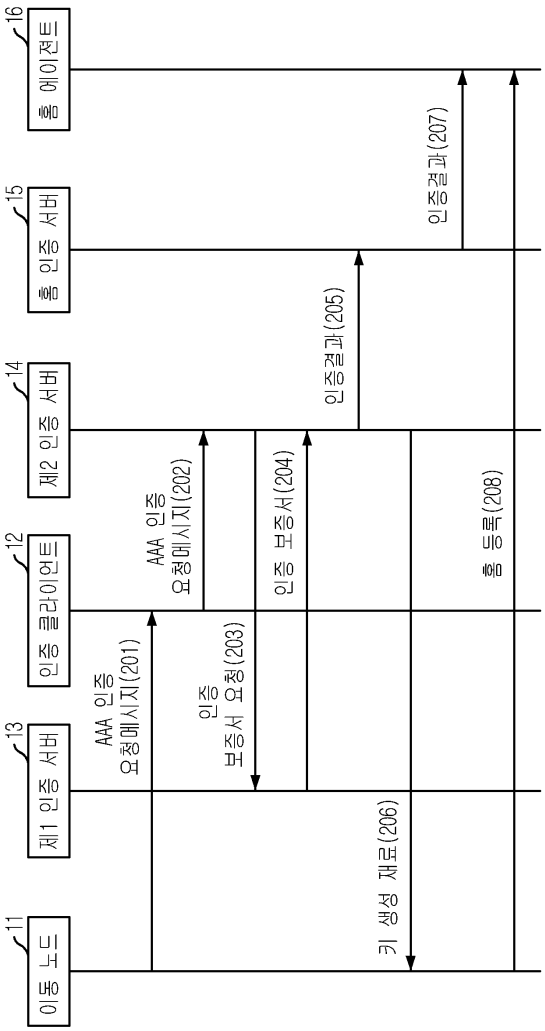
<6> 15 : 홈 네트워크 16 : 홈 에이전트

도면

도면1



도면2


11
이동 노드
13
제1 인증 서버
12
인증 클라이언트
14
제2 인증 서버
15
홈 인증 서버
16
홈 에이전트
AAA 인증
요청메시지(201)
인증
보증서 요청(203)
AAA 인증
요청메시지(202)
인증 보증서(204)
인증결과(205)
키 생성 재료(206)
인증결과(207)
홈 등록(208)