(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년01월12일
(11) 등록번호 10-1479922
(24) 등록일자 2014년12월31일

(51) 국제특허분류(Int. Cl.)
H04W 40/02 (2009.01) *H04W 8/02* (2009.01)
H04W 12/08 (2009.01)
(21) 출원번호 10-2013-7025446(분할)
(22) 출원일자(국제) 2010년01월22일
심사청구일자 2013년09월26일
(85) 번역문제출일자 2013년09월26일
(65) 공개번호 10-2013-0119507
(43) 공개일자 2013년10월31일
(62) 원출원 특허 10-2011-7021025
원출원일자(국제) 2010년01월22일
심사청구일자 2011년09월08일
(86) 국제출원번호 PCT/US2010/021761
(87) 국제공개번호 WO 2010/093506
국제공개일자 2010년08월19일
(30) 우선권주장
12/369,374 2009년02월11일 미국(US)
(56) 선행기술조사문헌
US20040202183 A1*
US20080065777 A1*
US20080137591 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
알까멜 루슨트
프랑스 92100 불론뉴-비영꾸르 루뜨 들 라 렌느 148/152
(72) 발명자
카쿠리브 바이오레타
미국 뉴져지 07041 밀번 하란 써클 4
선다람 가나파티
미국 뉴져지 08844 힐스보로 힉코리 힐 로드 10
(74) 대리인
장훈

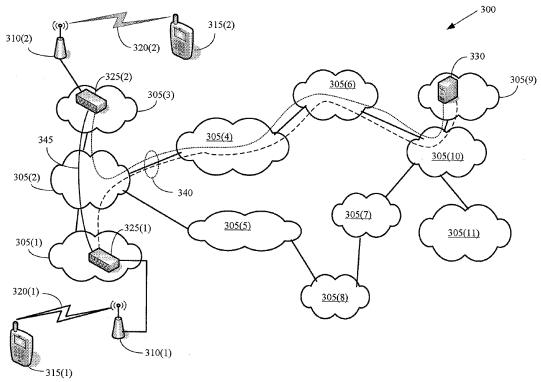
전체 청구항 수 : 총 7 항 심사관 : 이다나

(54) 발명의 명칭 **모바일 네트워크들에서 네트워크 기반 라우트 최적화를 보장하기 위한 방법**

(57) 요 약

본 발명은 제 1 홈 게이트웨이와 연관된 제 1 모바일 디바이스를 수반하는 라우트 최적화 방법을 제공한다. 이 방법의 일 실시예는 제 1 이동성 포워딩 엔티티에서 구현되고 제 1 이동성 포워딩 엔티티에 제 1 모바일 디바이스를 등록하는 단계를 포함한다. 제 1 모바일 디바이스는 제 1 모바일 디바이스에 의해 전송된 등록 메시지에 포함된 세션 키를 이용하여 등록된다. 실시예는 또한 세션 키를 이용하여 제 1 이동성 포워딩 엔티티와 종단 노드 사이에 보안 라우트를 확립하는 단계를 포함한다. 보안 라우트는 제 1 홈 게이트웨이를 바이패스한다.

대 표 도



특허청구의 범위

청구항 1

제 1 홈 게이트웨이와 연관된 제 1 모바일 디바이스를 수반하는 라우트 최적화(route optimization) 방법으로서, 제 1 이동성 포워딩 엔티티(first mobility forwarding entity)에서 구현되는, 상기 라우트 최적화 방법에 있어서:

상기 제 1 이동성 포워딩 엔티티에서, 상기 제 1 모바일 디바이스에 의해 전송된 등록 메시지에 포함된 세션 키를 이용하여 상기 제 1 모바일 디바이스를 등록하는 단계로서, 상기 세션 키는 상기 제 1 모바일 디바이스 및 상기 제 1 이동성 포워딩 엔티티에 의해 공유되고, 상기 등록 메시지 내의 상기 세션 키의 수신은 상기 제 1 모바일 디바이스를 대신하여 보안 라우트(secure route)를 확립하기 위한 인가(authority)를 상기 제 1 이동성 포워딩 엔티티에 위임하는, 상기 등록 단계; 및

상기 제 1 이동성 포워딩 엔티티에서, 상기 제 1 이동성 포워딩 엔티티와 종단 노드 사이에 보안 라우트를 확립하는 단계로서, 상기 보안 라우트는 상기 제 1 홈 게이트웨이를 바이패스하고, 상기 보안 라우트는 상기 제 1 모바일 디바이스와 상기 종단 노드 사이에 패킷들을 전송하도록 사용되는, 상기 보안 라우트 확립 단계를 포함하고,

상기 제 1 모바일 디바이스를 상기 제 1 이동성 포워딩 엔티티에 등록하는 단계는:

상기 제 1 모바일 디바이스로부터 바인딩 등록(binding registration)을 수신하는 단계로서, 상기 바인딩 등록은 세션 키를 이용하여 상기 제 1 모바일 디바이스에 의해 부호화되는(signed), 상기 바인딩 등록 수신 단계; 및

상기 제 1 모바일 디바이스가 상기 제 1 이동성 포워딩 엔티티에 등록되는 것을 나타내는 바인딩 확인응답을 상기 제 1 모바일 디바이스에 전송하는 단계로서, 이 전송에 따라 상기 제 1 이동성 포워딩 엔티티가 상기 제 1 모바일 디바이스를 대신하여 보안 라우트들을 확립하고 상기 제 1 모바일 디바이스에 대한 라우트 최적화를 수행하도록 인가되는, 상기 바인딩 확인응답 전송 단계를 포함하고, 상기 제 1 이동성 포워딩 엔티티가 상기 종단 노드의 식별 정보를 캐싱하는, 라우트 최적화 방법.

청구항 2

제 1 항에 있어서,

상기 종단 노드는 웹 서비스를 상기 제 1 모바일 디바이스에 제공하도록 구성된 서버이고, 상기 보안 라우트 확립 단계는 상기 서버 또는 상기 웹 서비스에 할당된 인터넷 프로토콜(IP) 어드레스 또는 도메인 네임 중 적어도 하나를 이용하여 상기 보안 라우트를 획립하는 단계를 포함하는, 라우트 최적화 방법.

청구항 3

제 1 항에 있어서,

상기 종단 노드는 제 2 모바일 디바이스와 연관된 제 2 이동성 포워딩 엔티티이고, 상기 보안 라우트 확립 단계는:

상기 제 2 이동성 포워딩 엔티티에 등록되는 상기 제 2 모바일 디바이스에 대한 라우트를 최적화하기 위해 상기 제 1 모바일 디바이스로부터의 요청에 응답하여 상기 제 2 이동성 포워딩 엔티티를 발견하는 단계를 포함하는, 라우트 최적화 방법.

청구항 4

제 1 항에 있어서,

상기 제 1 모바일 디바이스와 상기 종단 노드 사이에 제 1 호 세션을 확립한 후에, 상기 보안 라우트가 제 2 호 세션과 연관된 적어도 하나의 패킷을 포워딩하는데 이용될 수 있도록, 상기 제 1 이동성 포워딩 엔티티와 상기 종단 노드 사이에 상기 보안 라우트를 유지하는 단계를 포함하는, 라우트 최적화 방법.

청구항 5

제 1 및 제 2 홈 게이트웨이들과 각각 연관된 제 1 및 제 2 모바일 디바이스들 사이의 라우트 최적화 방법으로서, 제 1 이동성 라우팅 엔티티에서 구현되는 상기 라우트 최적화 방법에 있어서:

상기 제 1 이동성 라우팅 엔티티에서, 상기 제 1 모바일 디바이스 및 상기 제 1 이동성 포워딩 엔티티에 의해 공유된 세션 키를 이용하여 상기 제 1 모바일 디바이스를 등록한 제 1 이동성 포워딩 엔티티로부터, 상기 제 2 모바일 디바이스를 등록한 제 2 이동성 포워딩 엔티티를 발견하기 위한 요청을 수신하는 단계로서, 상기 요청은 상기 제 2 모바일 디바이스의 어드레스를 포함하고, 상기 세션 키의 수신은 상기 제 1 모바일 디바이스를 대신하여 보안 라우트들을 확립하도록 상기 제 1 이동성 포워딩 엔티티를 인가하는, 상기 요청 수신 단계;

상기 제 1 이동성 라우팅 엔티티에 의해 유지되는 데이터베이스 및 상기 제 2 모바일 디바이스의 어드레스를 이용하여 상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 적어도 하나를 발견하는 단계; 및

상기 제 1 및 제 2 홈 게이트웨이들을 바이패스하는 보안 라우트가 상기 제 1 및 제 2 이동성 포워딩 엔티티들 사이에서 확립될 수 있도록, 상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나를 상기 제 1 이동성 포워딩 엔티티에 제공하는 단계를 포함하고,

상기 제 2 이동성 포워딩 엔티티가 바인딩 확인응답을 전송하기 전에, 상기 제 1 모바일 디바이스의 위치를 검증하는, 라우트 최적화 방법.

청구항 6

제 5 항에 있어서,

상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나를 발견하는 단계는:

상기 데이터베이스가 상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나와 상기 제 2 모바일 디바이스의 어드레스 사이의 이전에 결정된 연관을 포함할 때, 상기 제 2 모바일 디바이스의 어드레스 또는 아이덴티티 중 상기 적어도 하나를 이용하여 상기 데이터베이스로부터 상기 제 2 이동성 포워딩 엔티티의 어드레스를 액세스하는 단계;

상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나 및 상기 제 2 모바일 디바이스의 어드레스를 연관시키는 정보를 획득하기 위해, 상기 데이터베이스가 상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나와 상기 제 2 모바일 디바이스의 어드레스 사이의 이전에 결정된 연관을 포함하지 않을 때, 적어도 하나의 다른 이동성 라우팅 엔티티 또는 적어도 하나의 다른 엔티티를 질의하는 단계;

상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나 및 상기 제 2 모바일 디바이스의 어드레스 사이의 상기 연관을 상기 데이터베이스에 추가하는 단계; 및

상기 제 2 이동성 포워딩 엔티티의 어드레스 또는 아이덴티티 중 상기 적어도 하나를 상기 제 1 이동성 포워딩 엔티티에 제공하는 단계를 포함하는, 라우트 최적화 방법.

청구항 7

제 1 홈 게이트웨이와 연관된 제 1 모바일 디바이스를 수반하는 라우트 최적화 방법으로서, 상기 제 1 모바일 디바이스에서 구현되는, 상기 라우트 최적화 방법에 있어서:

상기 제 1 모바일 디바이스에 의해 전송된 등록 메시지에 포함된 세션 키를 이용하여 제 1 모바일 포워딩 엔티티에 상기 제 1 모바일 디바이스를 등록하는 단계로서, 상기 세션 키는 상기 제 1 모바일 디바이스 및 상기 제 1 이동성 포워딩 엔티티에 의해 공유되고, 상기 등록 메시지 내의 상기 세션 키의 수신은 상기 제 1 모바일 디바이스를 대신하여 보안 라우트들을 확립하도록 상기 제 1 이동성 포워딩 엔티티를 인가하는, 상기 등록 단계;

상기 세션 키를 이용하여 상기 제 1 모바일 포워딩 엔티티와 종단 노드 사이에 보안 라우트를 확립하기 위한 요청을 상기 제 1 이동성 포워딩 엔티티에 전송하는 단계로서, 상기 보안 라우트는 상기 제 1 홈 게이트웨이를 바이패스하는, 상기 전송 단계; 및

상기 종단 노드를 향한 상기 보안 라우트 상의 전송을 위한 적어도 하나의 패킷을 상기 제 1 이동성 포워딩 엔

티티에 전송하는 단계를 포함하고,

상기 제 1 모바일 디바이스 등록 단계는 상기 제 1 이동성 포워딩 엔티티에 바인딩 등록을 제공하는 단계로서, 상기 바인딩 등록은 상기 세션 키를 이용하여 상기 제 1 모바일 디바이스에 의해 부호화되는, 상기 제공 단계를 포함하고,

상기 종단 노드가 바인딩 확인응답을 전송하기 전에, 상기 제 1 모바일 디바이스의 위치를 검증하는, 라우트 최적화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 통신 시스템들에 관한 것이고, 특히 무선 통신 시스템들에 관한 것이다.

배 경 기 술

[0002] 통상적인 무선 통신 시스템들은 무선 액세스 네트워크들, 또는 액세스 포인트들, 기지국들, 기지국 라우터들 등과 같은 다른 무선 엔티티들을 이용한 무선 접속을 제공한다. 예를 들면, 모바일 유닛은, 네트워크에 통신 가능하게 결합되는 무선 액세스 네트워크와의 공중 인터페이스를 통해 무선 통신 링크를 확립할 수 있다. 모바일 유닛은, 다른 모바일 유닛과의 통신 세션을 확립하는 것과 같이, 네트워크에 의해 제공되는 서비스들에 액세스하기 위해 무선 통신 링크를 이용할 수 있다. 2개의 모바일 유닛들 사이의 통신 세션을 이용하여 전송되는 정보는 아날로그 또는 디지털 정보일 수 있고, 모바일 유닛들 사이의 통신 경로는 회로-스위칭된 아키텍처 또는 패킷-스위칭된 아키텍처를 이용하여 형성될 수 있다. 회로-스위칭된 아키텍처에서, 전용 통신 경로는, 예를 들면, 2개의 모바일 유닛들 사이에 형성되고, 2개의 모바일 유닛들에 의해서만 이용될 수 있다. 대조적으로, 패킷-스위칭된 아키텍처들은 패킷들로 정보를 나누고, 패킷들은 모바일 유닛들과 그들 네트워크 피어들 사이에서 패킷들을 포워딩하기 위해 공용 패킷 네트워크 인프라스트럭처를 이용하여 2개의 모바일 유닛들 사이의 수많은 경로들을 따라 전송될 수 있다. 따라서, 패킷-스위칭된 네트워크 인프라스트럭처를 통하는 경로들의 일부 또는 전부는 네트워크 서버 또는 고정된 가입자와 같은 패킷-스위칭된 네트워크에 접속된 다른 엔티티들 또는 다른 모바일 유닛들에 의해 공유될 수 있다. 또한, 거의 모든 패킷-스위칭된 무선 시스템들은 라우팅 및 포워딩을 위한 인터넷 프로토콜(IP)에 의존한다. 패킷 스위칭된 네트워크들은 더욱 개방형이고, 이러한 이유로 공격들에 취약하다. 따라서, 보안은 패킷-스위칭된 네트워크들에서 가장 중요하다.

[0003] 무선 통신 시스템은 개념적으로 다중층 모델로 구성될 수 있다. 예를 들면, 개방형 시스템간 상호접속(OSI: Open Systems Interconnection) 기준 모델은 7개층들을 포함한다: 애플리케이션층, 프리젠테이션층, 세션층, 전송층, 네트워크층, 데이터 링크층, 및 물리층. 애플리케이션층은 "가장 높은" 층이고, 따라서 최종 사용자에게 가장 가깝다. 애플리케이션층은 다양한 애플리케이션들을 제공하기 위한 소프트웨어를 포함한다. 프리젠테이션층은 콘텍스트를 확립하고, 상이한 애플리케이션층 엔티티들 간을 변환한다. 세션층은 상이한 컴퓨터들 사이에서 확립된 세션들을 제어하고 로컬 및 원격 애플리케이션들 사이의 접속들을 관리한다. 전송층은 최종-사용자들 사이의 투명한 데이터 전달을 제공하고, 상부층들로의 신뢰 가능한 데이터 전달 서비스들을 지원한다. 네트워크층은 소스로부터 하나 이상의 네트워크들을 통해 목적지로 가변 길이 데이터 시퀀스들을 전달하기 위한 기능적이고 절차적인 지원을 제공한다. 데이터 링크층은 네트워크 엔티티들 사이의 데이터 전달뿐만 아니라, 에러 정정을 제공하기 위한 기능적이고 절차적인 지원을 제공한다. 물리층은 "가장 낮은" 층이며, 전기적이고 물리적인 명세들뿐만 아니라, 디바이스들 사이에서 에러없는 전송을 위해 필요한 인코딩 및 변조 방식들을 규정한다.

[0004] 패킷 데이터 애플리케이션들을 지원하기 위해 다양한 무선 액세스 기술들이 물리층 및 링크층에서 구현될 수 있다. 일부 예시적인 무선 액세스 기술들은, HRPD, 1X-EVDO, UMTS/HSPA, WIMAX/IEEE-802.16, 3GPP2-UMB, 및 3GPP-LTE과 같은 제 2 세대(2G), 제 3 세대(3G), 및 제 4 세대(4G) 기술들을 포함한다. 이들 무선 액세스 기술들은 제 3 세대 파트너쉽 프로젝트들(3GPP, 3GPP2) 및 WiMAX 포럼 네트워크 작업 그룹(NWG: Network Working Group)에 의해 확립된 표준들 및/또는 프로토콜들과 같이, 표준들 및/또는 프로토콜들에 따라 동작한다. 이미 배포된 기술들의 기존 커버리지 영역들 및 상이한 신호 세기들의 이점을 취하기 위하여, 기기 판매상들은, 다중 무선 액세스 기술들을 이용하여 통신할 수 있는 듀얼 모드(또는 멀티-모드) 모바일 유닛들을 개발 및 배포하고 있다. 예를 들면, 듀얼-모드 모바일 유닛은 2개의 상이한 무선 액세스 기술들에 따라 동작하는 IP 접속의 2개의 독립된 수단을 구현할 수 있다. 동시에, 서비스 제공자들은 무선 접속을 제공하기 위해 하나보다 많은 무선 액세스 기술을 점점 더 이용하고 있다. 예를 들면, 일부 서비스 제공자들은, 오버레이된 메시들 및/또는 상이한

액세스 기술들과의 오버랩핑 커버리지 영역들을 포함하는 이종 네트워크들(heterogeneous networks)을 배치하였다. 오버레이된 메시들 및 오버랩핑 커버리지 영역들은 레거시 기술에서 더 새로운 기술로의 진화의 일부로서, 또는 배치 및/또는 동작 비용들을 감소시키고, 전체 통신 스펙트럼 특성들을 개선하는 등과 같은 다른 이유들로 이용될 수 있다.

[0005] 애플리케이션층 기술들도 또한 급속하게 진화되고 있다. 예를 들면, 새로운 브라우저 기술들이 구식 WAP 기반 방법들을 신속하게 대체하고, 거의 모든 인터넷 애플리케이션들이 모바일 가입자들에 제공하도록 '동원(mobilized)'되는 출발점에 있다. 더 많은 인터넷 프로토콜(IP) 기반 모바일-대-모바일 서비스들도 또한 기존의 셀룰러 모바일-대-모바일 서비스들을 보완 및 업그레이드하기 위해 도입되고 있다. 이들 모바일 대 모바일 서비스들의 예들은 기존의 셀룰러 음성 서비스들을 보완하는 모바일 VoIP, 및 통상적인 셀룰러 SMS의 풍부한 버전들을 익스플로어링하는 것을 공유하는 텍스트, 오디오 및 비디오를 가진 모바일 IM을 포함한다. 인터넷 전화(VoIP)는 오디오 신호들(음성 신호들과 같은)을 디지털 포맷으로 인코딩하기 위한 기술이며, 디지털 포맷은 네트워크층에서 인터넷 프로토콜(IP)을 이용하는 패킷-스위칭된 네트워크를 통한 전송을 위한 패킷들을 형성하기 위해 이용될 수 있다. VoIP 패킷들은, 목적지 VoIP 세션 피어(예를 들면, 모바일 유닛)에서의 연속하는 패킷들 사이 또는 전송기에서 수신기로의 전송시 큰 지연들이 소스 피어에 의해 생성된 오디오 신호의 품질을 저하시킬 수 있기 때문에, 통상적으로 지연-불허용 및 지터 민감 정보라 칭해진다. 결과적으로, VoIP 애플리케이션들은 통상적으로 VoIP 패킷들을 선택된 서비스 품질(QoS) 레벨로 제공하도록 제약된다. 예를 들면, 모바일 유닛에서 구현되는 VoIP 애플리케이션은 네트워크를 통해 전송된 패킷들에 대해 최소 레벨들의 지연, 지연 지터 등을 유지하도록 요구될 수 있다. 일부 경우들에서, 고객들은 특정 애플리케이션들에 대해 더 높은 QoS 레벨들의 전체 더 높은 QoS 레벨들을 획득하기 위해 더 큰 비용들을 지불할 수 있다.

[0006] 통상적인 무선 액세스 네트워크는 일반적으로 2개의 구성요소들로 나누어진다: 무선 네트워크 및 코어 네트워크. 통상적인 코어 네트워크는 두 레벨들의 IP 게이트웨이들을 포함하며, IP 게이트웨이들은 도 1에 도시된 통신 네트워크(100)에 의해 도시된 바와 같이, 모바일 유닛들이 인터넷에 액세스하도록 허용한다. 방문된 게이트웨이들(VGW)은 코어 네트워크와 무선 네트워크 사이에 인터페이스를 제공하며, 이는 기지국들, 기지국 제어기들, 기지국 라우터들, 액세스 포인트들 등과 같은 엔티티들을 포함한다. 홈 게이트웨이들(HGW)은 방문된 게이트웨이와 통신하고 코어 네트워크와 인터넷 사이에 인터페이스를 제공한다. 홈 게이트웨이는 통상적으로, 인터넷에 대한 게이트웨이로서 서빙하는 것 외에도, IP 어드레스 할당 및 관리를 책임진다. 홈 게이트웨이 및 방문된 게이트웨이는, 도 2에 도시된 통신 네트워크(200)에 의해 도시된 바와 같이, 특히 홈 게이트웨이 및 방문된 게이트웨이가 상이한 서비스 제공자들에 의해 동작될 때 및/또는 2개의 게이트웨이들이 서로로부터 지리적으로 또는 위상적으로 떨어져 있을 때 하나 이상의 피어 네트워크들에 의해 분리될 수 있다.

[0007] 홈 게이트웨이, 방문된 게이트웨이, 및 이들 게이트웨이들 사이의 임의의 피어 네트워크들은 인터넷에 또는 이로부터 이동하는 패킷들에 대한 초크 포인트들(choke points)이 될 수 있다. 예를 들면, 2개의 모바일 유닛들이 확립된 호 세션을 가지는 경우, 2개의 모바일 유닛들에 대한 코어 네트워크 게이트웨이들은 2개의 상이한 도시들에 있을 수 있다. 공중 인터페이스들을 제공하는 기지국들은 또한, 코어 네트워크 게이트웨이들 중 어느 하나와는 완전히 상이한 도시들에 있을 수 있다. 일부 경우들에서, 기지국과 홈 게이트웨이 사이의 라우트는 백본 오퍼레이터들에 걸친 피어링 관계들로 인해 상이한 도시들의 다수의 피어링 네트워크들을 통해 가로지를 수 있다. 네트워크의 토폴로지에 의존하여, 동일 방문된 게이트웨이에 의해 서빙되는 호들에서도 다수의 게이트웨이들 및/또는 피어링 네트워크들을 통해 라우팅될 수 있다. 예를 들면, 시카고의 회의에 참여하는 두 사용자들(뉴욕 시티로부터 하나 및 로스 앤젤레스로부터 하나) 사이의 호는, 호가 걸릴 때 사용자들이 동일한 건물에 있을 수 있을 때에도, 시카고에서 뉴욕 도시로 로스 앤젤레스로 라우팅된 다음 다시 시카고로 라우팅되어야 할 수 있다. 이 시나리오는 때때로 "트라이앵글 라우팅 문제"를 나타내며, 이것은 패킷들이, 인터넷 호스트로부터 모바일 노드로(즉, 트라이앵글의 빗변) 직접 경로의 존재에도 불구하고, 인터넷 호스트로부터 홈 에이전트를 통해 모바일 노드로(즉, 트라이앵글의 2개의 다리들을 따라) 라우팅되기 때문이다.

[0008] 실제 통신 네트워크들의 다이버시티는 트라이앵글 라우팅 문제를 상당히 복잡하게 한다. 사용자의 위치들에서의 지리적 다이버시티, 무선 네트워크, 코어 네트워크의 방문된 게이트웨이, 및 코어 네트워크 내의 전송으로 인해, 오퍼레이터들은 인터넷으로 트래픽을 라우팅하기 위해 다양한 피어링 포인트들을 이용하도록 강요받는다. 사실상, 네트워크들의 다수의 클러스터들은 다양한 표준들 및 피어링 정책들에 의해 지시된 라우팅 및 포워딩 경로들로 생성되며, 이것은 비효율성들을 도입할 수 있다. 예를 들면, 다중 피어링 포인트들을 통한 모바일 유닛 호들의 강요된 라우팅은 최종-사용자 불만으로 변하는 단-대-단 레이턴시의 극적인 증가뿐만 아니라, 추가되는 조작 비용(OPEX)을 유발할 수 있는 전송시의 증가된 비용을 야기할 수 있다. 초크 포인트들은 또한 고장-허

용범위의 태생적 결여로 인해 대규모의 사용불능들 및 비효율성들을 생성할 잠재성을 가진다. 이들 결함들은 물리층 및 애플리케이션층 기술들의 진화에 의해 제공되는 네트워크에 대한 액세스의 효율성을 손상시킬 수 있다. 이들 효과들은 또한, 상당한 비율의 모바일-대-모바일 호가 동일 방문된 게이트웨이에 의해 잠재적으로 서빙된 지리적 영역 내로 제한될 수 있다는 사실에 의해 악화될 수 있다.

[0009] 다양한 인터넷/무선 표준들 초안들 및 연구 간행물들은 트라이앵글 라우팅 문제를 개선하기 위한 방식들을 제안하였다. 한가지 기술은 모바일 IPv6의 일부로서 채택된 클라이언트-기반 최적화 기술이다. 그러나, 이 기술은 클라이언트의 관여(예를 들면, 인터넷 호스트 및/또는 모바일 노드)를 필요로 하고, 각각의 대응 노드마다 하나씩 수행된다. 또한, 프로토콜은 모바일 노드 및 대응 노드 둘다가 IPv6와 순응하고 IPv6 홈 및 케어-오브 어드레스들(care-of addresses)을 이용하여 어드레스될 수 있을 때에만 적용한다. 클라이언트-기반 라우트 최적화 기술들은 이들이 정교하고, 다루기 힘들고, 보안 실수들을 하기 쉽기 때문에 광범위하게 구현되지 않았다.

[0010] 트라이앵글 라우팅 문제를 처리하기 위한 다른 방식은, 클라이언트에 대한 다중 IP 어드레스들을 이용하고 정책들에 기초하여 특정 흐름들을 라우팅하는 정책 기반 로컬 브레이크아웃 기술(policy based local breakout technique)이다. 정책 기반 로컬 브레이크아웃 기술들은 주로, 한 네트워크에서 다른 네트워크로 및/또는 다중 서비스 제공자들 사이에서 로밍하는 가입자들을 처리하려는 것이다. 예를 들면, US 네트워크를 방문하는 아시아 가입자를 고려한다. 이 경우, 정책 기반 로컬 브레이크아웃 기술은 2개의 '홈' 게이트웨이들 - 아시아에 하나 그리고 US의 다른 하나에 가입자를 할당한다. 그 후에, 호들이 라우팅되는 방법을 결정하기 위해 하나 이상의 정책들이 이용될 수 있다. 예를 들면, 정책들은 레이턴시 민감 호들이 US 홈 게이트웨이에 의해 할당된 IP 어드레스를 이용하여 국부적으로 라우팅되는 것을 지시할 수 있다. 정책들은 또한, 다른 애플리케이션들이 아시아의 홈 게이트웨이를 통해서만(예를 들면, 가입자의 언어로 된 음악 서비스) 라우팅되는 것을 지시할 수 있다. 아시아 홈 게이트웨이를 통해 라우팅되는 애플리케이션들은 아시아 홈 게이트웨이에 의해 할당된 IP 어드레스를 이용하여 사용자의 모바일을 처리할 것이다.

[0011] 다른 대안은 미디어-자각 라우팅 개념들(media-aware routing concepts)을 이용하는 것이며, 이것은 다양한 타입들의 디바이스들(유선 및 무선 둘다)과 통신하는 이종 네트워크들에서 이용될 수 있다. 예를 들면, 미디어-자각 라우팅을 구현하는 시스템은, 전송중인 미디어의 타입에 기초하여 최적의 라우트를 제공하도록 시도할 수 있다. 예를 들면, 한 정책에 따라 VoIP 호들이 라우팅될 수 있고, 다른 정책에 따라 스트리밍 비디오가 라우팅될 수 있고, 또 다른 정책에 따라 텍스트 메시지들이 라우팅될 수 있다.

발명의 내용

해결하려는 과제

[0012] 개시된 요지는 상기에 기재된 하나 이상의 문제들의 영향들을 처리하기 위한 것이다. 다음은 개시된 요지의 일부 양태들의 기본적인 이해를 제공하기 위해 개시된 요지의 간략화된 요약을 제공한다. 이 요약은 개시된 요지의 총망라된 개요가 아니다. 이것은 개시된 요지의 키 또는 중요한 요소들을 식별하거나 개시된 요지의 범위를 나타내려는 것이 아니다. 그것의 전적인 목적은 나중에 논의되는 더욱 상세한 기술에 대한 도입부의 간략화된 형태로 일부 개념들을 제공하기 위한 것이다.

과제의 해결 수단

[0013] 일 실시예에서, 제 1 홈 게이트웨이와 연관된 제 1 모바일 디바이스를 수반하는 라우트 최적화 방법이 제공된다. 이 방법의 일 실시예는 제 1 이동성 포워딩 엔티티(first mobility forwarding entity)에서 구현되고 제 1 이동성 포워딩 엔티티에서 제 1 모바일 디바이스를 등록하는 단계를 포함한다. 제 1 모바일 디바이스는 제 1 모바일 디바이스에 의해 전송된 등록 메시지에 포함된 세션 키를 이용하여 등록된다. 실시예는 또한, 세션 키를 이용하여 제 1 이동성 포워딩 엔티티와 종단 노드 사이에 보안 라우트를 확립하는 단계를 포함한다. 보안 라우트는 제 1 홈 게이트웨이를 바이패스한다.

[0014] 개시된 요지는 첨부 도면들과 함께 취해진 다음의 기술을 참조하여 이해될 수 있으며, 도면들에서 동일한 참조 번호들은 동일한 요소들을 식별한다.

도면의 간단한 설명

[0015] 도 1은 예시적인 무선 통신 시스템을 개념적으로 도시한 도면.

도 2는 모바일 스위칭 센터들의 통상적인 네트워크 및 다양한 피어링 네트워크들을 통한 상호접속들을 개념적으로 도시한 도면.

도 3은 보안 프록시-기반 라우트 최적화를 지원하는 무선 통신 시스템의 제 1 예시적인 실시예를 개념적으로 도시한 도면.

도 4는 보안 프록시-기반 라우트 최적화를 지원하는 무선 통신 시스템의 제 2 예시적인 실시예를 개념적으로 도시한 도면.

도 5는 보안 프록시-기반 라우트 최적화 방법의 예시적인 일 실시예를 개념적으로 도시한 도면.

발명을 실시하기 위한 구체적인 내용

[0016] 개시된 요지는 다양한 수정들 및 대안적인 방법들을 수용할 수 있고, 그 특정 실시예들이 도면들에 예의 방식으로 도시되었고 본 명세서에 상세하게 기술되었다. 그러나, 특정 실시예들의 본 명세서의 기술은 개시된 요지를 개시된 특정 형태들로 제한하려는 것이 아니라, 반대로, 첨부된 특허청구범위의 범위 내에 있는 모든 수정들, 등가들 및 대안들을 커버하려는 의도임을 알아야 한다.

[0017] 예시된 실시예들은 하기에 기술된다. 명확히 하기 위하여, 실제 구현들의 모든 특징들이 이 명세서에 기술되는 것은 아니다. 임의의 이러한 실제 실시예의 전개에서 수많은 구현-특정 판단들은 시스템-관련 및 비즈니스-관련 제약들과의 순응과 같이 개발자의 특정 목적들을 달성하려는 것이고, 이것은 구현마다 다를 것임을 당연히 알 것이다. 또한, 이러한 개발 효과는 복잡하고 시간-소모적일 수 있지만, 그럼에도 본 개시내용의 이점을 갖는 본 기술분야의 통상의 기술자에게는 일상적인 작업임을 알 것이다.

[0018] 개시된 요지가 지금부터 첨부된 도면들을 참조하여 기술될 것이다. 본 기술분야의 통상의 기술자에게 잘 알려진 세부사항들로 본 발명을 모호하게 하지 않도록 단지 설명하기 위한 목적으로 다양한 구조들, 시스템들 및 디바이스들이 도면들에 개략적으로 도시된다. 그렇지만, 개시된 요지의 예시적인 예들을 기술하고 설명하기 위해 첨부된 도면들이 포함된다. 본 명세서에 이용된 단어들 및 구문들은 관련 기술분야의 통상의 기술자에 의한 단어들 및 구문들의 이해와 일관된 의미를 가지는 것으로 이해되고 해석되어야 한다. 단어 또는 구문의 특정 정의, 즉 본 기술분야의 통상의 기술자에 의해 이해되는 일상적이고 관습적인 이해와 상이한 정의는 본 명세서의 단어 또는 구문의 일관된 사용에 의해 내포하기 위한 의도가 없다. 용어 또는 구문이 특정 의미, 즉 당업자에 의해 이해되는 것 이 외의 의미를 가지려 한다면, 이러한 특정 정의는 단어 또는 구문에 대한 특정 정의를 직접적이고 명확하게 제공하는 정의 방식으로 명세서에 명확히 기재될 것이다.

[0019] 일반적으로 말하면, 본 출원의 주제는 레이턴시를 감소시킴으로써 높은 최종 사용자 경험 품질(QoE)을 제공하는 보안 프록시 기반(또는 네트워크-기반) 라우트 최적화이다. 본 명세서에 기술된 기술들은 또한, 완전히 독립된 국유지 모바일 데이터 네트워크(PLMN: public land mobile data network)에 이르는 네트워크 효율성을 개선할 수 있으며, PLMN은 또한 모바일 인터넷이라고 칭해질 수 있다. 본 명세서에 기술된 보안 프록시 기반 라우트 최적화 기술들의 실시예는 다음의 설계 원리들 중 하나 이상을 구현한다:

[0020] • 최적화된 라우트들은 잘 알려진 서비스 거부(DoS) 공격들을 제거하는 보안 라우팅을 제공한다. 또한, 보안 라우팅은 최적의 방식으로 다수의 모바일 오퍼레이터들 사이에서 작업해야 한다.

[0021] • 네트워크(또는 프록시) 기반 라우트 최적화 기술들은 값비싼 공중 인터페이스를 통한 트래픽 뿐만 아니라 클라이언트 입력을 최소화하도록 적응될 수 있다. 네트워크 기반 방법들을 이용하는 것은 또한 클라이언트들에 대한 암시적 보호를 제공하고 클라이언트 디바이스의 역할을 감소시킬 수 있고, 그에 의해 클라이언트 디바이스의 동작/설계를 간략화하고 배터리 전력을 절약한다.

[0022] • 보안 라우트 최적화 기술들은 기존의 표준들, 모바일 네트워크들 및 인터넷과의 상호 작용 및/또는 역호환성을 지원하는 진화적 방식을 반영한다. 따라서, 본 명세서에 기술된 보안 라우트 최적화 기술들의 실시예들은 IPv4 뿐만 아니라 IPv6과 같은 인터넷 프로토콜들 및 레거시 모바일에 대해 작동할 수 있고, 액세스 네트워크에서 구현되는 매크로-이동성 관리 프로토콜들과 무관한 다수의 액세스 네트워크들에 걸쳐 무결절로 작동할 수 있다. 따라서, 본 명세서에 기술된 보안 라우트 최적화 기술들의 일부 실시예들은 기존 표준들 및 네트워크들에 대한 강화들(enhancements)로서 다루어질 수 있고, 그에 의해 보안 라우트 최적화 기술들의 점진적인 롤-아웃(roll-out)을 가능하게 한다.

[0023] 일 실시예에서, 본 명세서에 기술된 보안 라우트 최적화 기술은, 본 명세서에서 이동성 라우팅 엔티티(MRE: Mobility Routing Entity) 및 이동성 포워딩 엔티티(MFE: Mobility Forwarding Entity)로서 칭해지는 2개의 새로운 기능적 엔티티들을 도입함으로써 구현될 수 있다. 그러나, 본 기술분야의 통상의 기술자들은 이들 기능적 엔티티들의 상이한 실시예들이 상이한 용어를 이용하여 나타낼 수 있음을 알아야 한다. 새로운 기능적 엔티티들을 이용하면 기존의 모바일 데이터 네트워크 표준들, 제품들뿐만 아니라 인터넷과의 용이한 통합 및 상호-작용을 허용할 수 있다. 본 명세서에 이용된 바와 같이, 단어 "라우팅(routing)"은 무선 표시 시스템을 통해 데이터를 라우팅하기 위해 이용되는 제어 비행기 경로들, 테이블들 또는 정책들의 생성을 의미하는 것으로 이해될 것이다. 본 명세서에 이용된 바와 같이, 단어 "포워딩(forwarding)"은 무선 통신 시스템을 통해 정보(일반적으로 패킷들의 형태로)를 이동시키는 라우팅 기능들에 의해 생성되는 정책들에 대한 작동의 처리를 의미하는 것으로 이해될 것이다.

[0024] 보안 라우트 최적화는 (가능하면 이종) 무선 통신 시스템을 통해 통신하는 2개의 모바일 디바이스들의 맥락에서 본 명세서에서 주로 논의된다. 모바일 디바이스들 둘다는 상이한 공중 인터페이스들을 통해 무선 통신 시스템에 액세스할 수 있다. 그러나, 본 개시내용의 이점을 갖는 본 기술분야의 통상의 기술자들은 본 명세서에 기술된 기술들이 인터넷 외부 또는 무선 통신 시스템에서 로밍 모바일 디바이스와 임의의 다른 종점 또는 종단 노드 사이의 보안 라우트들을 확립하기 위해 이용될 수 있음을 알 것이다. 예를 들면, 본 명세서에 기술된 기술들은 로밍 모바일 디바이스와 연관된 이동성 포워딩 엔티티와 로밍 모바일 디바이스에 의해 액세스되는 웹 페이지를 제공하는 서버 사이의 보안 라우트를 확립하기 위해 이용될 수 있다. 이 시나리오에서, 보안 라우트 최적화는 IP 어드레스 또는 서버의 다른 식별자를 이용하여 서버와 이동성 포워딩 엔티티 사이의 보안 라우트를 확립할 수 있다.

[0025] 본 명세서에 기술된 보안 라우트 최적화 기술들의 실시예들은 기존의 기술들을 능가하는 다수의 이점들을 가진다. 보안성은 회로 네트워크들의 폐쇄된 속성에 의해 주로 음성 네트워크들에서 제공된다. 유사하게, 제 2 세대 셀룰러 네트워크들에서 구현되는 로컬-브레이크아웃 기술들은 로컬 중계방식(local trunking)에 기초하며, 이것은 표면상 회로 개념이다. 결과적으로, 이들 기술들은 현재 및 미래의 IP 기반(즉, 개방형) 모바일 데이터 네트워크들에 대한 충분한 보안성을 제공하지 않는다. 본 명세서에 기술된 보안 라우트 최적화 기술들은 제 3 세대 및 후속 셀룰러 네트워크들에서 구현되는 이종 개방형 네트워크들을 통한 보안 경로들을 제공한다. 또한, 제 2 세대 셀룰러는 제 1 세대 셀룰러 배치들이 그 시간에 흔치 않기 때문에 기존의 네트워크들에 관련되지 않고 혁신 실행의 혜택을 누렸다. 그러나, 최근에 생겨난 셀룰러 데이터 네트워크들에 대한 풍경은 매우 상이하고, 10억 모바일 데이터 가입자들에 가까운 큰 중심부들을 지원하는 기존의 표준들 및 네트워크들을 준수해야 한다. 본 명세서에 기술된 보안 라우트 최적화 기술들의 역 호환성은 기존 및 최근에 생겨난 셀룰러 데이터 네트워크들과의 통합을 용이하게 하도록 도울 수 있다.

[0026] 이제 도 3을 참조하여, 무선 통신 시스템(300)의 제 1 예시적인 실시예가 도시된다. 예시된 실시예에서, 무선 통신 시스템(300)은 다수의 상호 접속된 제공자 네트워크들(305(1-11))을 포함한다. 특징적인 인덱스들(1-11)은 개별 제공자 네트워크들 또는 제공자 네트워크들의 서브세트들을 나타내기 위해 이용될 수 있다. 그러나, 이들 인덱스들은 제공자 네트워크들(305)을 집합적으로 참조할 때 생략될 수 있다. 이러한 관습은 도면들에 도시된 다른 요소들에 적용될 수 있고 숫자 및 하나 이상의 특징적인 인덱스들에 의해 식별될 수 있다. 본 개시내용의 이점을 가진 본 기술분야의 통상의 기술자들은 백본 제공자 네트워크들(305)이라고도 칭해질 수 있는 제공자 네트워크들(305)이 다양한 표준들 및/또는 프로토콜들에 따라 동작할 수 있음을 알아야 한다. 예를 들면, 무선 통신 시스템(300)은 2G 및 3G 표준들 및/또는 프로토콜들의 혼합에 따라 동작하는 제공자 네트워크들(305)을 포함하는 이종 시스템일 수 있다. 또한, 구현을 위한 기술들 및 제공자 네트워크들(305)의 동작은 본 기술분야에 알려져 있고, 명확히 하기 위해, 본 출원에 기술된 요지와 관련된 제공자 네트워크들(305)의 동작 및 구현의 양태들만 본 명세서에 더 기술될 것이다.

[0027] 무선 통신 시스템(305)은 또한 무선 접속성을 제공하기 위해 이용되는 무선 액세스 포인트들(310)을 포함한다. 단 2개의 무선 액세스 포인트들(310)이 도 3에 도시되어 있지만, 본 개시내용의 이점을 갖는 본 기술분야의 통상의 기술자들은 무선 통신 시스템(305)이 더 많은 액세스 포인트들(310)을 포함할 수 있음을 알아야 한다. 또한, 액세스 포인트(310)는 기지국, 기지국 라우터들, 블루투스 액세스 포인트들, IEEE 802 프로토콜들에 따라 동작하는 액세스 포인트들 등을 포함할 수 있다. 따라서, 모바일 유닛들(315)은 모바일 유닛들(315)과 액세스 포인트들(310) 사이의 공중 인터페이스(320)를 통해 무선 통신(305)에 액세스할 수 있다. 모바일 유닛들(315)은 또한, 모바일 노드, 대응 노드, 이동국, 사용자 기기, 가입자 기기, 가입자 스테이션 등과 같은 단어들을 이용하여 나타낼 수 있다.

[0028] 예시된 실시예에서, 모바일 유닛(315(1))은 기지국(310(1))에 부착되며, 기지국(310(1))은 제공자 네트워크(305(1))에서 구현되는 방문된 게이트웨이(325(1))에 접속된다. 모바일 유닛(315(2))은 기지국(310(2))에 부착되며, 기지국(310(2))은 제공자 네트워크(305(3))에서 구현되는 방문된 게이트웨이(325(2))에 접속된다. 예시된 실시예에서, 두 모바일 유닛들(315(1-2))은 동일한 홈 게이트웨이(330)에 고정된다. 방문된 게이트웨이들(325)은 홈 게이트웨이(330)로부터 지리적으로 및/또는 위상적으로 분리되는 이러한 시나리오는 방문된 게이트웨이들(325)의 수가 홈 게이트웨이(330)의 수보다 통상적으로 훨씬 더 많기 때문에 매우 공평하다. 또한, 홈 게이트웨이들(330)은 IP 어드레스들 및 정책들을 할당하고 관리하기 위해 홈 게이트웨이들(330)에 대해 더 쉽게 하기 위하여 중앙집중화될 수 있다. 그러나, 본 개시내용의 이점을 가진 본 기술분야의 통상의 기술자들은 대안적인 실시예들에서 모바일 유닛들(315)이 상이한 홈 게이트웨이들(330)에 고정될 수 있다는 것을 알아야 한다.

[0029] 홈 게이트웨이(330)를 통한 통상적인 경로(340)는 도 3에 도시된 바와 같이, 다수의 백본 네트워크들(310) 및 피어링 포인트들을 통한 전송을 관련시킨다. 통상적인 경로(340)에서의 다수의 백본 네트워크들(310) 및/또는 피어링 포인트들은, 지연들, 손상된 패킷들, 증가된 레이턴시, 및 사용자의 경험 품질을 저하시킬 수 있는 다른 결함들을 유발할 수 있다. 동작에 있어서, 보안 라우트 최적화는 방문된 게이트웨이들(325) 사이의 보안 최적화된 경로(345)를 생성하기 위해 이용될 수 있다. 예시된 실시예에서, 보안 최적화된 경로(345)는 홈 게이트웨이(330)를 바이패스하고, 따라서, 통상적인 경로(340)에 비해, 개재된 제공자 네트워크들(305)의 수를 감소시킨다. 보안 라우트 최적화는 모바일 유닛(315(1))의 등록, 모바일 유닛(315(2))과 연관되는 방문된 게이트웨이(325(2))의 발견, 방문된 게이트웨이들(325) 사이의 보안 라우트(345)를 확립하는 것 및 그 후 보안 라우트(345)를 통해 패킷들을 전송하는 것을 포함한다. 예시된 실시예에서, 모바일 유닛(315(1))은 보안 라우트 최적화를 수행하기 위해 방문된 게이트웨이(325(1))를 인가하고, 그 후에 모바일 유닛(315(1))은 이 기능에 대한 책임을 방문된 게이트웨이(325(1))에 위임한다. 이 경우, 모바일 유닛(315(1))만이 임의의 주어진 흐름에 대한 '권리들(rights)'을 가지고, 라우트들에서의 임의의 변경들은 모바일 유닛(315(1))에 의해 인가될 수 있으며, 그 후에 이러한 동작들을 수행하기 위한 책임을 방문된 게이트웨이(325(1))에 위임한다.

[0030] 일 실시예에서, 방문된 게이트웨이들(325)은, 보안 라우트 최적화 기능을 구현하기 위해 이용되는 로컬 엔티티인 이동성 포워딩 엔티티(MFE, 도 3에 도시되지 않음)를 각각 지원할 수 있다. MFE는 또한, 모바일 유닛들(315) 사이에 패킷들을 전송하기 위해 규정되고 이용되는 보안 라우트를 위한 종점들로서 이용될 수 있는 다른 MFE들을 식별하기 위해 이동성 라우팅 엔티티(MRE)와 상호작용한다. 일 실시예에서, MRE는 방문된 네트워크들(325)의 식별들뿐만 아니라 모바일 유닛들(315)의 방문된 위치에 관한 정보를 제공하는 큰 분산형 데이터베이스이다. 도 3이 2개의 모바일 유닛들(315) 사이의 통신을 도시하지만, 본 기술분야의 통상의 기술자들은 본 명세서에 기술된 기술들이 또한, 하나의 모바일 유닛(315)과 연관된 이동성 포워딩 엔티티와, IP 어드레스에 의해 식별되는 웹사이트에 대한 서버와 같은 임의의 다른 네트워크 종점 또는 종단 노드 사이에 보안 라우트 최적화를 제공하기 위해 이용될 수 있음을 알아야 한다.

[0031] 도 4는 무선 통신 시스템(400)의 제 2 예시적인 실시예를 개념적으로 도시한다. 예시된 실시예에서, 무선 통신 시스템(400)은 공중 인터페이스들(415)을 통해 모바일 유닛들(410)에 대한 무선 접속을 제공하기 위해 이용되는 기지국들(405)을 포함한다. 무선 통신 시스템(400)의 제 2 예시적인 실시예는 또한 기지국들(405)에 통신 가능하게 결합된 복수의 이동성 포워딩 엔티티들(420)을 포함한다. 하나 이상의 이동성 라우팅 엔티티들(425)은 또한 무선 통신 시스템(400)에 포함된다. 다양한 대안적인 실시예들에서, 이동성 라우팅 엔티티들(425)은 독립적일 수 있거나 또는 분산형 이동성 라우팅 엔티티(425)의 일부일 수 있다. 본 개시내용의 이점을 갖는 본 기술분야의 통상의 기술자들은 특정 수의 엔티티들 및 도 3에 도시된 이들 엔티티들 사이의 상호접속성이 예시하려는 것이며, 대안적인 실시예들이 상이한 방식으로 상호접속되는 상이한 수들의 이들 엔티티들을 포함할 수 있음을 알아야 한다.

[0032] 도 4에 도시된 제 2 예시적인 실시예에 도시된 다양한 엔티티들은 일부 경우들에서 도 3에 도시된 엔티티들에서 구현되거나 및/또는 이와 오버랩할 수 있다. 예를 들면, 하나 이상의 이동성 포워딩 엔티티들(420) 및/또는 이동성 라우팅 엔티티들(425)은 도 3에 도시된 하나 이상의 방문된 게이트웨이들(325) 또는 홈 게이트웨이들(330)에서 구현될 수 있다. 그러나, 본 개시내용의 이점을 갖는 본 기술분야의 통상의 기술자들은 이것이 본 명세서에 기술된 기술들의 실시에 필요하지 않음을 알아야 한다. 일부 실시예들에서, 이동성 포워딩 엔티티들(420) 및/또는 이동성 라우팅 엔티티들(425)은 방문된 게이트웨이들(325) 및 홈 게이트웨이들(330)과 무관하게 구현된 독립형 엔티티들일 수 있으며, 예를 들면, 이동성 엔티티들이 상이한 물리적 위치들에 배치될 수 있는 상이한 "박스들"에서 구현될 수 있다.

[0033] 예시된 실시예에서, 모바일 유닛(410(1))은 기지국(405(1))에 부착되며, 기지국(405(1))은 이동성 포워딩 엔티

티(420(1))와 통신할 수 있다. 모바일 유닛(410(1))은 모바일 유닛(410(2))과 호 세션을 확립하도록 시도할 수 있으며, 모바일 유닛(410(2))은 기지국(405(2)) 및 이동성 포워딩 엔티티(420(2))에 부착된다. 그 후에, 보안 라우트 최적화는 패킷들이 보안 라우트(430)를 통해 이동성 포워딩 엔티티들(420(1-2)) 사이에 직접 터널링되도록 허용하기 위해 수행될 수 있다.

[0034] 보안 라우트 최적화 기술은 이동성 포워딩 엔티티(420(1))에 등록하는 모바일 유닛(410(1))으로 시작한다. 일 실시예에서, 정책 기반 라우트 최적화를 강화하기 위해 다중-단계 등록 처리가 이용되고, 모바일 유닛(410(1))으로 하여금 보안 라우트 최적화를 수행하기 위한 권한을 이동성 포워딩 엔티티(또는 방문된 게이트웨이)(420(1))에 위임할 수 있게 한다. 등록은 모바일 유닛(410(1))이 네트워크에서 보안 라우트 최적화 서비스들을 호출하도록 인가되는지의 여부를 검증하도록 무선 통신 시스템(400)을 허용할 수 있다. 예를 들면, 모바일 유닛(410(1))은 이동성 포워딩 엔티티(420(2))가 보안 프록시-기반(또는 네트워크-기반) 라우트 최적화 및/또는 이동성 포워딩 엔티티(420(1))에 의해 제공될 수 있는 다른 서비스들에 대한 광고를 전송하는 것을 요청하기 위한 광고를 요구할 수 있다. 그 후에, 이동성 포워딩 엔티티(420(1))는 제공된 라우트 최적화 서비스들을 광고할 수 있고, 일부 경우들에서, 등록 및 위임을 위해 모바일 유닛(410(1))과 논스들(nonces)을 교환할 수 있다. 또한, 이동성 포워딩 엔티티(420(1))는 다른 서비스들 및 성능 강화들을 광고할 수 있고, 이것은 헤더 압축, 방화벽 서비스들, 암호화 등을 포함할 수 있다.

[0035] 그 후에, 모바일 유닛(410(1))은 이동성 포워딩 엔티티(420(1))에 부호화된 바인딩 등록을 전송할 수 있고, 이것은 바인딩 확인응답을 리턴할 수 있다. 그러나, 본 기술분야의 통상의 기술자들은 본 기술이 바인딩 등록들 및/또는 바인딩 확인응답들의 전송에 제한되지 않고 대안적인 실시예들이 다른 메시지들의 교환을 지원할 수 있음을 알아야 한다. 모바일 유닛(410(1))으로부터의 바인딩 등록은 보안 라우트 최적화 서비스와 연관된 서비스 ID를 포함할 수 있다. 모바일 유닛(410(1))은 마찬가지로 부가의 서비스를 고르도록 선택할 수 있고, 바인딩 등록에서 부가의 서비스들을 나타낼 수 있다. 이동성 포워딩 엔티티(420(1))로부터의 바인딩 확인응답은 모바일 유닛(410(1))이 후속 통신을 위해 이용할 수 있는 논스들을 포함할 수 있다. 바인딩은 유한한 유지 시간을 가질 수 있고, 그래서 모바일 유닛(410(1))은 바인딩을 계속 이용하기를 원하는 경우에 등록의 만료 전에 재등록할 필요가 있다. 성공적인 바인딩 등록 및 확인응답은 모바일 유닛(410(1))이 보안 라우트 최적화(및 다른 서비스들)를 수행하기 위한 권한을 네트워크에 위임하고, 네트워크가, 모바일 유닛(410(1))이 이러한 서비스들에 대해 인가되었음을 확인응답하는 것을 나타낸다. 일 실시예에서, 모바일 유닛(410(1)) 및 이동성 포워딩 엔티티(420(1))는, 바인딩 등록 및 확인응답 둘다를 위해 지정되는 세션 키를 공유하고 바인딩 등록을 부호화하기(signed) 위해 이용될 수 있다. 일 실시예에서, 세션 키는 이전 액세스 인증 절차로부터 도출될 수 있다.

[0036] 일단 모바일 유닛(410(1))이 이동성 포워딩 엔티티(420(1))에 등록되었으면, 모바일 유닛(410(2))에 근접한 이동성 포워딩 엔티티(420(2))를 찾기 위한 발견이 수행될 수 있다. 발견은 호 셋업과 동시에 또는 트래픽 흐름이 개시된 후에 수행될 수 있다. 일 실시예에서, 모바일 유닛(410(1))은 바인딩 확인응답에 전송되는 논스들의 리스트로부터 하나의 논스를 선택하고 목적지 모바일 유닛(410(2))의 IP 어드레스와 보안 프록시-기반 라우트 최적화 서비스 ID를 가진 요청 메시지를 전송한다. 요청 메시지는 세션 키를 이용하여 부호화될 수 있다. 모바일 유닛(410(1))이 동일한 목적지 모바일 유닛(410(2))과의 온고잉 흐름(ongoing flow)을 이미 가지고 있는 경우, 소스 모바일 유닛(410(1))은 부호화된 메시지에 새로운 흐름(목적지 IP 어드레스 외에도)에 대한 소스 및 목적지 포트 번호들을 포함한다.

[0037] 이러한 프로토콜 지점에서, 모바일 포워딩 엔티티(420(1))는 목적지 모바일 유닛(410(2))에 고정되는 방문된 네트워크를 잠재적으로 인지하지 못한다. 따라서, 소스 이동성 포워딩 엔티티(420(1))는 목적지 모바일 유닛(410(2))의 IP 어드레스를 가진 로컬 이동성 라우팅 엔티티(425(1))에 보안 요청을 전송할 수 있다. 예시된 실시예에서, 이동성 라우팅 엔티티(425(1))는 방문된 네트워크들의 식별들뿐만 아니라 모바일들의 방문된 위치에 관한 정보를 제공하는 분산형 데이터베이스를 유지한다. 따라서, 이동성 라우팅 엔티티(425(1))는 이동성 포워딩 엔티티(420(2))의 목적지 IP 어드레스를 찾기 위해 목적지 모바일 유닛(410(2))의 IP어드레스를 이용하여 분산형 데이터베이스를 검색할 수 있다. 이동성 라우팅 엔티티(425(1))는 또한, 모바일 유닛(410(2))의 방문된 좌표들(예를 들면, 목적지 이동성 포워딩 엔티티(420(2))의 IP 어드레스)을 획득하기 위해 다른 이동성 라우팅 엔티티(예를 들면425(2))를 접촉할 필요가 있을 수 있다. 이동성 라우팅 엔티티(425(1))는 그 후에, 목적지 이동성 포워딩 엔티티(420(2))의 도메인 네임 또는 아이덴티티뿐만 아니라 목적지 이동성 포워딩 엔티티(420(2))의 IP 어드레스를 리턴할 수 있다.

[0038] 모바일 유닛(410(1))이 서버(도 4에 도시되지 않음)에 의해 제공되는 웹 서비스에 액세스하고 있는 시나리오들에서, 보안 라우트의 하나의 종점은 서버이고, 이것은 연관된 이동성 포워딩 엔티티(420)를 가지지 않을 수 있

다. 모바일 유닛(410(1))과 서버 사이의 통신 경로는 따라서 제 2 이동성 포워딩 엔티티(420)를 포함하지 않을 수 있다. 대신, 이동성 포워딩 엔티티(420(1))는 라우트 최적화 절차에 적합한 종점으로서 서버를 식별하기 위해 서버의 알려진 IP 어드레스 또는 다른 식별자를 이용할 수 있다. 따라서, 이동성 포워딩 엔티티(420(1))는 이동성 라우팅 엔티티(425(1))와 통신할 필요 없이 서버를 식별할 수 있다.

[0039] 목적지 이동성 포워딩 엔티티(420(2))를 식별하는 정보는 미래의 포워딩 판단들을 위해 소스 이동성 포워딩 엔티티(420(1))에 의해 캐싱될 수 있다. 달리 말하면, 이 단계는 소스 이동성 포워딩 엔티티(420(1))가 목적지 이동성 포워딩 엔티티(420(2))의 아이덴티티 및 IP 어드레스를 이미 인지하고 있는 경우에는 실행될 필요가 없을 수 있다. 식별 정보(예를 들면, 목적지 이동성 포워딩 엔티티(420)의 IP 어드레스 및/또는 도메인 네임 또는 아이덴티티)를 캐싱하는 것은 이 정보가 이미 소스 이동성 포워딩 엔티티(420)에 제공된 경우들에서 이 정보가 비교적 신속히 액세스되도록 허용할 수 있다. 결과적으로, 식별 정보를 캐싱하는 것은 레이턴시를 감소시킴으로써 시스템의 성능을 상당히 개선시킬 수 있다. 이동성 라우팅 엔티티(425(1))가 그 데이터베이스에서 목적지 이동성 포워딩 엔티티(420(2))의 IP 어드레스를 찾을 수 없다면, 다른 이동성 라우팅 엔티티들(425(1))과 같이 무선 통신 시스템(400) 내의 다른 엔티티들에 이 정보에 대한 요청들을 전송할 수 있고, 이 정보를 데이터베이스에 이주시키기 위해 이용할 수 있고, 요청된 정보를 리턴할 수 있다.

[0040] 그 후에, 보안 라우트(430)가 소스 및 목적지 이동성 포워딩 엔티티들(420(1-2)) 사이에 확립될 수 있다. 일 실시예에서, 보안 라우트(430)를 셋업하기 위해, 상호 인증된 키 협정이 소스 및 목적지 이동성 포워딩 엔티티들(420(1-2)) 사이에서 협상될 수 있다. 목적지 및 소스 이동성의 여부에 의존하여 상이한 절차들이 뒤따를 수 있다.

[0041] 목적지 및 소스 이동성 포워딩 엔티티들(420(1-2))이 그들 사이에서 활성 세션을 확립하지 못한 시나리오들에서, 소스 이동성 포워딩 엔티티(420(1))는 소스 및 목적지 이동성 포워딩 엔티티들(420(1-2))의 아이덴티티들에 기초하여 목적지 이동성 포워딩 엔티티(420(2))와의 인증된 키 교환 절차를 실행한다. 포워딩 엔티티들은 인증된 키 교환이 인증서들 또는 아이덴티티 기반 암호화(IBE: Identity Based Encryption) 프로토콜들을 이용하여 수행될 수 있는 경우에는 미리 공유된 키를 가지 않을 수 있다. 상호 인증된 키 협정에 기초한 IBE의 이점은 고유한 평이성(PKI 없음)이고 키-조건부 날인 없이 완전한 포워드 보완성을 유지할 수 있다. 일단 이 단계가 실행되면, 소스 이동성 포워딩 엔티티(420(1))는 목적지 이동성 포워딩 엔티티(420(2))에 소스 및 목적지 모바일들(410(1-2))의 IP 어드레스들을 포함하여 부호화된 바인딩 등록을 전송한다. 이 등록은 흐름에 대한 라우트들을 최적화하려는 의도를 목적지 이동성 포워딩 엔티티(420(2))에 효과적으로 통보한다. 응답적으로, 목적지 이동성 포워딩 엔티티(420(2))는 목적지 모바일 유닛(410(2))이 목적지 이동성 포워딩 엔티티(420(2))에 고정되는 경우 바인딩을 확인응답한다. 목적지 이동성 포워딩 엔티티(420(2))는 또한 목적지 모바일 유닛(410(1))이 목적지 이동성 포워딩 엔티티(420(2))에 보안 프록시-기반 라우트 최적화에 대해 등록되었음을 확인응답한다. 바인딩 확인응답을 전송하기 전에, 목적지 이동성 포워딩 엔티티(420(2))는 로컬 이동성 포워딩 엔티티(420(1))를 접촉함으로써 소스 모바일 유닛(410(1))의 위치를 검증하도록 선택적으로 택할 수 있다. 검증 단계는 부당한 MFE가 위조된 흐름을 설정하는 것을 방지할 수 있다.

[0042] 소스 및 목적지 이동성 포워딩 엔티티들(420(1-2))이 활성 세션을 이미 공유하고 있는 시나리오에서, 예를 들면, 이들이 서로 인증했고 잠재적으로 상이한 모바일들 사이의 어떤 다른 호에 대해 동일한 이동성 포워딩 엔티티들(420(1-2)) 사이의 이전 보안 프록시-기반 라우트 최적화 요청으로 인해 세션 키를 가지기 때문이다. 이 시나리오에서, 바인딩 등록 및 바인딩 확인응답들이 실행되지만 인증된 키 협정 단계는 스킵될 수 있다. 소스 및 목적지 모바일 유닛들(410(1-2))이 이미 활성 세션을 공유하는 경우, 소스 이동성 포워딩 엔티티(420(1))는 등록 메시지에 소스 및 목적지 포트들(모바일들의 IP 어드레스들 외에도)을 포함할 수 있다.

[0043] 패킷들은 보안 라우트(430)를 통해 포워딩될 수 있다. 소스 모바일 유닛(410(1))으로부터 수신된 패킷들은 목적지 모바일 유닛(410(2))의 IP 어드레스를 목적지 IP 어드레스로서 포함하고, 따라서, 경로의 임의의 변경은 중간 라우터들이 패킷을 거부하지 않는 것을 보장하기 위해 패킷의 수정을 요구할 것이다. 이것은 터널링, 네트워크 어드레스 변환, 및 라우팅 헤더의 수정을 포함한 다수의 방식들로 달성될 수 있다.

[0044] 터널링은 이동성 포워딩 엔티티들(420(1-2)) 사이에 IP-in-IP(또는 GRE) 터널을 확립함으로써 달성될 수 있다. 유사한 터널링 기술들의 예들은 모바일 IP, GTP 뿐만 아니라 프록시 모바일 IP에 이용되는 터널링 기술들이다. 일 실시예에서, 패킷들의 캡슐화에 앞서 패킷 오버헤드들을 최소화하기 위해 헤더 압축이 이용될 수 있다.

[0045] 네트워크 어드레스 변환 메커니즘들이 또한 구현될 수 있다. 예를 들면, 이동성 포워딩 엔티티들(420(1-2))이 바인딩 등록들 및 확인응답들을 교환할 때 방문된 도메인들에 특정한 모바일 특정 방문된 어드레스들이 교환될

수 있다. 달리 말하면, 두 이동성 포워딩 엔티티들(420(1-2))은 그들 각각의 모바일들에 대한 모바일 특정 공동-배치된 케어-오브 어드레스들을 생성하여 이들을 교환할 수 있다. 일단 이것이 행해지면, 패킷들이 MFE(업스트림 또는 다운스트림)에 모바일에 의해 전송될 때, 모바일들의 IP 어드레스가 그들 대응하는 공동 배치된 케어 오브 어드레스들(care-of addresses)로 대체되는 적합한 네트워크 어드레스 변환들이 이루어진다. 유사하게, MFE가 모바일에 패킷을 전송할 준비를 할 때, 공동-배치된 케어 오브 어드레스들로부터 모바일들의 IP 어드레스(홈 네트워크에 의해 할당된)로의 역변환이 이루어질 것이다. 이러한 절차들은 IPv4 및 IPv6 모바일들 둘다에 적용 가능하고, 주어진 모바일에 대한 공동-배치된 케어-오브 어드레스는 모바일에 알려질 필요가 없다.

[0046] 예를 들면, 소스 및 목적지 모바일 유닛들(410(1)) 둘다가 IPv6 인에이블될 때 라우터 헤더들이 이용될 수 있다. 예를 들면, MFE가 모바일로부터 패킷을 수신할 때, 다른 MFE의 IP 어드레스는 목적지에 도착하기 전에 중간 홉으로서 라우트 헤더에 추가된다.

[0047] 일부 실시예들에서, 이동성 포워딩 엔티티들(420)은 또한, 포워딩 처리 동안 트래픽 흐름들의 암호화 및 헤더 압축과 같은 서비스들을 지원할 수 있다. 예를 들면, 소스 및 목적지 이동성 포워딩 엔티티들(420)은 트래픽 흐름들을 암호화 및 부호화하기 위해 인증된 키 협정 단계 동안 암호화 및 트래픽 인증 키를 도출할 수 있다. 유사한 방식으로, 등록 절차들은 모바일 유닛(410)이 이러한 성능 강화들을 제공하기 위해 네트워크에 위임하도록 허용하고 네트워크는 이러한 서비스들이 모바일에 인가되는지를 검증할 수 있다.

[0048] 이동성 라우팅 엔티티들(MRE)(425)의 각각은 모바일들(410)의 방문된 좌표를 저장하는 데이터베이스를 유지한다. 데이터베이스 좌표는, 각각의 모바일 유닛(410)이 등록되는 이동성 포워딩 엔티티들(420)의 IP 어드레스와 등록된 이동성 포워딩 엔티티(420)의 도메인 네임 또는 아이덴티티를 포함한다. 각각의 모바일 유닛(410)은 따라서 홈 IP 어드레스를 이용하여 어드레싱 가능할 수 있고, 이동성 라우팅 엔티티들(425)은 보안 프록시-기반 라우트 최적화 동작에 관련된 방문된 네트워크의 좌표를 제공할 수 있다. 일 실시예에서, 이동성 라우팅 엔티티(425)는 로컬 데이터베이스들을 구성하고 상이한 위치들에서 유지되는 분산형 데이터베이스로서 구현될 수 있다. 그럼에도 불구하고, 분산형 이동성 라우팅 엔티티(425)는 질의될 때 하나의 단일 통합된 데이터베이스로서 기능할 수 있다. 일반적으로, 이동성 라우팅 엔티티들(425)은 MFE(420)로부터의 질의들에 응답하고, 다른 MRE(425)로부터의 질의들에 응답하고, 이동성 이벤트들이 발생할 때마다 데이터베이스를 업데이트한다.

[0049] 이동성 라우팅 엔티티들(425)은 모바일 유닛들(410)과 연관된 이동성 포워딩 엔티티들(420)을 찾기 위해 데이터베이스를 이용한다. 예를 들면, 이동성 라우팅 엔티티(MRE)(425(1))는 모바일 유닛(410(2))과 연관된 다른 이동성 포워딩 엔티티(420(2))의 아이덴티티 및/또는 위치에 대한 요청을 이동성 포워딩 엔티티(420(1))로부터 수신할 수 있다: MRE(425(1))는 정보가 국부적으로 이용 가능한 경우, 이동성 포워딩 엔티티(420(2))를 나타내는 어드레싱 정보 및/또는 모바일 유닛(410(2))의 방문된 좌표로 대응할 수 있다. 정보가 국부적으로 이용 가능하지 않은 경우, 예를 들면, 모바일 유닛(410(1))이 모바일 유닛(410(3))에 접촉하려고 시도하고 있는 경우, MRE(425(1))는 모바일 유닛(410(3)) 및/또는 이동성 포워딩 엔티티(420(3))의 방문된 좌표를 획득하기 위해 모바일 유닛(410(3))의 홈 네트워크에 있는 다른 MRE(425(2))를 접촉할 수 있다. 그 후에, 이 정보는 MFE(420(1))과 공유될 수 있고, 또한 미래를 위해 캐싱될 수 있다. MRE(425(1))가 '적당한(reasonable)' 시간에 질의를 해결할 수 없는 경우, MFE(420(1))에 다시 '알려지지 않은 좌표(coordinates unknown)' 메시지를 리턴할 수 있다. 이러한 결과는 모바일의 홈 게이트웨이를 통한 '디폴트' 라우트가 방해되지 않기 때문에, 최악이 되지 않을 수 있다.

[0050] 일 실시예에서, MRE(425(1))가 모바일 유닛의 홈 네트워크에 있는 다른 MRE(425(2))를 접촉할 때, MRE(425(2))의 IP 어드레스(또는 도메인 네임)는 MRE(425(1))에 의해 알려지지 않을 수 있다. 예를 들면, MRE들(425)은 모바일 호스트의 오퍼레이터가 접촉하는 MRE의 오퍼레이터와 상이할 때 서로의 IP 어드레스들 또는 도메인 네임들을 알지 못할 수도 있다. 이 문제는 2 단계 처리에 의해 해결될 수 있다. 먼저, 로컬 MRE(425(1))는, 로컬 MRE(425(1))와 동일한 오퍼레이터에 의해 유지되어 MFE(420(1))로부터 수신된 요청을 전송하는 그 자신의 홈 MRE에 도착한다. 정보가 국부적으로 이용 가능한 경우, 그것은 로컬 MRE(425(1))에 넘겨진다. 그렇지 않은 경우, '홈 MRE'는 모바일의 '홈 MRE'(관련 오퍼레이터의 도메인에)에 도착하고 모바일의 방문된 좌표를 획득한다. 상기 실시예에는 2개의 기초를 이루는 가정들이 존재한다. 첫째, 홈 네트워크의 MRE는 로컬 데이터베이스에 이를 유지하기 위해 홈 게이트웨이와 동작하는 것이 가정될 수 있다. 둘째, 각각의 오퍼레이터는 하나 이상의 MRE들을 '홈 MRE들'로 표시할 수 있고, 또한 이들 요소들은 다른 오퍼레이터 네트워크들에서 다양한 '홈 MRE들'의 좌표를 유지한다. 달리 말하면, MRE들은 오퍼레이터 경계들에 걸쳐 동작하는 계층적인 분산형 데이터베이스로 구성될 수 있다. 이것은 방문된 네트워크 당 하나의 로컬 MRE 및 홈 게이트웨이 당 하나의 '홈 MRE'를 가짐으로써 쉽게 달성될 수 있다. 부가의 MRE들은 국부적으로 추가될 수 있거나 리던던시를 목적으로 추가될 수

있다. 또한 방문된 네트워크들은 그들 네트워크들에 부착된 모바일들의 좌표를 가진 로컬 MRE들과 정보를 공유할 수 있다. 초기에 관찰된 바와 같이, 이러한 질의 처리를 이용하여 획득된 정보는 관련된 MRE들 중 하나씩 나중 이용을 위해 캐싱될 수 있다. 일 실시예에서, 캐싱된 정보와 연관된 만료 시간이 존재할 수 있다.

[0051] 모바일 유닛들(410)은 무선 통신 시스템(400) 전반을 계속 로밍할 수 있고, 그래서 무선 통신 시스템(400)은 매크로-이동성 기능을 지원할 수 있다. 일 실시예에서, 모바일 유닛(410)이 하나의 방문된 게이트웨이에서 다른 게이트웨이로 스위칭할 때, 모바일 유닛(410)의 홈 게이트웨이가 통보된다. 예를 들면, 최근에 생겨난 네트워크들에서, 타겟 방문된 게이트웨이와 홈 게이트웨이 사이의 프록시 모바일 IP 바인딩 업데이트 및 확인응답은 매크로-이동성을 지원하기 위해 이용될 수 있다. 업데이트/확인응답의 경우에, 수반된 방문된 게이트웨이들은 대응하는 로컬 MRE 데이터베이스를 업데이트할 수 있고 홈 게이트웨이는 홈 MRE를 업데이트할 수 있다. 데이터베이스 업데이트의 속성(즉, 이벤트 기반 푸시(push) 또는 주기적인 풀(pull))은 설계적인 선택사항의 문제이다.

[0052] MFE(420)가 MRE(425)로부터 정보를 요청할 때, MRE(425)에 캐싱된 정보는 잠재적으로 진부해질 수 있고, MRE(425)는 캐싱된 정보가 진부해졌는지를 인지하지 못할 수 있다. MFE(420)가 진부한 정보를 이용하고 모바일 유닛(410)의 방문된 네트워크를 접촉할 때, 정보가 진부하다는 것이 명확해질 수 있다. 이러한 환경들 하에서, 소스 FME(420)는 이전 질의에서 수신된 정보가 진부하다는 부가의 표시를 하여 MRE(425)에게 다시 질의할 수 있다. MRE(425)는 모바일 유닛(410)의 좌표를 획득하기 위해, (이전에 논의된 바와 같이) 모바일 유닛(410)의 방문된 좌표를 획득하기 위해, 캐싱된 엔트리를 삭제하고 모바일 유닛(410)의 홈 네트워크의 MRE(425)로 돌아갈 수 있다. 이 이벤트가 발생할 때, '호(call)'가 디폴트 라우트들을 통해 모바일 유닛들(410) 사이에 계속된다. 후속적으로, 최적의 라우트가 확인되고 셋업되었으면, 최적의 경로들을 따른 패킷들의 포워딩이 발생할 수 있다.

[0053] 무선 통신 시스템(400)은 보안 프록시-기반 라우트 최적화를 지원하기 위한 다양한 보안 원리들을 구현할 수 있다. 일 실시예에서 네트워크 기반 라우트 최적화가 인가된 흐름들에 대해서만 지원될 수 있다. 이것은 네트워크 집행 오퍼레이터 정책들에 의해 렌더링된 서비스들을 보장하려는 것이며 (인가되지 않은) 상대방들에는 이용 가능하지 않다. 또한, 주어진 모바일 유닛(410)에 대한 흐름이 보안 프록시-기반 라우트 최적화에 의해 제공된 성능 강화들을 수신하도록 인가될 때, 모바일 유닛(410)은, 네트워크가 모바일 유닛(410)과 연관된 흐름들에 대해 보안 프록시-기반 라우트 최적화를 수행할 수 있기 전에 필요시(예를 들면, 캡슐화 또는 네트워크 어드레스 변환 등) 패킷들을 수정하기 위한 책임을 네트워크에 위임하게 될 수 있다. 네트워크 및 모바일 유닛(410)은 특권들을 확립하고 책임들을 위임하기 위해 기존의 링크층 인증 메커니즘들에 대해, 가능하다면, 피기백할 수 있다. 라우트 최적화에 수반된 네트워크 요소들은 또한 정보 교환 및 이벤트들을 시그널링하는 것에 앞서 보안성 연관들을 공유하거나 확립할 수 있다. 이것은 세션들이 인가되지 않은 상대방들에 의해 악용될 수 있을 가능성을 감소시키려는 것이다. 다양한 보안 요건들은 세션 셋업 뿐만 아니라 업데이트들 제공 및 정보를 획득하기 위해 데이터베이스와의 통신들을 위해 집행될 수 있다.

[0054] 무선 통신 시스템(400)에서 구현될 수 있는 보안성 아키텍처의 예시적인 일 실시예에서, 모바일 유닛들(410)은 표준들에서 기존의 프로토콜들을 이용하여 액세스 네트워크와 자체 인증할 수 있다. 따라서 인증 및 키 협정 방법은 표준들이 특정될 수 있다. 성공적인 인증 다음에, 모바일 유닛(410) 및 인증 센터(도 4에 도시되지 않음)는 보안 프록시-기반 라우트 최적화에 이용되는 부가 키를 도출할 수 있다. 부가 키는 기존의 키 도출 처리들을 수정함으로써 모바일 유닛들(410)에 의해 도출될 수 있다. 네트워크의 인증 센터는 동일한 키를 동시에 도출할 수 있고 방문된 네트워크에 이를 전달할 수 있다. 예를 들면, WiMAX 및 UMB 기반 네트워크들에서, 액세스 인증은 다양한 EAP 방법들에 기초한다. 더욱 최근에, EAP-AKA'는 마찬가지로 진화된 HRPD 시스템들에 대한 액세스 인증 프로토콜로서 채택되었다. EAP 인증 프로토콜은 2개의 키들 - MSK 및 EMSK의 생성을 허용한다. MSK는 액세스 네트워크에 전달되지만, EMSK는 미래의 사용을 위해 AAA에서 유지된다. 일 실시예에서, 보안 프록시-기반 라우트 최적화 키는 EMSK로부터 도출될 수 있다. 보안 프록시-기반 라우트 최적화 키는 그 후에 방문된 네트워크의 MFE로 이전될 수 있고, 프로토콜의 등록 단계에서 이용될 수 있다. 다른 예로서, 3GPP 기반 HSPA 및 LTE 네트워크들에서, 액세스 인증은 모바일 유닛들(410)의 SIM 카드가 세션 키들의 세트를 도출한 AKA에 기초한다. HSPA 시스템들에 대해, 네트워크들에서, AKA는, 서빙 GPRS 지원 노드(SGSN)라고 불리는 방문된 게이트웨이로 이전되는 세션 키들을 포함하는 벡터를 이용한다. LTE 시스템들에 대해, 네트워크에서, AKA는 이동성 관리 엔티티(MME)로 이전되는 세션 키들을 포함하는 벡터를 이용한다. 보안 프록시-기반 라우트 최적화 키는 도출되어 무선 통신 시스템(400) 내의 적합한 엔티티들로 이전되는 부가 키일 수 있다. 예를 들면, MME는 그 후에 보안 프록시-기반 라우트 최적화 키를 MFE(420)로 이전할 수 있다.

[0055] 키들(보안 프록시-기반 라우트 최적화 키)의 이전을 수반하는 트랜잭션들은 미리 구성된 보안 세션들에 기초하

여 보안 터널들을 통해 수행되어야 한다. MRE(425)와의 통신들, 특히 이동성 이벤트들로 인한 데이터베이스 업데이트들도 또한 보안 터널들을 통해야 한다. 이것은 데이터베이스들이 상대방들에 의해 오류 정보로 오류가 생기지 않는 것을 보장하는 것이 중요하다; 이것은 파국적으로 고장날 수 있는 '라우트 포이즈닝(route poisoning)'이라고 불리는 서비스 거부 공격들(DoS)을 유발할 수 있다. 소스 MFE와 목적지 MFE 사이의 보안성 연관들은 인증된 키 협정 프로토콜들에 기초할 수 있다. 일 실시예는 IKE와 유사한 증명서들 및 후속 키 교환의 이용을 구현한다. 대안적인 일 실시예는 식별 기반 암호화(IBE: Identity Based Encryption) 프로토콜들의 이용이다. 상호 인증된 키 교환에 기초한 IBE의 이점은 고유한 평이성(PKI 없음)이고 키-조건부 날인 없이 완전한 포워드 보안성(secrecy)을 유지할 수 있다.

[0056] 무선 통신 시스템(400)에서 구현된 보안 프록시-기반 라우트 최적화 기술들은 기존 네트워크들에서 구현되고 및/또는 이와 통합될 수 있다. 본 명세서에 기술된 보안 프록시-기반 라우트 최적화 기술들의 실시예들은 IPv4 및 IPv6 흐름들 둘다에 적용 가능하고 액세스 네트워크 아키텍처 및 프로토콜들과 무관한 임의의 모바일 네트워크에 적용 가능할 수 있다. 예를 들면, 로컬 MRE들(425)와 MFE들(420) 사이의 일 대 일 대응이 존재할 수 있고, 일부 실시예들에서, 도 3에 도시된 방문된 게이트웨이들(325)과 같은 방문된 게이트웨이마다 하나의 MFE(420)가 존재할 수 있다. 일 실시예에서, 도 3에 도시된 홈 게이트웨이들(330)과 같은 홈 게이트웨이마다 하나의 홈 MRE(425)가 존재할 수 있다. HRPD 네트워크들에 대해, MFE(420)는 PDSN에 통합될 수 있고, 로컬 MRE(425)가 로컬 AAA 상에 개별 데이터베이스로서 유지될 수 있다. 홈 MRE들(425)은 기존의 홈 AAA 서버들에 추가될 수 있다. HSPA 네트워크들에 대해, 로컬 MRE 및 MFE가 SGSN에 통합될 수 있고, 홈 MRE는 복합 HSS에 통합될 수 있다. WiMAX 네트워크들에 대해, MFE는 ASN 게이트웨이에 통합될 수 있고, MRE는 로컬 AAA 상의 개별 데이터베이스로서 유지될 수 있다. 홈 MRE는 기존의 홈 AAA 서버들에 추가될 수 있다. UMB/CAN 네트워크들에 대해, MFE는 AGW에 추가될 수 있고 MRE는 로컬 AAA에 추가될 수 있다. HRPD, HSPA, WiMAX, 및 UMB/CAN 네트워크들에 대해, MRE(425) 및 MFE(420)는 다이어미터 인터페이스로서 구현될 수 있고, MRE간 인터페이스들도 또한 다이어미터 인터페이스들로서 구현될 수 있다. LTE/SAE 기반 EPS 네트워크들에 대해, 로컬 MRE는 MME에 추가될 수 있고 MFE는 서빙 SAE 게이트웨이에 추가될 수 있다. 홈 MRE 서버는 3GPP-AAA 서버 또는 HSS에 통합될 수 있다.

[0057] 상기 인터페이스들 외에도, 증명서들이 활용되는 경우, MFE들(420)은 증명서들의 권한 설정, 허가 취소 및 업데이트들에 대한 인증 기관들과 인터페이싱할 수 있다. IBE 기반 인증된 키 협정이 이용되는 경우, 키 생성 기능(KGF)에 대한 인터페이스들이 제공될 수 있다. 프로토콜 논의들이 통상적으로 모바일-대-모바일 애플리케이션들에 대해 집중되었지만, 보안 프록시-기반 라우트 최적화도 역시 모바일-대-인터넷 애플리케이션들에서 구현될 수 있다. 또한, 모바일-대-인터넷 애플리케이션들은 네트워크 어드레스 변환 후 로컬 인터넷 POP에 대한 트래픽을 오프로딩한 방문된 MFE로 최적화하기가 더욱 용이할 수 있다. 인터넷으로부터의 패킷들은 방문된 MFE에 의해 할당된 IP 어드레스가 방문된 게이트웨이에 의해 관리된 라우팅 도메인에 대응하기 때문에, 방문된 MRE를 통해 라우팅될 수 있다.

[0058] 도 5는 보안 프록시-기반 라우트 최적화(SPRO)의 방법(500)의 일 실시예를 개념적으로 도시한다. 예시된 실시예에서, 모바일 노드(MN)는 소스 이동성 포워딩 엔티티(S-MFE)로부터 SPRO(및 잠재적으로 다른 서비스들도 마찬가지로)에 대한 광고를 요청한다(505에서). S-MFE는 제공된 SPRO 서비스들을 광고하고(510에서), 예시된 실시예에서, S-MFE는 또한 등록 및 위임을 위해 논스들을 광고할 수 있다(510에서). 또한, S-MFE는, MN에 제공된 다른 서비스들 및/또는 성능 강화들을 광고할 수 있다(510에서). MN은 S-MFE에 바인딩 등록을 전송한다(515). MN으로부터의 바인딩 등록은 SPRO 서비스 식별자(ID)를 포함할 수 있다. MN은 마찬가지로 부가 서비스들을 고르도록 선택할 수 있다. S-MFE는 모바일이 후속 통신을 위해 이용될 수 있는 논스들을 포함할 수 있는 바인딩 확인응답을 전송한다(520에서). 방법(500)에서 화살표(520) 아래에 점선으로 표시된 이 지점에서, MN은 S-MFE에 등록될 수 있다.

[0059] 방법(500)의 다음 단계는 타겟 이동성 포워딩 엔티티(T-MFE)의 발견을 포함한다. MN은 수신된 논스를 선택하고(520에서), SPRO 서비스를 위해 네트워크와 협상된 세션 키를 이용하여 부호화된 SPRO 서비스 ID 및 목적지 대응 모바일(CN)의 IP 어드레스와 함께 요청 메시지를 S-MFE에 전송한다(525에서). S-MFE가, 목적지 모바일이 현재 고정되는 방문된 네트워크를 알 수 없기 때문에, S-MFE는 목적지 모바일(CN)의 IP 어드레스를 가진 로컬 MRE에 보안 요청을 전송한다(530에서). MRE는 적합한 데이터베이스를 이용하여 T-MFE의 발견을 수행하고(533에서) T-MFE의 도메인 네임 또는 아이덴티티뿐만 아니라 T-MFE의 IP 어드레스를 리턴한다(535에서). 방법(500)에서 화살표(535) 아래에 점선으로 표시된 이 지점에서, T-MFE은 S-MFE 및 MRE에 의해 발견되었다. 본 명세서에 논의된 바와 같이, MN이 서버에 의해 제공되는 서비스에 액세스하는 실시예들에서(도 5에 도시되지 않음), 보안 라우트의 다른 종점은 이동성 포워딩 엔티티가 아닌 서버일 수 있다. 방법(500)의 일부 실시예들은 따라서 서버를 식

별하거나 "발견"하기 위해 IP 어드레스 또는 다른 식별자를 이용하도록 수정될 수 있다.

[0060] S-MFE는 그들 아이덴티티들에 기초하여 T-MFE와 인증된 키 교환 절차를 실행한다(540에서). 예를 들면, 인증은 IBE 인증 방식을 이용하여 수행될 수 있다(540에서). 인증시, S-MFE는 소스 및 목적지 모바일들의 IP 어드레스들을 포함하는 부호화된 바인딩 등록을 T-MFE에 전송한다(545에서). 바인딩 확인응답을 전송하기에 앞서, T-MFE는 로컬 MRE를 접촉함으로써(550에서) 소스 모바일의 위치를 검증하기 위하여 선택적으로 택할 수 있다. 검증시, T-MFE는 바인딩을 확인응답하고(555에서)(목적지 모바일이 실제로 타겟 MFE에 고정되는 경우), 그 목적지 모바일은 타겟 MFE에 SPRO에 대해 등록된다. 방법(500)에서 화살표(555) 아래에 점선으로 표시된 이 지점에서, T-MFE 및 S-MFE는, MN/CN 또는 다른 통신 노드들 사이의 현재 세션 또는 다른 미래 세션들과 연관된 패킷들을 포워딩하기 위해 이용될 수 있는 보안 라우트 또는 터널을 공유한다.

[0061] 소스 및 목적지 모바일 사이에서 패킷들이 포워딩된다(560에서). 예를 들면, 패킷들은 T-MFE와 S-MFE 사이의 보안 IP-in-IP 터널을 이용하여 포워딩될 수 있다(555에서). 그러나 본 개시내용의 이점을 가진 본 기술분야의 통상의 기술자들은 대안적인 보안 라우팅 및/또는 터널링 기술들이 이용될 수 있음을 알아야 한다.

[0062] 개시된 요지의 부분들 및 대응하는 상세한 기술은 소프트웨어, 또는 알고리즘들 및 컴퓨터 메모리 내의 데이터 비트들에 대한 동작들의 기호 표현들의 형태로 제공된다. 이들 기술들 및 표현들은 본 기술분야의 통상의 기술자들이 본 기술분야의 다른 통상의 기술자들에게 그들 작업 내용을 효과적으로 전달하는 것들이다. 알고리즘은, 이 용어가 본 명세서에 이용되는 바와 같이, 그리고 일반적으로 이용되는 바와 같이, 원하는 결과를 유발하는 단계들의 일관성 있는 시퀀스인 것으로 생각된다. 단계들은 물리적인 양들의 물리적인 조작들을 요구하는 것들이다. 일반적으로, 필수적인 것은 아니지만, 이들 양들은 저장, 이전, 조합, 비교, 그렇지 않으면 조작될 수 있는 광, 전기 또는 자기 신호들의 형태를 취한다. 이들 신호들을 비트들, 값들, 원소들, 기호들, 글자들, 단어들, 숫자들 등으로 나타내는 것이 주로 공용 사용의 이유로 편리한 것으로 판명되었다.

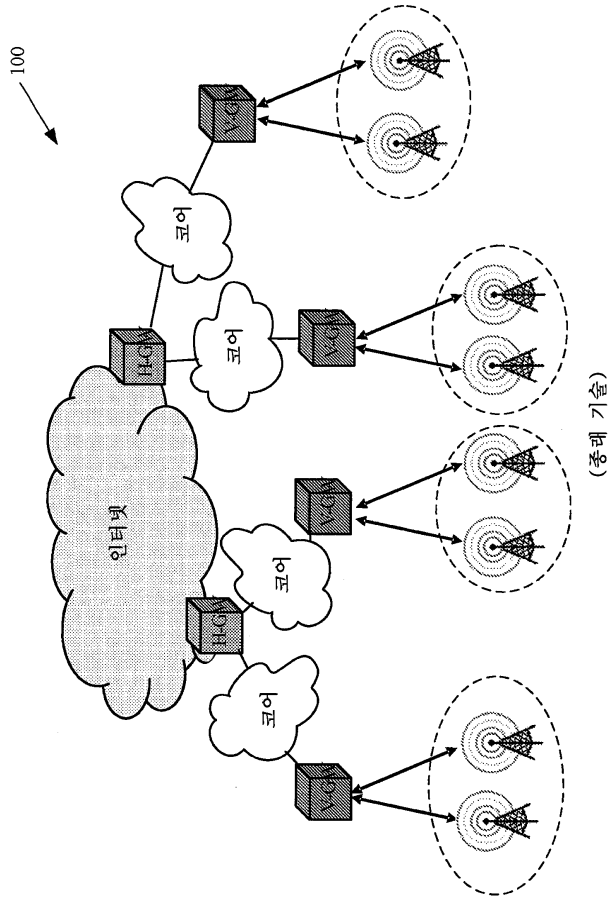
[0063] 그러나, 이들 및 유사한 단어들 모두는 적절한 물리적인 양들과 연관되기 위한 것이고 이들 양들에 적용되는 편리한 라벨들일 뿐임을 유념해야 한다. 달리 특별히 언급되지 않거나 논의로부터 명확하지 않으면, "처리(processing)" 또는 "컴퓨팅(computing)" 또는 "계산(calculating)" 또는 "결정(determining)" 또는 "디스플레이(displaying)" 등과 같은 단어들은 컴퓨터 시스템 또는 유사한 전자 컴퓨팅 디바이스의 동작 및 처리들을 의미하며, 이것은 컴퓨터 시스템의 레지스터들 및 메모리들 내의 물리적, 전자적인 양들로서 표현되는 데이터를 컴퓨터 시스템 메모리들 또는 레지스터들 또는 기타 정보 저장장치, 전송 또는 디스플레이 디바이스들 내의 물리적인 양들로서 유사하게 표현된 다른 데이터로 조작 및 변환한다.

[0064] 개시된 요지의 소프트웨어 구현된 양태들은 통상적으로 어떤 형태의 전송 매체를 통해 구현되거나 어떤 형태의 프로그램 저장 매체 상에서 인코딩됨을 유념한다. 프로그램 저장 매체는 자기(예를 들면, 플로피 디스크 또는 하드드라이브) 또는 광(예를 들면, 컴팩트 디스크 판독 전용 메모리 또는 "CD ROM")일 수 있고, 판독 전용 또는 랜덤 액세스일 수 있다. 유사하게, 전송 매체는 연선들, 동축 케이블, 광 섬유 또는 본 기술분야에 알려진 어떤 다른 적절한 전송 매체일 수 있다. 개시된 요지는 임의의 주어진 구현의 양태들에 의해 제한되지 않는다.

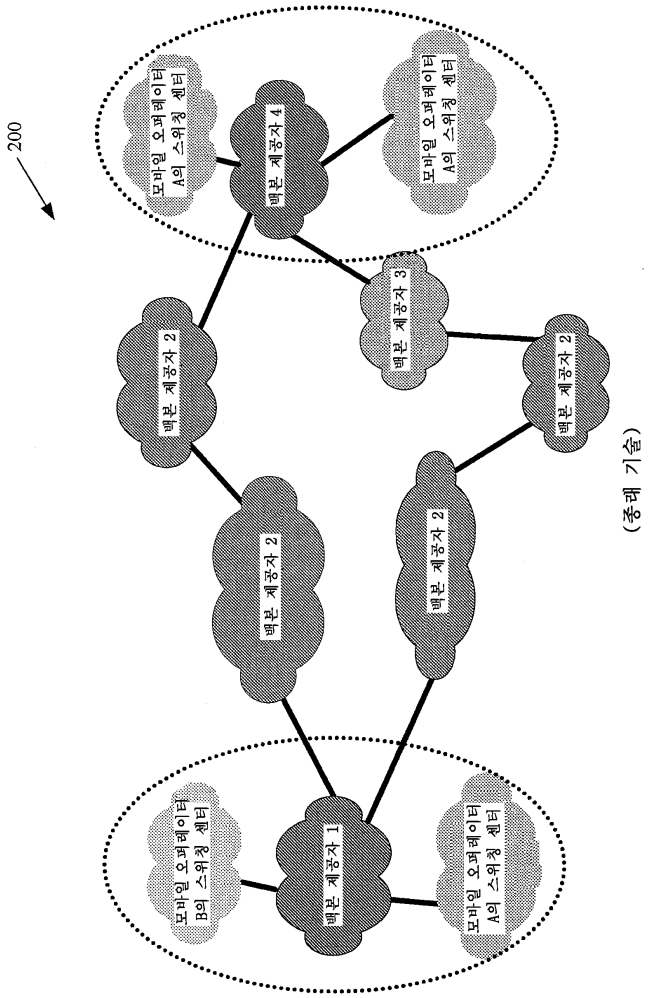
[0065] 상기에 개시된 특정 실시예들은, 개시된 요지가 본 명세서의 개시내용들의 이점을 가진 본 기술분야의 통상의 기술자들에 명백한 상이하지만 등가의 방식으로 수정되고 실시될 수 있으므로, 단지 예시적이다. 또한, 하기의 특허청구범위들에 기술된 것들 이외에 본 명세서에 도시된 구성 또는 설계의 세부사항들에 제한하려는 의도가 없다. 따라서, 상기 개시된 특정 실시예는 변경되거나 수정될 수 있고, 모든 이러한 변형들은 개시된 요지의 범주 내에 있는 것으로 간주되는 것이 명백하다. 따라서, 본 명세서에서 추구하는 보호범위는 하기의 특허청구범위에 기재된 바와 같다.

도면

도면1

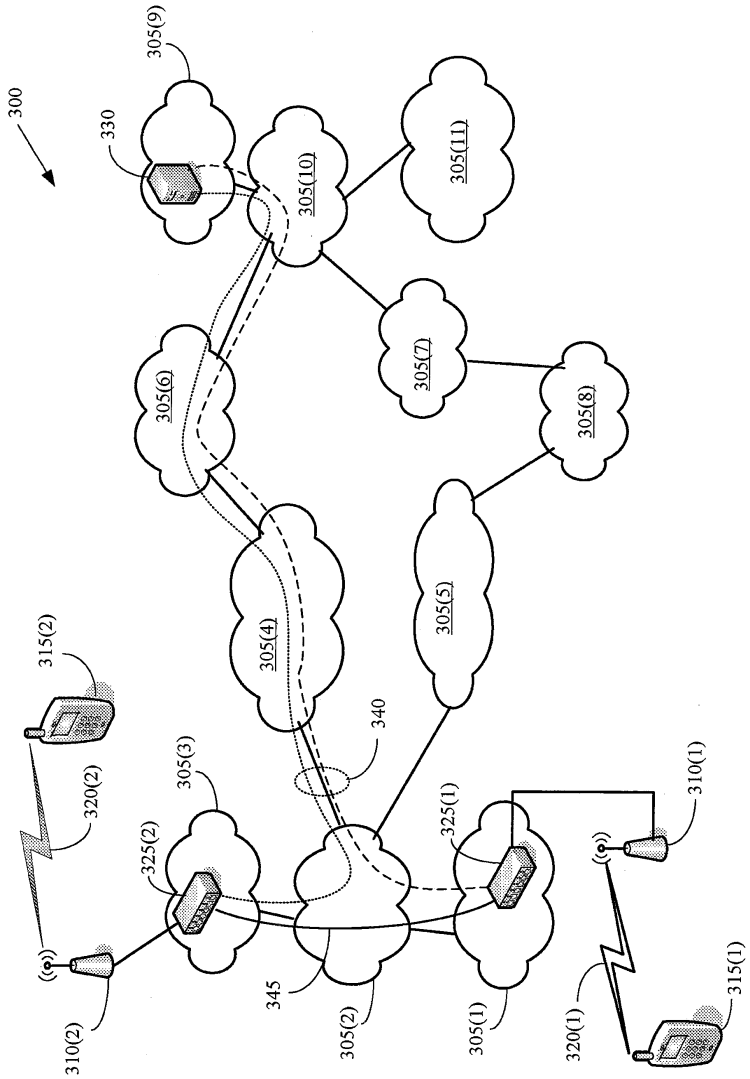


도면2

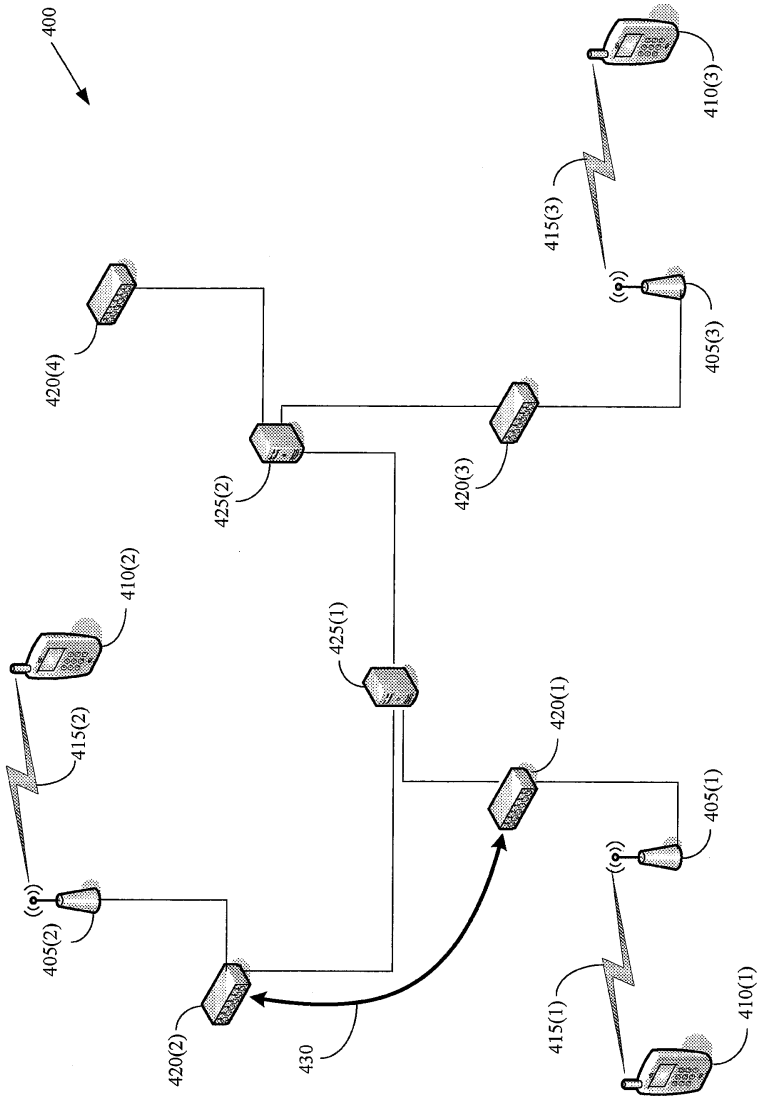

200
모바일 오퍼레이터 A의 스위칭 센터
백본 제공자 4
모바일 오퍼레이터 A의 스위칭 센터
백본 제공자 3
백본 제공자 2
백본 제공자 2
백본 제공자 2
백본 제공자 2
모바일 오퍼레이터 B의 스위칭 센터
백본 제공자 1
모바일 오퍼레이터 A의 스위칭 센터

(종래 기술)

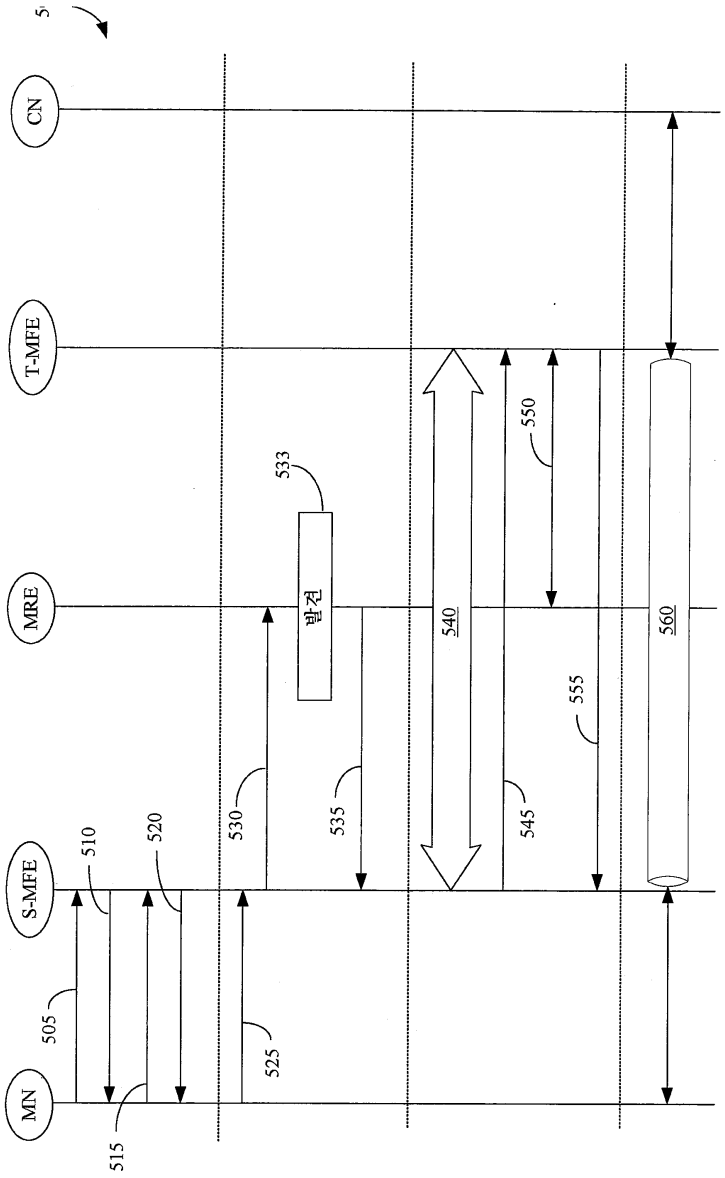
도면3


300
305(9)
330
305(10)
305(11)
305(6)
305(7)
305(8)
305(4)
305(5)
340
315(2)
320(2)
305(3)
325(2)
325(1)
310(1)
345
305(2)
305(1)
320(1)
315(1)
310(2)

도면4


400
410(3)
415(3)
405(3)
420(4)
420(3)
425(2)
410(2)
425(1)
415(2)
420(1)
405(1)
405(2)
415(1)
410(1)
420(2)
430

도면5


CN
T-MFE
MRE
S-MFE
MN
발견
505
510
515
520
525
530
533
535
540
545
550
555
560