(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년03월27일
(11) 등록번호 10-2094216
(24) 등록일자 2020년03월23일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2009.01) *H04W 12/08* (2009.01)
(21) 출원번호 10-2013-0133171
(22) 출원일자 2013년11월04일
심사청구일자 2018년11월05일
(65) 공개번호 10-2015-0051568
(43) 공개일자 2015년05월13일
(56) 선행기술조사문헌
WO2013095001 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자 주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
서경주
서울 강남구 영동대로114길 56, 101동 1102호 (삼성동, 삼성래미안아파트)
(74) 대리인
윤동열

전체 청구항 수 : 총 12 항 심사관 : 이준석

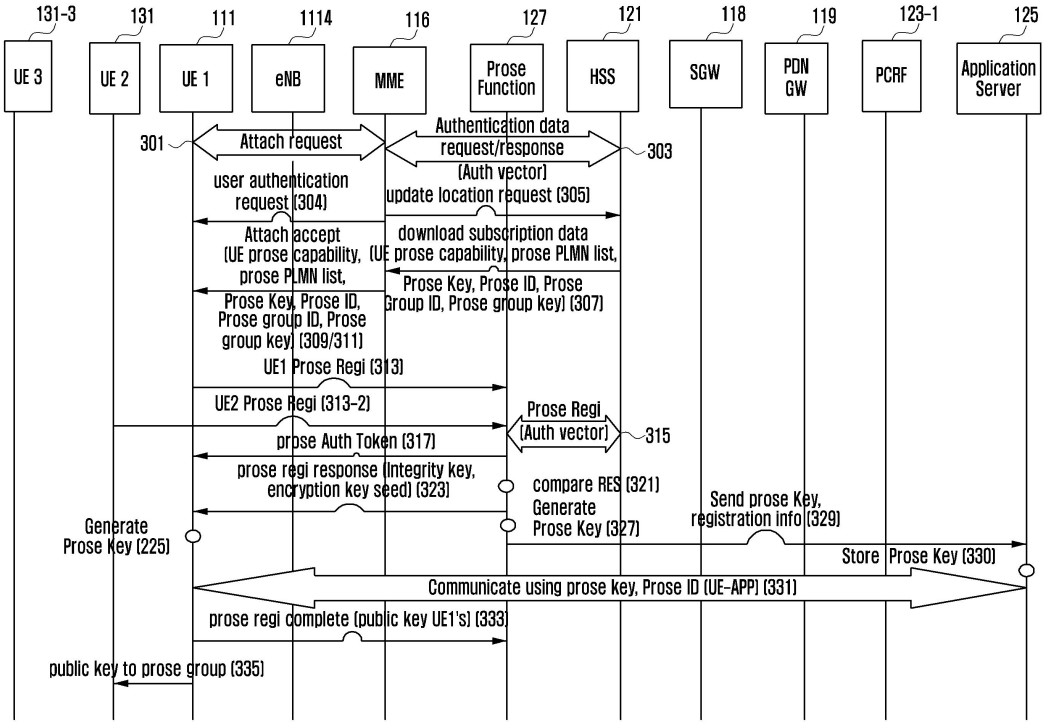
(54) 발명의 명칭 **이동 통신 시스템 환경에서 프락시미티 기반 서비스 단말 간 발견 및 통신을 지원하기 위한 보안 방안 및 시스템**

(57) 요 약

본 발명은 이동통신 네트워크에서 프락시미티 기반 서비스 (Proximity based services : 이하 Prose 로 표기), prose discovery, prose communication, 기기 간 통신 (divice to device : 이하 D2D 로 표기) 을 함에 있어서, 기기 간 통신을 위한 기기간 발견, 기기간 통신시 관련된 보안 방안에 대한 것으로서, 본 발명을 통하여, 통신을

(뒷면에 계속)

대 표 도



수행하는 기기 (device)는 prose discovery, prose communication 을 위한 보안 방법을 수행할 수 있다.

한편, 단말 (UE) 이 서로 간 다른 단말을 발견하고, 단말간 통신을 수행함에 있어서 인증하고, 보안 관련 정보를 수신하고 검증함으로써 안전한 통신을 수행할 수 있다. 이러한 인증과 조정(control)등은 단말(UE) 이 하거나 혹은 기지국(eNB) 의 도움을 받는 방법 등의 다양한 실시 예가 가능할 것이다.

따라서 본 발명을 통해 EUTRAN (Evolved Universal Terrestrial Radio Access Network : 이하 EUTRAN 표기) 혹은 UTRAN (Universal Terrestrial Radio Access Network : 이하 UTRAN 표기) / GERAN (GSM/EDGE Radio Access Network : 이하 GERAN 으로 표기) 등과 같은 환경하에서 단말 (device)이 단말간 혹은 네트웍의 도움을 받아 서로간 정보를 제공하거나 받을 수 있고, 보안키 관련 정보를 수신하거나, 이러한 보안키를 이용하여 보안 절차를 수행함으로써, 통신의 효율성 및 보안성이 강화되는 이점이 있다.

명 세 서

청구범위

청구항 1

이동 통신 시스템에서 제1 단말의 ProSe(proximity based service) 통신 방법에 있어서,

제1 단말의 공개 키를 ProSe 그룹의 적어도 하나의 단말로 브로드캐스트하는 단계;

제2 단말로부터 상기 ProSe 통신과 관련된 지시자를 포함하는 페이징 메시지를 수신하는 단계;

상기 제2 단말로부터 ProSe 통신 요청을 수신하는 단계;

상기 공개 키에 기반하여 암호화된 인증 정보를 포함하는 제1 메시지를 상기 제2 단말로 전송하는 단계;

상기 제2 단말로부터 제2 메시지를 수신하는 단계;

상기 인증 정보 및 상기 제2 메시지에 기반하여 상기 제1 단말이 상기 ProSe 통신 요청을 위한 타겟 단말인지를 판단하는 단계;

상기 인증 정보가 상기 제2 메시지에 포함되어 있으면, ProSe 통신 응답 메시지를 상기 제2 단말에게 전송하는 단계; 및

상기 제2 단말과 상기 ProSe 통신을 수행하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 인증 정보는 난수 또는 타임 스탬프 중 적어도 하나를 포함하는 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서,

상기 공개 키를 위한 등록 요청 메시지를 ProSe 기능 노드로 전송하는 단계; 및

상기 ProSe 기능 노드로부터 상기 공개 키를 수신하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 4

이동 통신 시스템에서 ProSe(proximity based service) 통신을 위한 제1 단말에 있어서,

송수신부; 및

상기 송수신부와 연결되고, 제1 단말의 공개 키를 ProSe 그룹의 적어도 하나의 단말로 브로드캐스트하며, 제2 단말로부터 상기 ProSe 통신과 관련된 지시자를 포함하는 페이징 메시지를 수신하고, 상기 제2 단말로부터 ProSe 통신 요청을 수신하며, 상기 공개 키에 기반하여 암호화된 인증 정보를 포함하는 제1 메시지를 상기 제2 단말로 전송하고, 상기 제2 단말로부터 제2 메시지를 수신하며, 상기 인증 정보 및 상기 제2 메시지에 기반하여 상기 제1 단말이 상기 ProSe 통신 요청을 위한 타겟 단말인지를 판단하고, 상기 인증 정보가 상기 제2 메시지에 포함되어 있으면, ProSe 통신 응답 메시지를 상기 제2 단말에게 전송하며, 상기 제2 단말과 상기 ProSe 통신을 수행하도록 제어하는 제어부를 포함하는 제1 단말.

청구항 5

제4항에 있어서, 상기 인증 정보는 난수 또는 타임 스탬프 중 적어도 하나를 포함하는 것을 특징으로 하는 제1 단말.

청구항 6

제4항에 있어서, 상기 제어부는,

상기 공개 키를 위한 등록 요청 메시지를 ProSe 기능 노드로 전송하고, 상기 ProSe 기능 노드로부터 상기 공개 키를 수신하도록 제어하는 것을 특징으로 하는 제1 단말.

청구항 7

이동 통신 시스템에서 제2 단말의 ProSe(proximity based service) 통신 방법에 있어서,

제1 단말로부터 상기 제1 단말의 공개 키를 수신하는 단계;

상기 제1 단말에게 상기 ProSe 통신과 관련된 지시자를 포함하는 페이징 메시지를 전송하는 단계;

상기 제1 단말에게 ProSe 통신 요청을 전송하는 단계;

상기 제1 단말로부터 상기 공개 키에 기반하여 암호화된 인증 정보를 포함하는 제1 메시지를 수신하는 단계;

상기 제1 단말에게 제2 메시지를 전송하는 단계;

상기 인증 정보가 상기 제2 메시지에 포함되어 있으면, 상기 제1 단말로부터 ProSe 통신 응답 메시지를 수신하는 단계; 및

상기 제1 단말과 상기 ProSe 통신을 수행하는 단계를 포함하는 방법.

청구항 8

제7항에 있어서, 상기 인증 정보는 난수 또는 타임 스탬프 중 적어도 하나를 포함하는 것을 특징으로 하는 방법.

청구항 9

제7항에 있어서,

상기 공개 키를 위한 등록 요청 메시지를 ProSe 기능 노드로 전송하는 단계; 및

상기 ProSe 기능 노드로부터 상기 공개 키를 수신하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 10

이동 통신 시스템에서 ProSe(proximity based service) 통신을 위한 제2 단말에 있어서,

송수신부; 및

상기 송수신부와 연결되고, 제1 단말로부터 상기 제1 단말의 공개 키를 수신하며, 상기 제1 단말에게 상기 ProSe 통신과 관련된 지시자를 포함하는 페이징 메시지를 전송하고, 상기 제1 단말에게 ProSe 통신 요청을 전송하며, 상기 제1 단말로부터 상기 공개 키에 기반하여 암호화된 인증 정보를 포함하는 제1 메시지를 수신하고, 상기 제1 단말에게 제2 메시지를 전송하며, 상기 인증 정보가 상기 제2 메시지에 포함되어 있으면, 상기 제1 단말로부터 ProSe 통신 응답 메시지를 수신하고, 상기 제1 단말과 상기 ProSe 통신을 수행하도록 제어하는 제어부를 포함하는 제2 단말.

청구항 11

제10항에 있어서, 상기 인증 정보는 난수 또는 타임 스탬프 중 적어도 하나를 포함하는 것을 특징으로 하는 제2 단말.

청구항 12

제10항에 있어서, 상기 제어부는,

상기 공개 키를 위한 등록 요청 메시지를 ProSe 기능 노드로 전송하고, 상기 ProSe 기능 노드로부터 상기 공개 키를 수신하도록 제어하는 것을 특징으로 하는 제2 단말.

발명의 설명

기 술 분 야

[0001] 본 발명은 3GPP EPS 를 비롯한 진화된 이동 통신 시스템에 있어서 기기 간 통신을 가능하도록 하는 방안 및 기기 간 통신에 있어서 보안을 설정 관리하는 방안에 관한 것이다.

배 경 기 술

[0002] 본 발명은 기기 (device) 에 통신 기능이 수행 가능하도록 하는 시스템에 대한 것으로서, 이때 기기(device) 는 종래의 이동 통신 단말이나 machine type communication 을 수행하는 기기, Consumer Devices, 등 다양한 기기가 포함될 수 있다.

[0003] 본 발명은 이러한 기기간 통신을 수행하도록 함에 있어 proximity based service 즉 prose discovery 및 prose communication에 대한 것으로, 특히 proximity based service, 단말간 통신이 가능하도록 관련 정보, 보안 설정 등이 가능하도록 하는 방안을 적용하여, 보안상 안전한 통신 수행이 가능하도록 하는 방법 및 시스템에 관한 것이다.

[0004] 하지만, 현재 종래의 통신 시스템 구조하에서는 기기간 통신을 수행하도록 함에 있어서, 단말 관련 정보의 보안상 노출에 따른 취약점 및 기타 운영상의 어려움으로 인하여 기기 간 통신을 위한 보안 설정, 관리를 위한 시스템 및 방안에 대한 논의가 부족하여, 보안상 취약성, 혹은 통신 수행에 있어서 비 효율적인 문제가 발생할 수 있는 여지가 있었다.

발명의 내용

해결하려는 과제

[0005] 본 발명을 통하여 기기 간 통신을 수행하려는 기기는 기기 간 통신을 수행하기 위한 정보를 획득하고, 기기 간 통신을 수행하기 위한 보안키를 획득하고, 기기 간 통신을 수행하기 위한 보안을 설정하여 안전한 통신을 수행할 수 있다.

과제의 해결 수단

[0006] 본 발명의 일 실시 예에 따르면, 프로즈 함수(prose function) 노드로 프로즈(prose) 등록 요청 메시지를 전송하는 단계, 상기 프로즈 함수(prose function) 노드로부터 프로즈(prose) 인증 토큰을 수신하는 단계, 상기 수신한 인증 토큰에 대한 응답 값을 포함하는 메시지를 상기 프로즈 함수(prose function) 노드로 전송하는 단계, 상기 단말과 어플리케이션 서버 간 통신을 위한 무결성 키(integrity key) 및 암호화 시드 키(encryption key seed)를 포함하는 프로즈(prose) 등록 응답 메시지를 수신하는 단계 및 상기 프로즈(prose) 등록 응답 메시지에 대응하여 상기 어플리케이션 서버와 통신을 수행하기 위한 프로즈 키(prose key)를 생성하는 것을 특징으로 하는 보안 방법을 제공한다.

[0007] 또한, 본 발명의 일 실시 예에 따르면, 이동 통신 네트워크의 적어도 하나의 노드와 통신을 수행하는 송수신부 및 프로즈 함수(prose function) 노드로 프로즈(prose) 등록 요청 메시지를 전송하고, 상기 프로즈 함수(prose function) 노드로부터 프로즈(prose) 인증 토큰을 수신하며, 상기 수신한 인증 토큰에 대한 응답 값을 포함하는 메시지를 상기 프로즈 함수(prose function) 노드로 전송하고, 상기 단말과 어플리케이션 서버 간 통신을 위한 무결성 키(integrity key) 및 암호화 시드 키(encryption key seed)를 포함하는 프로즈(prose) 등록 응답 메시지를 수신하며, 상기 프로즈(prose) 등록 응답 메시지에 대응하여 상기 어플리케이션 서버와 통신을 수행하기 위한 프로즈 키(prose key)를 생성하도록 제어하는 제어부를 포함하는 것을 특징으로 하는 장치를 제공한다.

발명의 효과

[0008] 본 발명을 통해 EUTRAN (Evolved Universal Terrestrial Radio Access Network : 이하 EUTRAN 표기) 혹은 UTRAN (Universal Terrestrial Radio Access Network : 이하 UTRAN 표기) / GERAN (GSM/EDGE Radio Access Network : 이하 GERAN 으로 표기) 등과 같은 환경에서 기기(device)가 단말 간 혹은 네트웍의 도움을 받아 서로 간 정보를 제공하거나 받을 수 있다. 또한, Prose discovery, prose communication 을 위한 prose 관련 보안을 설정하기 위한 보안키 관련 정보를 전달 받고, 이러한 보안키를 이용하여 보안 절차를 수행함으로써, Prose discovery, prose communication 에 있어서 통신의 효율성 및 보안성이 강화되는 이점이 있다.

도면의 간단한 설명

[0009] 도 1는 본 발명의 일 실시 예에 따른 네트워크 환경을 설명하는 도면이다.

도 2a 및 도 2b 는 본 발명의 일 실시 예에 따른 prose discovery, prose communication 단말간 통신의 보안을 위한 통신 및 보안 절차를 설명하는 메시지 흐름도이다.

도 3a 및 도 3b는 본 발명의 일 실시 예에 따른 prose discovery, prose communication 단말 간 통신의 보안을 위한 통신 및 보안 절차를 나타낸 메시지 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 것으로서 이는 사용자 및 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0011] 후술되는 본 발명의 요지는 이동 통신 시스템 환경하에서 상기 기술된 다양한 기기가 단말(UE)로 동작하여 기기 간 서로를 발견하고(discovery), 서로간 통신(communication)을 수행하도록 하기 위하여, 관련 정보를 전달하고, 보안 절차를 수행하고, 안전하게 통신이 가능하도록 하는 방안을 제공하는 것이다.

[0012] 이하 본 발명을 구체적으로 설명하는데 있어, 3GPP 를 기반으로 하는 EPS 시스템, UTRAN, GERAN 을 이용할 것이며, 본 발명은 다른 이동 시스템에서도 이용 가능할 것이다.

[0013] 한편 본 발명에서는 단말이 기기 간 통신을 함에 있어서 관련 정보를 전달 받고, 보안 관련 정보를 전달받고, 보안 절차를 수행함에 있어서 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다.

[0014] 한편 본 발명의 도 1에서 보는 바와 같이 본 발명의 실시예는 본 발명의 기본 목적인 통신 단말을 포함한 다양한 기기가 EUTRAN 혹은 3GPP 환경하에서 기기간 통신을 수행하려고 할 때 관련 정보를 전달하고, 보안 절차를 수행하며, 안전한 통신이 가능하도록 하는 관리 방법을 제기한 것으로, 이러한 방법은 유사한 기술적 배경 및 채널 형태, 혹은 네트웍 구조 (architecture) 또는 유사한 프로토콜 혹은 프로토콜은 상이하나 유사한 동작을 하는 프로토콜을 가지는 여타의 이동통신 시스템에서도 본 발명의 범위를 크게 벗어나지 아니하는 범위에서 약간의 변형으로 적용 가능하며, 이는 본 발명의 분야에서 숙련된 기술적 지식을 가진 자의 판단으로 가능할 것이다.

[0015] 도 1은 본 발명의 일 실시예에 따른 prose discovery, prose communication 의 보안 설정 및 prose communication 을 위한 환경을 도시한 블록도 이다. 여기에서는 일 예로서 3GPP EPS 시스템 구조를 도시하였다. 본 발명의 경우 EUTRAN 을 중심으로 기술하였으며, 이러한 방법은 유사한 다른 이동 통신 시스템에서도 사용할 수 있다.

[0016] 도 1을 참조하면, 기기(device) 또는 단말 (UE: user equipment) (111) 은 종래의 이동 통신 단말(UE : user equipment)이나 machine type communication 을 수행하는 기기, Consumer Devices등 다양한 기기가 포함될 수 있다.

[0017] 본 발명의 도 1에서는 UE1(111) 과 UE2(131) 가 prose discovery 를 하고 prose 통신을 함에 있어서 적용할 수 있는 환경이다. UE (111)는 eNB (114), MME (116) 을 통해서 일반적은 EUTRAN communication 을 수행할 수 있고, serving gateway(118), PDN gate way (119) 등을 통해서 data 통신을 수행한다. 한편 prose 기능 수행을 위해서, prose 관련 기능을 수행하는 prose function server(127) 가 존재하여, prose 관련 등록 및 관련 정보의 전달 및 단말의 prose 관련 capability 등을 검증하며, prose 관련 기능을 수행하게 된다. 한편 HSS (121) 가 존재하여 UE 에 관한 subscription 의 정보 및 UE 관련 보안키 정보 등을 전달하게 된다. Prose 의 응용(application) 서버 기능은 prose 가 prose application server (125) 를 통하여 수행하게 되며, 이러한 prose application 을 수행하기 위해서는 PCRF (policy and charging rules function) (123-1) 과 연동하여 prose 관련 data 서비스를 수행하게 된다.

[0018] 따라서, 본 발명에서는 이동 통신 및 인터넷 통신에서 사용되는 프로토콜을 기반으로 기기 혹은 단말 (UE :111), eNB, MME, prose function, HSS, application server 등의 엔티티들이 proximity based service,

prose discovery, prose communication 를 가능하도록 하는 인증, 보안 및 통신 설정 과정 및 동작을 지원할 수 있도록 상기의 네트워크를 참조하여 이하 도 2내지 도 3을 설명하기로 한다.

[0019] 도 2 는 본 발명의 일 실시 예에 따른 prose discovery, prose communication 단말간 통신의 보안을 위한 통신 및 보안 절차를 나타낸 메시지 흐름도 이다. 도 2 의 실시예에서는 단말 대 단말의 (UE to UE) prose discovery 및 prose 통신을 위한 control 이 기지국(eNB) 에서 수행되는 경우를 일 실시예로 나타낸 경우이다.

[0020] 201 과정에서 UE는 eNB 로 attach request 메시지를 전송하여, 등록 절차를 수행하고, UE가 전송한 attach request 메시지는 MME 로 전송(transfer) 된다. 203 과정에서 MME 는 HSS 로 Authentication data request 메시지를 전송하고 HSS 는 MME 로 인증 벡터 (authentication vector) 등을 포함한 보안 관련 정보를 전송한다. 204 과정에서 MME 는 UE로 인증 토큰(AUTN) 을 포함하는 User authentication request 메시지를 전송하고 UE 는 MME 로 User authentication response 메시지와 함께 RES(response 보안값)을 전송한다. 205 과정에서 MME 는 HSS 로 update location request 메시지를 전송한다. 207 과정에서 HSS 는 MME 로 subscription data 를 전송하게 된다. 이 때 prose 서비스를 하기 위한 prose 식별자 (identity), Prose 그룹 식별자 (prose group identity), Prose Group Key, UE 의 prose 관련 능력(capacity),등록된 prose 식별자와 보안키가 있다면 proximity 관련 보안 키(prose key), prose PLMN list 등의 정보를 함께 전달한다. Proximity 관련 보안키는 proximity discovery 또는 proximity communication 을 위한 보안키로 이미 등록된 정보가 있는 경우 등록된 정보를 조회해서 알려주고, 등록된 정보가 없는 경우는 이후 인증후 생성하도록 한다. 209 과정에서는 MME 에서 eNB 로 attach accept 메시지가 전송되고 이 attach accept 메시지는 211 과정에서 eNB 에서 UE 로 전송된다. 이러한 209 과정과 211 과정에는 207 과정에서 HSS 로부터 전달된 prose 서비스를 하기 위한 prose 식별자 (identity), UE 의 prose 관련 능력(capacity), proximity 관련 보안 키, prose group key, prose group identity, prose PLMN list 등의 정보도 함께 전달된다.

[0021] 213 과정에서는 UE 로부터 prose function 으로 prose 등록 요청 메시지가 전송된다. 215 과정에서는 Prose function에서 HSS 로 prose 등록 요청 메시지가 전송되고 이후 HSS 에서 prose function 으로 prose 인증 벡터 (prose authentication vector) 가 전송된다. 이러한 인증 벡터에는 암호키 (Cipher Key : 이하 CK로 표기) 와 무결성키 (Integrity Key : 이하 IK로 표기) 가 포함되어 전송된다. 217 과정에서 prose function 으로부터 UE 로 prose 인증 토큰이 전송된다.

[0022] 221 과정에서는 prose 등록을 위해 prose function 에서 UE로 전송한 인증 토큰에 대한 응답값을 포함한 메시지가 UE에서 prose function 으로 전송되어 오고 prose function 에서는 RES 와 XRES 정보를 비교하여, 검증 한다. 223 과정에서 prose function 에서 UE 로 prose 등록 응답 메시지가 전송되고 이때 UE 와 application Server 간 통신을 보호해줄 integrity key, encryption key seed 가 전송된다.

[0023] 225 과정에서 UE 는 prose 통신을 하기 위한 Prose key 를 생성할 수 있으며, Prose Key 는 UE 와 application 통신에 사용된다. 이러한 prose key 는 IK, CK 로부터 생성되거나 KASME 를 이용하여 생성할 수 있다. 한편 227 과정에서 prose function 은 IK, CK 로부터 prose key 를 생성하거나, 혹은 prose function 은 KASME 로부터 prose key 를 생성할 수 있다. IK, CK 로부터 생성할 경우는 HSS 로부터 전달된 값을 이용하면 되고, 만일 KASME 로부터 생성할 경우는 MME 로부터 KASME 를 제공 받거나, prose function 이 MME 와 결합(combined) 된 구조에서 가능하다. 229 과정에서는 prose function 에서 application 서버로 prose key 와 prose function 에 UE 가 등록하는 과정에 prose 서비스를 위해 등록한 관련 정보가 전달된다. 또한 integrity key, encryption key 등을 위한 seed 정보도 함께 전달될 수 있다. 230 과정에서는 prose key, integration key seed, encryption key seed 등의 정보중 적어도 하나가 저장될 수 있다. 이후 231 과정에서 UE 와 application server는 prose key, prose 식별자 등을 이용해서 통신을 수행한다.

[0024] 이후의 과정은 UE 와 다른 UE 가 prose key 또는 Prose 식별자 (identity : 이후 ID) 등을 이용해서 통신을 수행하는 과정에 대한 설명이다.

[0025] 233 과정에서 UE2는 UE1와의 기기간 prose 통신 요청을 eNB 로 전송한다. 이 때 UE2의 prose identity (식별자 이후 ID로 표기) , UE1의 prose ID 그리고, prose group ID 가 식별자로 사용될 수 있다. 235 과정에서 eNB 는 UE2 가 해당 prose group 에 속하는지 검증한다. 이때 UE2 의 prose ID 를 가지고 prose 그룹을 검증하거나 또 다른 일 실시예로는 UE2 가 전송한 prose group ID 와 UE2 의 prose ID 가지고 검증할 수 있다. 237 과정에서 eNB 는 UE1 에게 paging 을 하는데, 이 때 UE to UE 통신임을 알리는 indication 을 마크해서 보냄으

로써, UE to UE 통신 임을 알 수 있다. 이후 239 과정에서 eNB 는 UE2 의 UE1 로의 기기간 prose 통신 요청을 전달(transfer) 한다. 이 때 일실시예로 UE1 의 prose ID 를 UE2 가 destination 으로서 아는 경우라면, UE1 으로 dedicated 하게 전송할 수 있다.(case 1) 혹은 또 다른 일 실시예(case 2) 로 239 과정과 241 과정에서와 같이 이러한 요청을 broadcast 를 하고, 243이나 245 과정에서와 같이 UE1 이나 UE3 로부터 응답이 온 경우 응답을 검증하는 과정을 통해서 적합한 destination 인지 검증할 수 있다. 이러한 경우는 일 실시예는(case2) broadcast 채널을 이용하거나, 또다른 일 실시예는(case 3) prose 를 위한 특정한 채널을 사용할수 있다. 이러한 239 과정이나 241 과정의 prose request 에는 prose 통신 요청자인 UE2 의 prose ID 가 포함될 수도 있다 (announce 모델: 나는 누구이다. 또는 요청자는 누구이다.). 또 다른 일 실시예에서는 UE2 의 prose ID 뿐 아니라, destination 인 UE1 의 prose ID 를 포함할 수도 있다

[0026] UE2의 기기간 통신 요청을 전달한 eNB 는 실시예에 따라 UE1 으로부터 응답을 받거나, UE1을 비롯한 여러 단말들로부터 응답을 받고, 그중 UE 1 으로부터 응답인지를 판단해야 하므로, 247 과정 혹은 249 과정내지 253 과정의 검증 단계를 거치게 된다. 247 과정에서는 일 실시예로 eNB 수준에서 기기간 통신 요청에 대한 검증이 있는 것이다. 249 과정내지 253 과정은 Prose function 수준에서 기기간 통신 요청에 대한 검증이 있는 경우 이다. 247 과정에서의 검증은 일 실시예에 의하면 (case 1) 목적(target) 상대 UE 가 UE1 인지를 검증하는 것이다. 즉 UE2 가 prose 통신을 요청한 target 엔티티가 UE1 인지를 검증한다. 이에 대한 검증은 UE2 가 prose 통신 가능한 통신 가능 리스트에 UE1이 있는지 확인하는 등의 방법을 통해 가능하다. 또 다른 일 실시예는 (case2) 는 같은 prose group 에 UE1 과 UE2 가 속하는지 판단하는 것이다. 이는 prose group 리스트나 prose group ID 에 의해서 판단이 가능하다. 이러한 실시예의 경우는 prose group ID 는 prose group 을 판단할 수 있도록 그룹 식별자와 개별 개체 식별자로 구성되어 있을 수 있다.

[0027] 또 다른 가능한 실시예 경우 2-2 (case 2-2) 는 249 과정내지 253 과정으로 이루어 진다. 즉 249 과정에서는 eNB 에서 Prose function 으로 검증 요청을 전송한다. 이후 251 과정에서 prose communication list 를 검증한다. 이러한 prose communication list 는 UE2 와 prose 통신이 가능한 prose 그룹에 있는 UE 들의 list 이다. 253 과정에서 검증에 대한 응답이 prose function 에서 eNB 로 보내진다. 이때 단순히 검증이 성공했는지 여부만 보낼 수도 있다. 혹은 또 다른 실시예는 가능한 리스트 들의 정보를 eNB 로 전송할 수도 있다. 그러한 경우는 그러한 리스트 들이 eNB 가 UE2 를 대신해서 target UE 를 찾아 통신 요청을 전송하는데 활용될 수 있다.

[0028] 한편 249 과정에서 보낸 prose function 검증 요청에 대해서 251 과정에서 또 다른 실시예 경우 3 (case 3) 의 경우는 prose UE to UE key (여기선 between UE1 and UE2) 를 생성할 수 있다. 이때 Prose UE to UE key 생성식은 다음과 같다.

[0029] 식 1 : Prose UE to UE key = KDF (prose group key , prose UE 1 ID, Prose UE2 ID, RAND, prose server ID)

[0030] 여기서 Key 로 prose group key 를 사용할 수도 있다.

[0031] RAND 는 난수 (random number), Proser server ID 는 prose server 의 식별자, 이들 Prose UE1 ID, Prose UE2 ID, RAND, prose server ID 등은 concatenation 되어 사용될 수 있다.

[0032] KDF는 key derivation function 으로 일 예를 들면 HMAC-SHA256 등이 될 수가 있다.

[0033] 이후 255 과정에서 eNB 는 UE1에 UE2 로부터 prose 통신 요청이 있음을 알린다. 또한 UE1 에게 UE2 의 address 를 알려줄 수도 있다. 257 과정에서 UE1 은 UE2의 prose 통신 요청에 대한 응답을 보낼 수 있다. 259 과정에선 UE2 는 UE1 에 prose 통신 요청 완성 (request complete) 를 보낼 수 있다. 상기의 255과정 후반부에서 259 과정은 또 다른 실시예에서는 생략될 수도 있다. 이후 261 과정에서 UE1 과 UE2는 UE 와 UE 간 prose 통신을 수행할 수 있다.

[0034] 도 3은 본 발명의 일 실시 예에 따른 prose discovery, prose communication 단말 간 통신의 보안을 위한 통신 및 보안 절차를 나타낸 메시지 흐름도이다. 도 3의 실시 예에서는 단말 대 단말의 (UE to UE) prose discovery 및 prose 통신을 위한 control이 UE에서 수행되는 경우를 일 실시 예로 나타낸 경우이다.

[0035] 301 과정에서 UE는 eNB로 attach request 메시지를 전송하여, 등록 절차를 수행하고, UE가 전송한 attach request 메시지는 MME 로 전송(transfer) 된다. 303 과정에서 MME는 HSS로 Authentication data request 메시지를 전송하고 HSS는 MME로 인증 벡터(authentication vector) 등을 포함한 보안 관련 정보를 전송한다. 304 과정에서 MME는 UE로 인증 토큰(AUTN)을 포함하는 User authentication request 메시지를 전송하고 UE는 MME로 User authentication response 메시지와 함께 RES(response 보안값)을 전송한다. 305 과정에서 MME는 HSS로

update location request 메시지를 전송한다. 307 과정에서 HSS는 MME로 subscription data를 전송하게 된다. 이때, prose 서비스를 하기 위한 prose 식별자 (identity), Prose 그룹 식별자 (prose group identity), UE의 prose 관련 능력(capacity), 등록된 prose 식별자와 보안키가 있다면 proximity 관련 보안 키(prose key), prose PLMN list 등의 정보를 함께 전달한다. Proximity 관련 보안키는 proximity discovery 또는 proximity communication 을 위한 보안키로 이미 등록된 정보가 있는 경우 등록된 정보를 조회해서 알려주고, 등록된 정보가 없는 경우는 이후 인증후 생성하도록 한다. 309 과정에서는 MME에서 eNB로 attach accept 메시지가 전송되고 이 attach accept 메시지는 311 과정에서 eNB에서 UE로 전송된다. 이러한 309 과정과 311 과정에는 307 과정에서 HSS로부터 전달된 prose 서비스를 하기 위한 prose 식별자 (identity), UE의 prose 관련 능력(capacity), proximity 관련 보안 키, prose group key, prose group identity, prose PLMN list 등의 정보도 함께 전달된다.

[0036] 313 과정에서는 UE로부터 prose function으로 prose 등록 요청 메시지가 전송된다. 이 과정에서는 UE 가 이후 다른 UE 와 통신을 위해 UE의 public key가 prose function으로 전송될 수도 있다. 이렇게 전송된 UE의 public key는 prose function 에 저장된다. 이러한 과정을 위해서 UE는 자신의 public key를 key authentication 센터로부터 받아와서 전송하거나 혹은 UE의 요청 메시지에 따라서 prose function이 UE의 public key를 key authentication center로부터 전송받아 저장할 수 있다. 이 과정에서 일어난 경우라면 333 과정에서와 같은 과정은 생략될 수 있다.

[0037] 313-2 과정에서는 UE2 도 UE1 처럼 prose 등록 요청 과정을 수행한다.이후 과정은 UE1 을 가지고 설명하지만, UE2 에 대해서 기본적으로 UE1 과 같은 등록 과정을 거치는 것으로 가정한다. 315 과정에서는 Prose function에서 HSS 로 prose 등록 요청 메시지가 전송되고 이후 HSS에서 prose function으로 prose 인증 벡터(prose authentication vector) 가 전송된다. 이러한 인증 벡터에는 암호키 (Cipher Key : 이하 CK로 표기) 와 무결성키 (Integrity Key : 이하 IK로 표기) 가 포함되어 전송된다. 317 과정에서 prose function 으로부터 UE 로 prose 인증 토큰이 전송된다.

[0038] 321 과정에서는 prose 등록을 위해 prose function 에서 UE로 전송한 인증 토큰에대한 응답 값을 포함한 메시지가 UE에서 prose function으로 전송되어 오고 prose function 에서는 RES 와 XRES 정보를 비교하여, 검증한다. 323 과정에서 prose function에서 UE로 prose 등록 응답 메시지가 전송되고 이때 UE 와 application Server 간 통신을 보호해줄 integrity key, encryption key seed 가 전송된다.

[0039] 325 과정에서 UE는 prose 통신을 할 수 Prose key를 생성할 수 있으며, Prose Key 는 UE 와 application 통신에 사용된다. 이러한 prose key 는 IK, CK 로부터 생성되거나 KASME를 이용하여 생성할 수 있다. 한편 327 과정에서 prose function 은 IK, CK 로부터 prose key 를 생성하거나, 혹은 prose function 은 KASME 로부터 prose key 를 생성할 수 있다. IK, CK 로부터 생성할 경우는 HSS 로부터 전달된 값을 이용하면 되고, 만일 KASME 로부터 생성할 경우는 MME 로부터 KASME 를 제공 받거나, prose function 이 MME 와 결합(combined) 된 구조에서 가능하다.

[0040] 329 과정에서는 prose function 에서 application 서버로 prose key와 prose function 에 UE가 등록하는 과정에 prose 서비스를 위해 등록한 관련 정보가 전달된다. 또한 integrity key, encryption key 등을 위한 seed 정보도 함께 전달될 수 있다. 330 과정에서는 prose key, integration key seed, encryption key seed 등의 정보 중 적어도 하나가 저장될 수 있다. 이후 331 과정에서 UE 와 application server는 prose key, prose 식별자 등을 이용해서 통신을 수행한다.

[0041] 이후의 과정은 UE 와 다른 UE 가 prose key 또는 Prose 식별자 (identity : 이후 ID) 등을 이용해서 통신을 수행하는 과정에 대한 설명이다.

[0042] 만일 이후의 371 과정에서 UE2 가 prose 통신을 위해 보낸 request 에 대해서 case 3) 의 경우와 같이 공개키 (public key) 를 통해 검증하고자 하는 경우는 333 과정에서와 같이 UE1으로부터 prose function으로 prose 등록 완성(registration complete) 메시지를 보내면서 UE의 public key 를 등록한다. 이 과정에서는 UE 가 이후 다른 UE 와 통신을 위해 UE 의 public key 가 prose function 으로 전송될 수도 있다. 이렇게 전송된 UE 의 public key 는 prose function 에 저장된다. 이러한 과정을 위해서 UE 는 자신의 public key 를 key authentication 센터로부터 받아와서 전송하거나 혹은 UE 의 요청 메시지에 따라서 prose function 이 UE 의 public key 를 key authentication center 로부터 전송 받아 저장할 수 있다. 만일 위의 prose regi 과정인 313 과정에서 public key 를 등록한 경우라면 이러한 과정은 생략될 수 있다.

[0043] 본 설명에서는 333 과정에서 UE1을 예로 들었지만, UE2 도 공개키로 검증하는 경우 UE의 public key 를 등록한다. 또 다른 일 실시 예로는 333 과정이나 313 과정에서와 같이 통신을 하기 위해서 자신의 public key 를 prose server 에 등록한 UE 들의 public key 를 그러한 UE 와 통신하고자 하는 UE 가 313 과정이나 334 과정에서와 같이 받아오는 방법을 통해서 통신하고자, 혹은 정보를 얻고자 하는 UE 의 public key 를 받아와서 검증하는데 활용할 수 있다. 즉 334 과정에서는 정보를 얻고자 하는, 혹은 통신하고자 하는 UE 의 public key 를 받아옴으로써 이후 해당 UE 의 메시지를 수신하고, 이를 검증하는데 활용할 수 있다.

[0044] 한편 335 과정에서와 같이 UE 1 가 (혹은 UE2 의 공개키로 검증하는 경우라면 UE2 의 공개키를 UE2 가) public key 를 prose group 으로 알려주며, 이렇게 알려주는 방법으로는 broadcast 등이 사용될 수도 있다.

[0045] 337 과정에서 UE2 는 paging 을 보낸다. 이 때 paging 메시지에는 UE 에서 UE 로 prose 통신을 위한 지시자 (indication) 이 포함되어 있을 수 있다.

[0046] 335 과정이나 337 과정과 같은 public key 를 prose group 에게 알려주거나, paging 하는 방법 등은 다른 일 실시예에 의하면 생략될 수도 있는 과정이다.

[0047] 한편 339 과정에서 UE2 는 다른 UE와 통신하기 원함을 알리며, prose 통신을 위해 요청(request) 하며, 이러한 request 방법에는 broadcast, broadcast IP 등을 사용하는 방법을 통해 이루어질 수도 있다.

[0048] UE2로부터 prose 통신 요청을 받은 UE1은 UE1이 목적 (target) prose 상대 노드 인지 판단해야 하므로, 371 과정 혹은 381 과정내지 383 과정의 검증 단계를 거치게 된다. 371 과정에서는 일 실시예로 UE 수준에서 기기간 통신 요청에 대한 검증이 있는 것이다. 381 과정 내지 385 과정은 Prose function 수준에서 기기간 통신 요청에 대한 검증이 있는 경우이다. 371 과정에서의 검증은 일 실시예에 의하면 (case 1) 목적(target) 상대 UE 가 UE1 인지를 검증하는 것이다. 즉 UE2가 prose 통신을 요청한 target prose ID 가 UE1 인지를 검증한다. 이에 대한 검증은 UE2 와 prose 통신 가능한 통신 가능 리스트에 UE1이 있는지 확인하는 등의 방법을 통해 가능하다.

[0049] 371 과정의 또 다른 일 실시예 (case2) 는 미리 공유된 preshared key 를 이용한 검증이다. 이러한 검증을 세부적으로 살펴보면, 337 -> 339 -> 361 -> 363 -> 371 -> 387 이후의 일련의 과정으로 이루어지는 과정이다. 이 때 337 과정은 생략될 수도 있다. 339 과정 이후 361 과정에서와 같이 UE1 은 random number 나 time stamp 등을 포함하는 시도 (challenge) 를 UE2 로 보내면 363 과정에서 UE2 는 preshared 키를 이용하여 random 값을 암호화 하여 보내고 이것을 371 과정에서 UE1 이 복호화 (decrypt) 하여 검증할 수 있다. 이 때 time stamp 값은 application 에서 사용하는 값을 사용할 수도 있으며, 또 다른 실시 예로는 radio frame 에서 사용하는 값을 사용함으로써 보다 정확한 time stamp 를 사용하여 수신과 송신의 동기를 맞출 수가 있고, 보안을 더욱 강화할 수도 있다.

[0050] 371 과정의 또 다른 일 실시예 (case 3) 는 public key 를 이용한 검증이다. 이러한 검증을 세부적으로 살펴보면, case 3-1 의 경우는 public key 를 이용하여 검증하는 방법으로 333 -> 334 -> 335 -> 337 -> 339 -> 341 -> 343 -> 345 -> 371 -> 387 이후의 일련의 과정으로 이루어진다. 이때 335, 337 과정은 생략될 수도 있다. 즉 335 과정은 334 과정의 형태로 public key 를 전송하는 경우와는 다른 실시 예로써, broadcast 등으로 사전에 상대편의 public key 를 획득하는 경우가 아니라면 334 과정에서와 같이 상대 노드의 public key 를 수신해 오는 과정이 있게 된다.

[0051] 341 과정에서 UE2 에서 UE1 로 시도 (challenge) 메시지가 보내지면 343 과정에서 UE1 에서 UE2 로 UE2 의 public key 로 encrypted 된 random number, 혹은 time stamp 를 보낸다. 이 때 time stamp 값은 application 에서 사용하는 값을 사용할 수도 있으며, 또 다른 실시 예로는 radio frame 에서 사용하는 값을 사용함으로써 보다 정확한 time stamp 를 사용하여 수신과 송신의 동기를 맞출 수가 있고, 보안을 더욱 강화할 수도 있다. 345 과정에서와 같이 UE2 는 UE2의 private 키로 복호화(decrypt)하여 UE1 로 random number, 혹은 time stamp 를 전송하여 보냄으로 검증이 완료 된다. 이 때 time stamp 값은 application 에서 사용하는 값을 사용할 수도 있으며, 또다른 실시예로는 radio frame 에서 사용하는 값을 사용함으로써 보다 정확한 time stamp 를 사용하여 수신과 송신의 동기를 맞출 수가 있고, 보안을 더욱 강화할 수도 있다.

[0052] 또 다른 일 실시예 case 3-2 의 경우는 public key 를 이용하여 검증하는 것으로, 암호화된 서명 (digital signature) 으로 송신자를 인증하는 방식이다. 즉, 333 -> 335 -> 337 -> 339 -> 351 -> 353 -> 371 -> 387의 일련의 과정으로 이루어 진다. 이때 335, 337 과정은 생략될 수도 있다. 즉 335 과정은 334 과정의 형태로

public key 를 전송하는 경우와는 다른 실시 예로써, broadcast 등으로 사전에 상대편의 public key 를 획득하는 경우가 아니라면 334 과정에서와 같이 상대 노드의 public key 를 수신해오는 과정이 있게 된다.

[0053] 한편 339 과정에서와 같이 UE2가 UE2의 private key 를 가지고, digital signature (서명)을 해서 보내는 경우는 UE1는 이미 UE2 의 public key 를 334 혹은 335 과정에서 획득하여 알고 있는 경우이다.이때 random number 혹은 time stamp 값이 활용될 수 있다. 이 때 time stamp 값은 application 에서 사용하는 값을 사용할 수도 있으며, 또 다른 실시 예로는 radio frame 에서 사용하는 값을 사용함으로써 보다 정확한 time stamp 를 사용하여 수신과 송신의 동기를 맞출 수가 있고, 보안을 더욱 강화할 수도 있다. 이렇게 339 과정이 검증하는 과정을 포함하는 경우는 다른 실시예와는 또 다른 실시예(case 5) 가 된다.

[0054] 따라서 339 과정에 따라서 UE2 가 UE 1으로 broadcast 메시지를 전송할 때 UE1 은 그 메시지를 수신하여 UE2 즉 메시지를 송신한 송신자를 인증할 수 있다.

[0055] 또 다른 일 실시예로 351 과정에서 UE1은 UE2 로 random number, 혹은 time stamp를 보내고, 353 과정에서 UE2에서 UE2의 private key로 서명(signature) 를 해서 보내어 371 과정에서와 같이 검증을 한다. 이때, time stamp 값은 application에서 사용하는 값을 사용할 수도 있으며, 또 다른 실시 예로는 radio frame에서 사용하는 값을 사용함으로써 보다 정확한 time stamp를 사용하여 수신과 송신의 동기를 맞출 수가 있고, 보안을 더욱 강화할 수도 있다.

[0056] 또 다른 가능한 실시예 경우 4 (case 4) 는 381 과정 내지 385 과정으로 이루어진다. 즉 381 과정에서는 UE1에서 Prose function 으로 검증 요청을 전송한다. 이후 383 과정에서 prose communication list를 검증한다. 이러한 prose communication list는 UE1과 prose 통신이 가능한 prose 그룹에 있는 UE 들의 list 이다. 383 과정에서 검증에 대한 응답이 prose function에서 UE1으로 보내진다. 이때 단순히 검증이 성공했는지 여부만 보낼 수도 있다.

[0057] 한편 381 과정에서 보낸 prose function 검증 요청에 대해서 383 과정에서 또 다른 실시예 경우 5 (case 5)의 경우는 검증후 prose UE to UE key (여기선 between UE1 and UE2)를 생성할 수 있다. 이때 Prose UE to UE key 생성식은 다음과 같다.

[0058] 식 1 : Prose UE to UE key = KDF (prose group key , prose UE 1 ID, Prose UE2 ID, RAND, prose server ID)

[0059] 여기서 Key 로 prose group key 를 사용할 수도 있다.

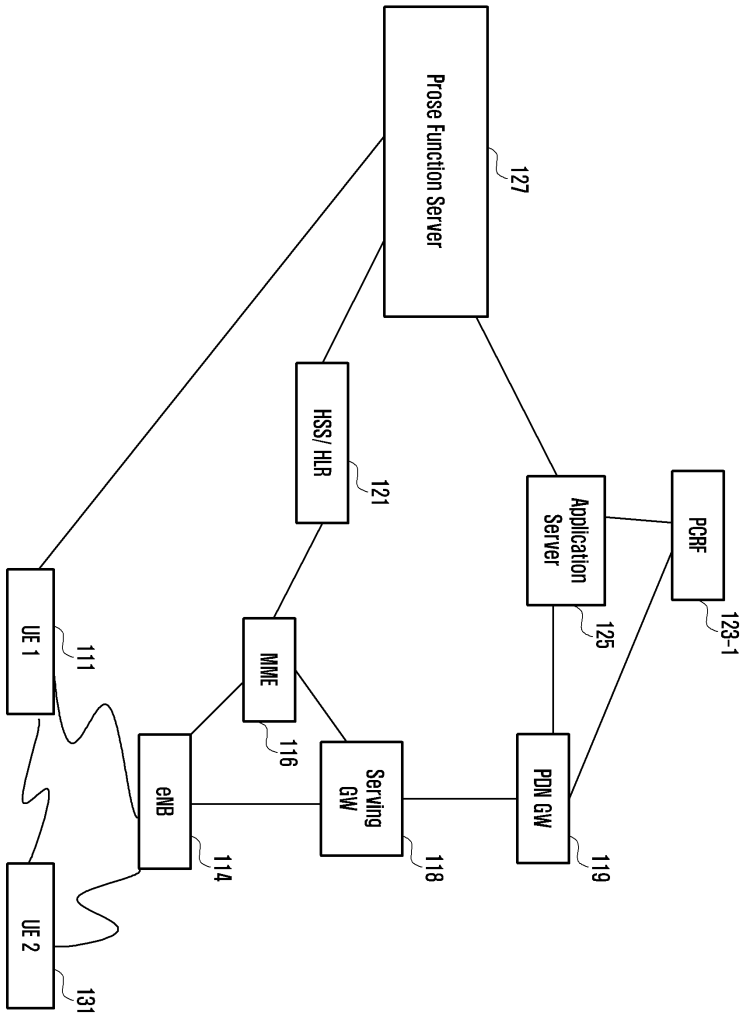
[0060] RAND 는 난수 (random number), Proser server ID 는 prose server 의 식별자, 이들 Prose UE1 ID, Prose UE2 ID, RAND, prose server ID 등은 concatenation 되어 사용될 수 있다. KDF 는 key derivation function 으로 일 예를 들면 HMAC-SHA256 등이 될 수가 있다.

[0061] 387 과정에서 UE1 은 UE2의 prose 통신 요청에 대한 응답을 보낼 수 있다. 389 과정에선 UE2 는 UE1 에 prose 통신 요청 완성 (request complete) 를 보낼 수 있다. 이러한 387, 389 의 과정은 일 실시예에 따라선 생략될 수 있는 과정이다. 이후 391 과정에서 UE1 과 UE2는 UE 와 UE 간 prose 통신을 수행할 수 있다.

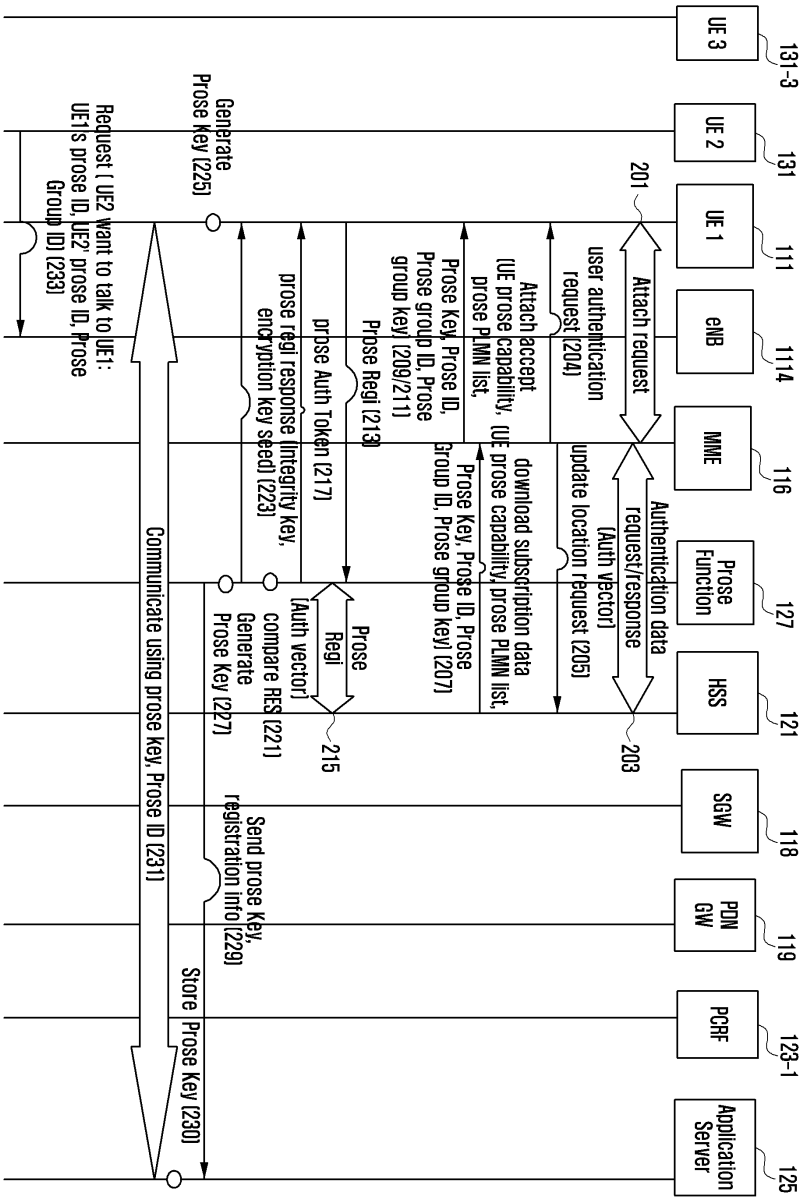
[0062] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

도면

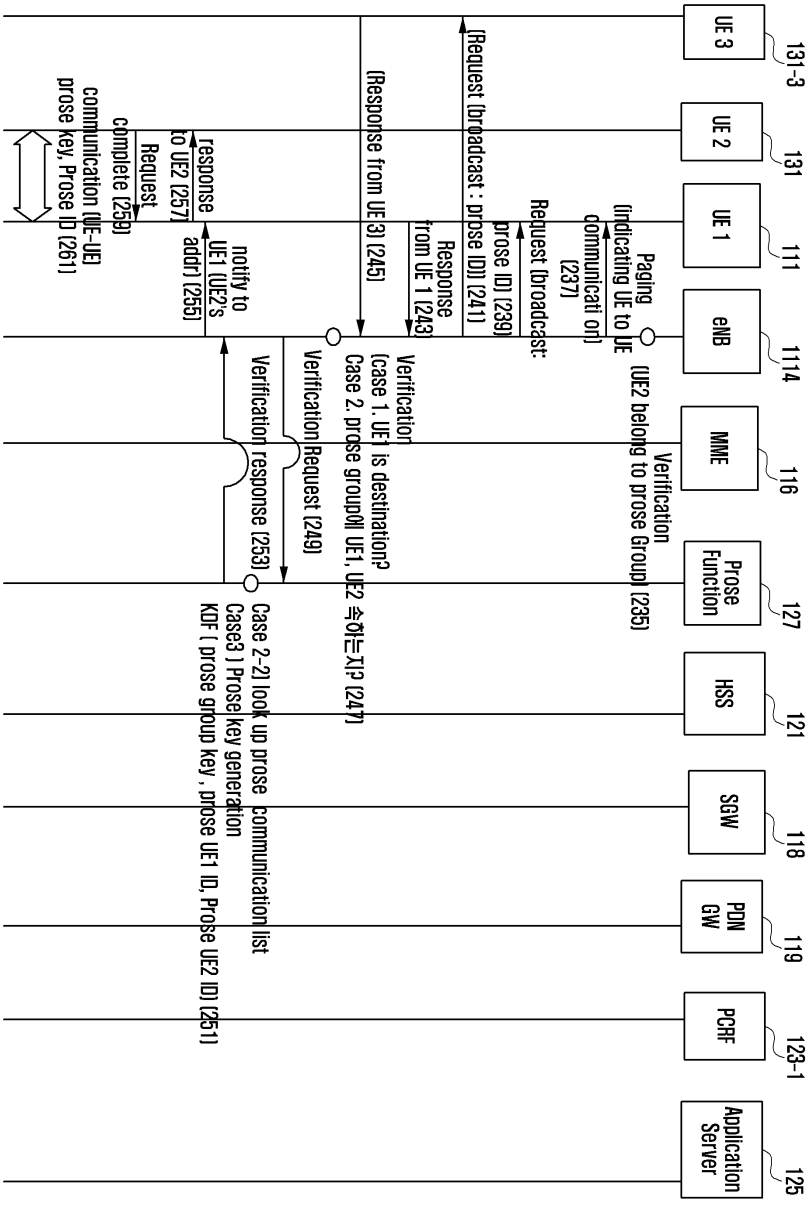
도면1


Prose Function Server
127
HSS/ HLR
121
Application Server
125
PCRF
123-1
UE 1
111
MME
116
eNB
114
Serving GW
118
PDN GW
119
UE 2
131

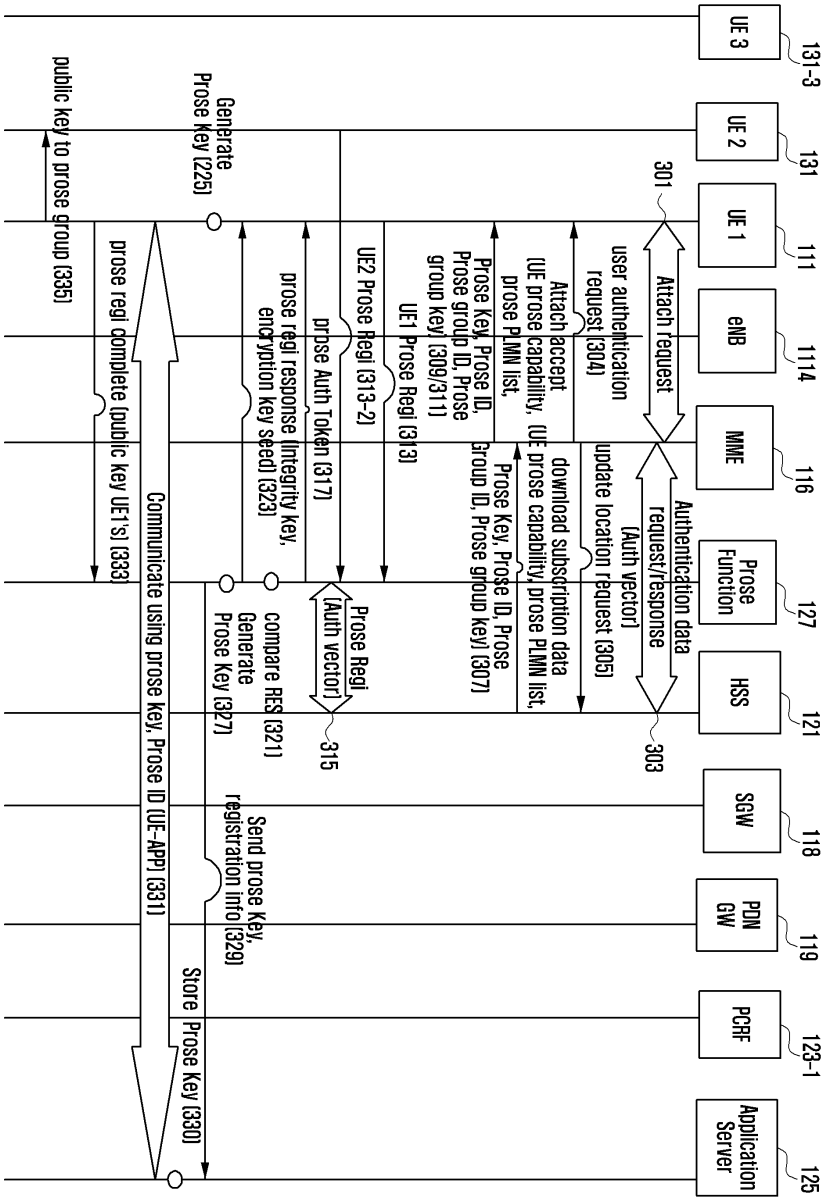
도면2a


UE 3
131-3
UE 2
131
UE 1
111
eNB
1114
MME
116
Prose Function
127
HSS
121
SGW
118
PDN GW
119
PCRF
123-1
Application Server
125
201
203
215
Attach request
user authentication request [204]
Authentication data request/response
[Auth vector]
update location request [205]
Attach accept
[UE prose capability, prose PLMN list,
download subscription data
[UE prose capability, prose PLMN list,
Prose Key, Prose ID, Prose group ID, Prose group key] [209/211]
Prose Key, Prose ID, Prose group ID, Prose group key] [207]
Prose Regi [213]
Prose Regi
[Auth vector]
prose Auth Token [217]
compare RES [221]
prose regi response [Integrity key, encryption key seed] [223]
Generate Prose Key [225]
Generate Prose Key [227]
Send prose Key, registration info [229]
Store Prose Key [230]
Request [UE2 want to talk to UE1: UE1's prose ID, UE2' prose ID, Prose Group ID] [233]
Communicate using prose key, Prose ID [231]

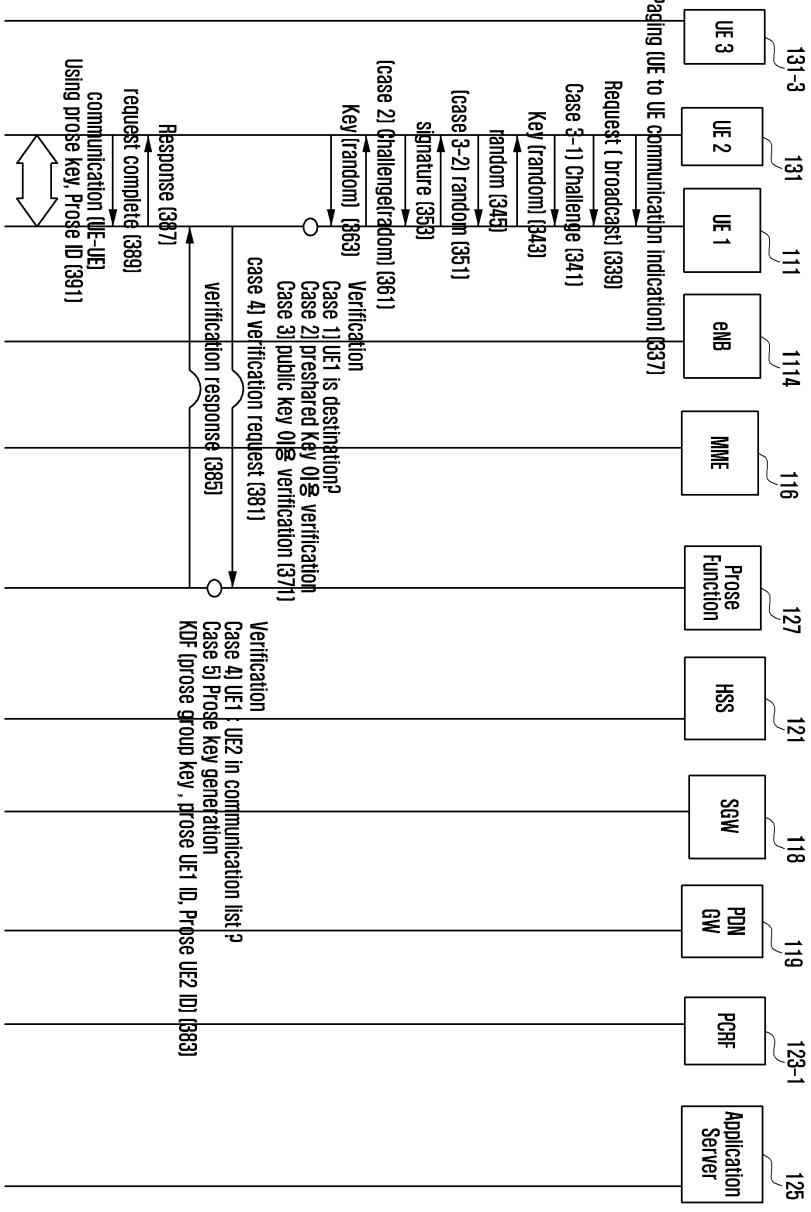
도면2b


UE 3
131-3
UE 2
131
UE 1
111
eNB
1114
MME
116
Prose Function
127
HSS
121
SGW
118
PDN GW
119
PCRF
123-1
Application Server
125
[Request [broadcast : prose ID] [241]
[Response from UE 3] [245]
Response from UE 1 [243]
Paging [indicating UE to UE communicati on] [237]
Request [broadcast: prose ID] [239]
(UE2 belong to prose Group) [235]
Verification
Verification [case 1. UE] is destination? Case 2. prose group에 UE1, UE2 속하는지? [247]
Verification Request [249]
Verification response [253]
Case 2-2] look up prose communication list Case3] Prose key generation KDF (prose group key , prose UE1 ID, Prose UE2 ID) [251]
notify to UE1 (UE2's addr) [255]
response to UE2 [257]
Request complete [259]
communication (UE-UE) prose key, Prose ID [261]

도면3a


UE 3
131-3
UE 2
131
UE 1
111
eNB
1114
MME
116
Prose Function
127
HSS
121
SGW
118
PDN GW
119
PCRF
123-1
Application Server
125
301
303
315
Attach request
Authentication data request/response [Auth vector]
user authentication request [304]
update location request [305]
Attach accept [UE prose capability, prose PLMN list,
download subscription data [UE prose capability, prose PLMN list,
Prose Key, Prose ID, Prose group ID, Prose group key] [309/311]
Prose Key, Prose ID, Prose group ID, Prose group key] [307]
UE1 Prose Regi [313]
UE2 Prose Regi [313-2]
prose Auth Token [317]
Prose Regi [Auth vector]
prose regi response [integrity key, encryption key seed] [323]
compare RES [321]
Generate Prose Key [327]
Send prose Key, registration info [329]
Store Prose Key [330]
Generate Prose Key [225]
public key to prose group [335]
prose regi complete [public key UE1's] [333]
Communicate using prose key, Prose ID [UE-APP] [331]

도면3b


UE 3
131-3
UE 2
131
UE 1
111
eNB
1114
MME
116
Prose Function
127
HSS
121
SGW
118
PDN GW
119
PCRF
123-1
Application Server
125
Paging [UE to UE communication indication] [337]
Request [broadcast] [339]
Case 3-1) Challenge [341]
Key [random] [343]
random [345]
[case 3-2] random [351]
signature [353]
[case 2] Challenge[radom] [361]
Key [random] [363]
Verification
Case 1] UE1 is destination?
Case 2] prestared Key 이용 verification
Case 3] public key 이용 verification [371]
case 4] verification request [381]
verification response [385]
Response [387]
request complete [389]
communication [UE-UE]
Using prose key, Prose ID [391]
Verification
Case 4] UE1 : UE2 in communication list ?
Case 5] Prose key generation
KDF [prose group key , prose UE1 ID, Prose UE2 ID] [383]