(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년07월16일
(11) 등록번호 10-2000717
(24) 등록일자 2019년07월10일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
H04W 12/08 (2009.01)
(52) CPC특허분류
H04W 12/06 (2019.01)
H04L 63/0876 (2013.01)
(21) 출원번호 10-2017-0134866
(22) 출원일자 2017년10월17일
심사청구일자 2018년04월06일
(65) 공개번호 10-2019-0001485
(43) 공개일자 2019년01월04일
(30) 우선권주장
1020170080910 2017년06월27일 대한민국(KR)
(56) 선행기술조사문헌
KR101629006 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이종경
경기도 화성시 동탄순환대로21길 15, 1353동 1202호 (청계동, 동탄2신도시 신안인스빌리베라)
이진근
경기도 성남시 분당구 동판교로 226, 403동 1503호 (삼평동, 봇들마을4단지아파트)
정치욱
충청북도 청주시 상당구 문의면 문의시내로 45-1
(74) 대리인
유미특허법인

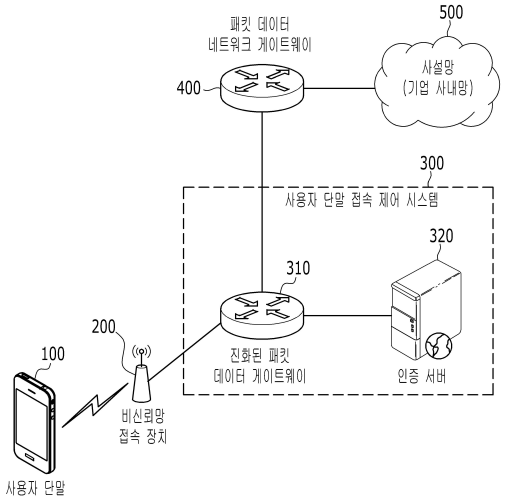
전체 청구항 수 : 총 15 항 심사관 : 이준석

(54) 발명의 명칭 **비신뢰망을 통해 사설망으로 접속하는 사용자 단말의 접속을 제어하는 시스템 및 방법**

(57) 요 약

사용자 단말 접속 제어 시스템이 사용자 단말의 사설망으로의 접속을 제어하는 방법으로서, 비신뢰망 접속 장치에 접속한 사용자 단말로부터, 패킷 데이터 네트워크 게이트웨이(Packet Data Network Gateway, P-GW)에 연결된 사설망으로 접속하기 위한 접속 요청을 수신하는 단계, 상기 접속 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 인증하는 단계, 그리고 상기 인증이 성공적으로 완료되면, 상기 패킷 데이터 네트워크 게이트웨이를 통해 상기 사용자 단말이 상기 사설망으로 접속하도록 허용하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0892 (2013.01)
H04L 69/28 (2013.01)
H04W 12/08 (2019.01)

명 세 서

청구범위

청구항 1

사용자 단말 접속 제어 시스템이 사용자 단말의 사설망으로의 접속을 제어하는 방법으로서,

비신뢰망 접속 장치에 접속한 사용자 단말로부터, 패킷 데이터 네트워크 게이트웨이(Packet Data Network Gateway, P-GW)에 연결된 사설망으로 접속하기 위한 접속 요청을 수신하는 단계,

상기 접속 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 인증하는 단계,

상기 인증이 성공적으로 완료되면, 상기 패킷 데이터 네트워크 게이트웨이를 통해 상기 사용자 단말이 상기 사설망으로 접속하도록 허용하는 단계, 그리고

상기 사용자 단말의 위치 정보에 기초하여 상기 사용자 단말에 대해 재인증 절차를 수행하여, 상기 사용자 단말의 상기 사설망으로의 접속을 제어하는 단계

를 포함하는 사용자 단말 접속 제어 방법.

청구항 2

제1항에서,

상기 인증하는 단계는

상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된 지역의 위치 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정하는 사용자 단말 접속 제어 방법.

청구항 3

제2항에서,

상기 사용자 단말의 위치 정보는

상기 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고,

상기 사설망으로 접속이 허용된 지역의 위치 정보는

상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함하는 사용자 단말 접속 제어 방법.

청구항 4

제1항에서,

상기 접속을 제어하는 단계는

상기 사용자 단말로 재인증 요청을 전송하는 단계,

상기 사용자 단말로부터 상기 재인증 요청에 대응하는 재인증 응답을 수신하는 단계,

상기 재인증 응답에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고

상기 재인증이 성공적으로 완료되면, 상기 사용자 단말의 상기 사설망으로의 접속을 유지하도록 하는 단계

를 포함하는 사용자 단말 접속 제어 방법.

청구항 5

제4항에서,

상기 재인증 응답에서 추출한 상기 사용자 단말의 위치 정보는

상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하며,

상기 재인증하는 단계는

상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정하는 사용자 단말 접속 제어 방법.

청구항 6

제1항에서,

상기 접속을 제어하는 단계는

상기 사용자 단말로부터 재인증 요청을 수신하는 단계,

상기 재인증 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고

상기 재인증이 성공적으로 완료되면, 상기 사용자 단말의 상기 사설망으로의 접속을 유지하도록 하는 단계

를 포함하는 사용자 단말 접속 제어 방법.

청구항 7

제6항에서,

상기 재인증 요청에서 추출한 상기 사용자 단말의 위치 정보는

상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하며,

상기 재인증하는 단계는

상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정하는 사용자 단말 접속 제어 방법.

청구항 8

제1항에서,

상기 접속을 제어하는 단계는

상기 비신뢰망 접속 장치와는 다른 새로운 비신뢰망 접속 장치에 접속한 사용자 단말로부터, 상기 사설망으로 재접속하기 위한 재접속 요청을 수신하는 단계,

상기 재접속 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고

상기 재인증이 성공적으로 완료되면, 상기 사용자 단말이 상기 사설망으로 재접속하도록 하는 단계

를 더 포함하는 사용자 단말 접속 제어 방법.

청구항 9

제8항에서,

상기 재접속 요청에서 추출한 상기 사용자 단말의 위치 정보는

상기 새로운 비신뢰망 접속 장치의 식별 정보 또는 상기 인증 이후 상기 사용자 단말의 GPS 정보를 포함하며,

상기 재인증하는 단계는

상기 새로운 비신뢰망 접속 장치의 식별 정보 또는 상기 인증 이후 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정하는 사용자 단말 접속 제어 방법.

청구항 10

사용자 단말 접속 제어 시스템으로서,

비신뢰망 접속 장치에 접속한 사용자 단말로부터 패킷 데이터 네트워크 게이트웨이에 연결된 사설망 접속을 위한 접속 요청을 수신하고, 상기 접속 요청에서 상기 사용자 단말의 위치 정보를 추출하는 진화된 패킷 데이터 게이트웨이(Evolved Packet Data Gateway, ePDG), 그리고

상기 진화된 패킷 데이터 게이트웨이로부터 상기 사용자 단말의 위치 정보를 포함하는 인증 요청을 수신하고, 상기 사용자 단말의 위치 정보에 기초하여 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 인증하는 인증 서버를 포함하며,

상기 인증이 성공적으로 완료되면 상기 진화된 패킷 데이터 게이트웨이는 상기 사용자 단말과 상기 사설망을 연결하고, 상기 사용자 단말은 상기 사설망과의 접속을 유지하기 위해 상기 사용자 단말의 위치 정보에 기초하여 상기 인증 서버와 재인증 절차를 수행하는 사용자 단말 접속 제어 시스템.

청구항 11

제10항에서,

상기 인증 서버는 상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된 지역의 위치 정보인 경우, 상기 진화된 패킷 데이터 게이트웨이로 인증 응답을 전송하는 사용자 단말 접속 제어 시스템.

청구항 12

제11항에서,

상기 사용자 단말의 위치 정보는

상기 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고,

상기 사설망으로 접속이 허용된 지역의 위치 정보는

상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함하는 사용자 단말 접속 제어 시스템.

청구항 13

제10항에서,

고객 관리 서버를 더 포함하고,

상기 사용자 단말은 상기 고객 관리 서버를 통해 재인증 요청을 상기 인증 서버로 전송하며,

상기 인증 서버는 상기 재인증 요청에 포함된 상기 사용자 단말의 위치 정보에 기초하여 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하고, 상기 재인증이 성공적으로 완료되면 상기 진화된 패킷 데이터 게이트웨이로 재인증 응답을 전송하고,

상기 재인증 응답을 수신하면, 상기 진화된 패킷 데이터 게이트웨이는 상기 사용자 단말과 상기 사설망의 접속을 유지하도록 하는 사용자 단말 접속 제어 시스템.

청구항 14

제13항에서,

상기 인증 서버는 상기 재인증 요청에 포함된 상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된

지역의 위치 정보인 경우, 상기 진화된 패킷 데이터 게이트웨이로 상기 재인증 응답을 전송하는 사용자 단말 접속 제어 시스템.

청구항 15

제14항에서,

상기 사용자 단말의 위치 정보는

상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고,

상기 사설망으로 접속이 허용된 지역의 위치 정보는

상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함하는 사용자 단말 접속 제어 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 비신뢰망을 통해 사설망으로 접속하는 사용자 단말의 접속을 제어하는 기술에 관한 것이다.

배 경 기 술

[0002] IMS 플랫폼을 통해 LTE망에서 ALL-IP 서비스를 제공하려는 시도가 지속적으로 이루어지고 있고, WiFi 네트워크 또한 비면허 대역을 이용한 무선통신 기술이라는 장점을 바탕으로 GiGA급 전송기술로의 고도화가 이루어지고 있다. 이에 따라, LTE와 WiFi 네트워크를 연동/병합할 필요성이 증가하고, 이를 위해 여러 기술들(LTE-A, LTE-U, LWA 및 MPTCP Proxy 등)이 시도되고 있다.

[0003] WiFi와 같은 비신뢰망에서 패킷 데이터 네트워크 게이트웨이(Packet Data Network Gateway, P-GW)에 연결된 사설망으로 접속하려면 신뢰망을 경유하여야 한다. 구체적으로, WiFi 액세스 포인트와 같은 비신뢰망 접속 장치를 통해 사설망으로 접속하려는 사용자 단말은 진화된 패킷 데이터 게이트웨이(Evolved Packet Data Gateway, ePDG)를 거쳐 신뢰망의 기지국으로 액세스한다. 이를 위해, 사용자 단말은 인증 서버와 상호 인증 과정을 수행하며, 인증 서버는 상호 인증에 성공한 경우 사용자 단말의 액세스를 허용한다.

[0004] 상호 인증 과정에서, 종래 기술은 SIM 기반의 인증방식(EAP-AKA 또는 EAP-SIM) 또는 EAP-MSCHAPv2 인증 방식을 통해 사용자 단말과 인증 서버간 상호 인증을 수행하였다.

[0005] 그러나, SIM 기반의 인증방식(예를 들어, EAP-AKA 또는 EAP-SIM 인증)은 통신사에 대한 종속성이 있어 B2B(Business to Business)를 대상으로 하는 서비스에서 사용될 경우 특정 사업자가 각기 다른 임직원의 통신사에 맞춰 서비스를 제공하기 어렵다는 문제가 있다.

[0006] 또한, 종래의 EAP-MSCHAPv2 방식은 사용자 단말의 위치정보(예를 들면, 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보)를 인증 서버로 전송할 수 없는바, 종업원이 비신뢰망을 통해 사설망으로 접속하는 경우, 어떤 액세스 포인트를 통해 접속하였는지, 어떤 지역에서 접속하였는지 결정하기 어려워 보안 측면에서 취약한 단점이 있었다.

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 과제는 사용자 단말의 위치 정보에 기초하여 사용자 단말의 사설망으로의 접속을 제어하는 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 사설망으로의 접속을 제어하는 방법은 비신뢰망 접속 장치에 접속한 사용자 단말로부터, 패킷 데이터 네트워크 게이트웨이(Packet Data Network Gateway, P-GW)에 연결된 사설망으로 접속하기 위한 접속 요청을 수신하는 단계, 상기 접속 요청에서 추출한 상

기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 인증하는 단계, 그리고 상기 인증이 성공적으로 완료되면, 상기 패킷 데이터 네트워크 게이트웨이를 통해 상기 사용자 단말이 상기 사설망으로 접속하도록 허용하는 단계를 포함한다.

[0009] 상기 인증하는 단계는 상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된 지역의 위치 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정한다.

[0010] 상기 사용자 단말의 위치 정보는 상기 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고, 상기 사설망으로 접속이 허용된 지역의 위치 정보는 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함한다.

[0011] 상기 사용자 단말 접속 제어 방법은 상기 사용자 단말로 재인증 요청을 전송하는 단계, 상기 사용자 단말로부터 상기 재인증 요청에 대응하는 재인증 응답을 수신하는 단계, 상기 재인증 응답에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고 상기 재인증이 성공적으로 완료되면, 상기 사용자 단말의 상기 사설망으로의 접속을 유지하도록 하는 단계를 더 포함한다.

[0012] 상기 재인증 응답에서 추출한 상기 사용자 단말의 위치 정보는 상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하며, 상기 재인증하는 단계는 상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정한다.

[0013] 상기 사용자 단말 접속 제어 방법은 상기 사용자 단말로부터 재인증 요청을 수신하는 단계, 상기 재인증 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고 상기 재인증이 성공적으로 완료되면, 상기 사용자 단말의 상기 사설망으로의 접속을 유지하도록 하는 단계를 더 포함한다.

[0014] 상기 재인증 요청에서 추출한 상기 사용자 단말의 위치 정보는 상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하며, 상기 재인증하는 단계는 상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정한다.

[0015] 상기 사용자 단말 접속 제어 방법은 상기 비신뢰망 접속 장치와는 다른 새로운 비신뢰망 접속 장치에 접속한 사용자 단말로부터, 상기 사설망으로 재접속하기 위한 재접속 요청을 수신하는 단계, 상기 재접속 요청에서 추출한 상기 사용자 단말의 위치 정보에 기초하여, 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하는 단계, 그리고 상기 재인증이 성공적으로 완료되면, 상기 사용자 단말이 상기 사설망으로 재접속하도록 하는 단계를 더 포함한다.

[0016] 상기 재접속 요청에서 추출한 상기 사용자 단말의 위치 정보는 상기 새로운 비신뢰망 접속 장치의 식별 정보 또는 상기 인증 이후 상기 사용자 단말의 GPS 정보를 포함하며, 상기 재인증하는 단계는 상기 새로운 비신뢰망 접속 장치의 식별 정보 또는 상기 인증 이후 상기 사용자 단말의 GPS 정보가 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보인 경우, 상기 사용자 단말의 인증이 성공적으로 완료된 것으로 결정한다.

[0017] 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템은 비신뢰망 접속 장치에 접속한 사용자 단말로부터 패킷 데이터 네트워크 게이트웨이에 연결된 사설망 접속을 위한 접속 요청을 수신하고, 상기 접속 요청에서 상기 사용자 단말의 위치 정보를 추출하는 진화된 패킷 데이터 게이트웨이(Evolved Packet Data Gateway, ePDG), 그리고 상기 진화된 패킷 데이터 게이트웨이로부터 상기 사용자 단말의 위치 정보를 포함하는 인증 요청을 수신하고, 상기 사용자 단말의 위치 정보에 기초하여 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 인증하는 인증 서버를 포함하며, 상기 인증이 성공적으로 완료되면, 상기 진화된 패킷 데이터 게이트웨이는 상기 사용자 단말과 상기 사설망을 연결한다.

[0018] 상기 인증 서버는 상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된 지역의 위치 정보인 경우, 상기 진화된 패킷 데이터 게이트웨이로 상기 인증 응답을 전송한다.

[0019] 상기 사용자 단말의 위치 정보는 상기 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고, 상기 사설망으로 접속이 허용된 지역의 위치 정보는 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함한다.

[0020] 상기 사용자 단말 접속 제어 시스템은 고객 관리 서버를 더 포함하고, 상기 사용자 단말은 상기 고객 관리 서버를 통해 재인증 요청을 상기 인증 서버로 전송하며, 상기 인증 서버는 상기 재인증 요청에 포함된 상기 사용자 단말의 위치 정보에 기초하여 상기 사용자 단말이 상기 사설망으로 접속이 허용된 단말인지 재인증하고, 상기 재인증이 성공적으로 완료되면 상기 진화된 패킷 데이터 게이트웨이로 재인증 응답을 전송하고, 상기 재인증 응답을 수신하면, 상기 진화된 패킷 데이터 게이트웨이는 상기 사용자 단말과 상기 사설망의 접속을 유지하도록 한다.

[0021] 상기 인증 서버는 상기 재인증 요청에 포함된 상기 사용자 단말의 위치 정보가 상기 사설망으로 접속이 허용된 지역의 위치 정보인 경우, 상기 진화된 패킷 데이터 게이트웨이로 상기 재인증 응답을 전송한다.

[0022] 상기 사용자 단말의 위치 정보는 상기 인증 이후 상기 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보 또는 상기 사용자 단말의 GPS 정보를 포함하고, 상기 사설망으로 접속이 허용된 지역의 위치 정보는 상기 사설망으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 상기 사설망으로 접속이 허용된 GPS 정보를 포함한다.

발명의 효과

[0023] 본 발명에 따르면, 사용자 단말의 위치 정보에 기초하여 사용자 단말의 접속을 제어함으로써, 더욱 정교한 보안 솔루션을 제공할 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 구현되는 환경을 도시하는 도면이다.

도 2는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 사설망으로의 접속을 제어하는 방법을 나타낸 흐름도이다.

도 3은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 EAP-MSCHAPv2 인증 방식을 통해 사용자 단말의 사설망으로의 접속을 제어하는 방법을 나타낸 흐름도이다.

도 4는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 환경을 도시하는 도면이다.

도 5는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

도 6은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 다른 방법을 나타낸 흐름도이다.

도 7은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 EAP-MSCHAPv2 인증 방식을 통해 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

도 8은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 핸드오버 발생시 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

도 9는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 고객 관리 서버와 연동하는 환경을 도시하는 도면이다.

도 10은 사용자 단말 접속 제어 시스템이 고객 관리 서버와 연동하여 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위

해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0026] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0027] 도 1은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 구현되는 환경을 도시하는 도면이다.

[0028] 도 1을 참고하면, 사용자 단말(100)은 IP(Internet Protocol)를 지원하는 운영 시스템(Operating System, OS), WiFi 모뎀, LTE 모뎀, LAN 등 IP 기반의 통신을 가능하게 하는 하드웨어를 포함하여, 인터넷에 접속이 가능한 단말이다.

[0029] 사용자 단말(100)은 비신뢰망 접속 장치(200)를 통해 패킷데이터 네트워크 게이트웨이(Packet Data Network Gateway, P-GW)(400)에 연결된 사설망(500)으로 접속을 시도한다.

[0030] 사용자 단말(100)은 사설망(500)으로 접속하기 위해, 전용 어플리케이션을 탑재하여 실행할 수 있고, 전용 어플리케이션은 스마트폰 앱, PC의 클라이언트 프로그램 등을 위한 응용 프로그램의 형태로 구현될 수 있다.

[0031] 사용자 단말(100)이 사설망(500)으로 접속을 시도하는 경우, 사용자 단말(100)은 진화된 패킷 데이터 게이트웨이(310)로 사설망(500)에 대한 접속을 요청한다. 이 경우, 접속 요청은 사용자 단말(100)의 위치 정보를 포함한다.

[0032] 사용자 단말(100)의 위치 정보는 비신뢰망 접속 장치(200)의 식별 정보 또는 사용자 단말(100)의 GPS 정보 중 적어도 하나를 포함할 수 있다.

[0033] 비신뢰망 접속 장치(200)는 비신뢰 접속망의 접속 장치로서, WiFi 액세스 포인트를 지칭할 수 있다.

[0034] 사용자 단말 접속 제어 시스템(300)은 진화된 패킷 데이터 게이트웨이(Evolved Packet Data Gateway, ePDG)(310) 및 인증 서버(320)를 포함한다.

[0035] 진화된 패킷 데이터 게이트웨이(310)는 3GPP에서 표준화된 네트워크 장치로서, 인증 서버(320) 및 패킷 데이터 네트워크 게이트웨이(400)와 연결된다.

[0036] 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)로부터 접속 요청을 수신하면, 접속 요청에서 사용자 단말(100)의 위치 정보를 추출하고, 사용자 단말(100)의 위치 정보를 포함하는 인증 요청을 인증 서버(320)로 전송한다.

[0037] 진화된 패킷 데이터 게이트웨이(310)는 인증 서버(320)에 의해 사용자 단말(100)의 인증이 성공적으로 완료되면, 사용자 단말(100)의 사설망(500)으로의 접속을 허용하는 접속 응답을 사용자 단말(100)로 전송한다.

[0038] 접속 응답을 수신한 사용자 단말(100)이 패킷 데이터 네트워크 게이트웨이(400)에 연결된 사설망(500)으로 접속 시, 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)과 패킷 데이터 네트워크 게이트웨이(400)에 연결된 사설망(500)을 연결한다.

[0039] 이 경우, 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)에서 패킷 데이터 네트워크 게이트웨이(400)에 연결된 사설망(500)으로 데이터를 이동시키는 게이트웨이 기능을 한다.

[0040] 인증 서버(320)는 사용자 단말(100)의 인증을 위한 인증 전용 서버로서, 진화된 패킷 데이터 게이트웨이(310)와 연결된다.

[0041] 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)로부터 수신한 사용자단말(100)의 위치 정보에 기초하여 사용자 단말(100)이 사설망(500)으로 접속이 허용된 단말인지 인증한다.

[0042] 구체적으로, 인증 서버(320)는 사설망(500)으로 접속이 허용된 사용자 단말의 위치 정보를 저장한다. 예를 들면, 인증 서버(320)는 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 사설망(500)으로 접속이 허용된 GPS 정보를 포함할 수 있다.

[0043] 인증 서버(320)는 사용자 단말(100)의 위치 정보가 사설망(500)으로 접속이 허용된 사용자 단말의 위치 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료되었음을 알리는 인증 응답을 진화된 패킷 데이터 게이트웨이

(310)로 전송한다.

[0044] 인증 응답을 수신한 진화된 패킷 데이터 게이트웨이(310)는 사설망(500)으로의 접속을 허용하는 접속 응답을 사용자 단말(100)로 전송한다.

[0045] 패킷 데이터 네트워크 게이트웨이(400)는 3GPP 표준 노드로서, 진화된 패킷 데이터 게이트웨이(310) 및 사설망(500)과 연결된다.

[0046] 패킷 데이터 네트워크 게이트웨이(400)는 사설망(500)을 위한 전용 P-GW일 수 있다.

[0047] 사설망(500)은 기업 인트라넷일 수 있다.

[0048] 이제, 도 2를 참고하여, 사용자 단말 접속 제어 시스템(300)이 사용자 단말(100)의 위치 정보에 기초하여 사용자 단말(100)의 사설망(500)으로의 접속을 허용하는 실시예를 설명한다.

[0049] 도 2는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 사설망으로의 접속을 제어하는 방법을 나타낸 흐름도이다.

[0050] 도 2를 참고하면, 비신뢰망 접속 장치를 통해 사설망으로 접속하려는 사용자는 사용자 단말(100)에 탑재된 전용 어플리케이션(미도시)을 실행하고 로그인한다(S100).

[0051] 로그인이 성공적으로 수행되면, 사용자 단말(100)은 기 저장된 사용자 단말(100)의 위치 정보를 획득하거나, 사용자가 로그인할 당시 사용자 단말(100)의 위치 정보를 획득한다.

[0052] 사용자 단말(100)의 위치 정보는 비신뢰망 접속 장치(200)의 식별 정보 또는 사용자 단말(100)의 GPS 정보 중 적어도 하나를 포함할 수 있다.

[0053] 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 획득하기 위해, 사용자 단말(100)에 탑재된 위치 어플리케이션을 실행하여 위치 정보를 수집할 수 있다.

[0054] 사용자 단말(100)은 진화된 패킷 데이터 게이트웨이(310)로 패킷 데이터 네트워크 게이트웨이(400)에 연결된 사설망(500) 접속을 위한 접속 요청을 전송한다(S110).

[0055] 접속 요청은 단계 S100에서 획득한 사용자 단말(100)의 위치 정보를 포함한다. 구체적으로, 사용자 단말(100)이 접속 요청으로서 접속 요청 메시지를 진화된 패킷 데이터 게이트웨이(310)로 전송하는 경우, 사용자 단말(100)은 접속 요청 메시지의 비어있는 슬롯(slot) 상에 사용자 단말(100)의 위치 정보 데이터를 포함시킬 수 있다.

[0056] 또한, 접속 요청은 사설망(500)으로 접속하기 위해 사용자 단말(100)의 인증이 필요한지 여부를 알리는 정보를 포함할 수 있다. 이러한 정보는 사용자 단말(100)이 진화된 패킷 데이터 게이트웨이(310) 및 인증 서버(320)와 이미 인증 과정을 수행하였는지 여부를 표시하는 정보를 포함할 수 있다.

[0057] 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)의 접속 요청을 분석하여 사용자 단말(100)의 인증이 필요한지 여부를 확인하고, 인증이 필요한 경우 인증 요청을 인증 서버(320)로 전송한다(S120).

[0058] 이 때, 진화된 패킷 데이터 게이트웨이(310)는 접속 요청에서 사용자 단말(100)의 위치 정보를 추출하고, 추출한 위치 정보를 인증 요청에 포함시킨다.

[0059] 인증 서버(320)는 인증 요청에 포함된 사용자 단말(100)의 위치 정보에 기초하여, 사용자 단말(100)이 사설망(500)으로 접속이 허용된 단말인지 인증한다(S130).

[0060] 구체적으로, 인증 서버(320)는 사용자 단말(100)의 위치 정보가 사설망(500)으로 접속이 허용된 지역의 위치 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정한다.

[0061] 예를 들면, 사용자 단말(100)의 위치 정보는 비신뢰망 접속 장치(200)의 식별 정보 및/또는 사용자 단말(100)의 GPS 정보를 포함할 수 있다. 이 경우, 인증 서버(320)는 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 사설망(500)으로 접속이 허용된 GPS 정보를 사설망(500)으로 접속이 허용된 지역의 위치 정보로서 저장할 수 있다.

[0062] 이 때, 인증 서버(320)는 비신뢰망 접속 장치(200)의 식별 정보 및/또는 사용자 단말(100)의 GPS 정보가 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 사설망(500)으로 접속이 허용된 GPS 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정할 수 있다.

[0063] 사용자 단말(100)의 인증이 성공적으로 완료되면, 인증 서버(320)는 사용자 단말(100)의 인증이 성공적으로 완료되었음을 알리는 인증 응답을 진화된 패킷 데이터 게이트웨이(310)로 전송한다(S140).

[0064] 인증 응답을 수신한 진화된 패킷 데이터 게이트웨이(310)는 사설망(500)으로의 접속을 허용하는 접속 응답을 사용자 단말(100)로 전송한다(S150). 이 경우, 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)과 패킷 데이터 네트워크 게이트웨이(400)에 연결된 사설망(500)을 연결한다.

[0065] 도 2에서, 사용자 단말(100)은 사용자 단말(100)의 단말 식별 정보 및 사용자 단말(100)의 사용자 식별 정보를 추가로 획득할 수 있다.

[0066] 예를 들면, 사용자 단말(100)은 단말 설정 상에 저장된 정보로부터 사용자 단말(100)의 단말 식별 정보를 획득할 수 있다. 또한, 사용자 단말(100)은 사용자 단말(100)의 보안을 위해 저장된 사용자의 생체인식 정보(예를 들면, 지문 등)를 사용자 식별 정보로서 획득할 수 있다.

[0067] 사용자 단말(100)은 단말 식별 정보 및 사용자 식별 정보를 접속 요청에 추가로 포함시킬 수 있다.

[0068] 이 경우, 인증 서버(320)는 사설망(500)으로의 접속이 허용된 단말의 단말 식별 정보 및 사용자 식별 정보를 추가로 저장한다.

[0069] 또한, 인증 서버(320)는 사용자 단말(100)의 단말 식별 정보 및 사용자 식별 정보가 사설망(500)으로의 접속이 허용된 단말의 단말 식별 정보 및 사용자 식별 정보와 각각 대응되는지 추가적으로 확인하여, 위치 정보, 단말 식별 정보 및 사용자 식별 정보가 모두 대응하는 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정할 수 있다.

[0070] 도 3은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 EAP-MSCHAPv2 인증 방식을 통해 사용자 단말의 사설망으로의 접속을 제어하는 방법을 나타낸 흐름도이다.

[0071] 비록 도 3에서는 사용자 단말 접속 제어 시스템(300)이 사용자 단말(100)의 접속을 제어하는 방법을 구체적으로 설명하기 위해 EAP-MSCHAPv2 인증방식에 한정하였으나, 다른 인증방식을 통해 사용자 단말(100)의 접속을 제어할 수 있다.

[0072] 도 3을 참고하면, 비신뢰망 접속 장치(200)를 통해 사설망(500)으로 접속하려는 사용자는 사용자 단말(100)에 탑재된 전용 어플리케이션을 실행하고 EAP-MSCHAPv2 인증을 위해 필요한 아이디 및 패스워드를 이용하여 로그인한다(S200).

[0073] 로그인이 성공적으로 완료되면, 사용자 단말(100)은 진화된 패킷 데이터 게이트웨이(310)로 사설망(500)에 대한 접속 요청을 전송한다(S210).

[0074] 사용자 단말 접속 제어 시스템(300)이 접속 요청을 수신하면, 사용자 단말(100)과 진화된 패킷 데이터 게이트웨이(310)는 초기 암호화를 수행하기 위해, IKEv2_SA_INIT를 교환한다(S220).

[0075] IKEv2_SA_INT 메시지 교환을 통해, IKE 메시지 보호에 필요한 IKE_SA를 생성하며, 교환 이후 모든 메시지는 IKEv2_SA_INIT 교환에서 협상된 암호화 알고리즘 및 키를 사용하여 암호로 보호된다.

[0076] IKE_SA를 생성한 후, 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 포함한 IKEv2_AUTH_REQ 메시지를 진화된 패킷 데이터 게이트웨이(310)로 전송한다(S230).

[0077] 구체적으로, 사용자 단말(100)은 기 저장된 사용자 단말(100)의 위치 정보를 획득하거나, 사용자가 로그인할 당시 사용자 단말(100)의 위치 정보를 획득한다.

[0078] 사용자 단말(100)의 위치 정보는 비신뢰망 접속 장치(200)의 식별 정보 또는 사용자 단말(100)의 GPS 정보 중 적어도 하나를 포함할 수 있다.

[0079] 이 후, 사용자 단말(100)은 IKEv2_AUTH_REQ 메시지에 포함된 IDi(Identification - Initiator)의 데이터 포맷을 변경하여 IDi에 사용자 단말(100)의 위치 정보를 추가한다.

[0080] 구체적으로, EAP-MSCHAPv2에서 IDi값은 NAI 포맷을 따르며, NAI에 대한 넘버링 규정 및 포맷은 3GPP TS23.003에 정의되어 있다. TS23.003에서 정의하는 IDi의 포맷은 다음과 같다.

[0081] *<IMSI>nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

[0082] 사용자 단말(100)은 위와 같은 IDi 포맷에 ACCESS POINT INFORMATION 섹션을 추가하고, 추가된 섹션에 사용자

단말(100)의 위치 정보의 데이터 값을 포함시킨다. 추가 데이터가 포함된 IDi의 포맷은 다음과 같다.

[0083] *<IMSI>@LOCATION INFORMATION: nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

[0084] 추가 데이터가 포함된 IDi의 포맷은 다음의 규칙을 따른다.

[0085] 추가 데이터 값은 nai앞에 위치한다.

[0086] 만일 사용자 단말(100)의 접속 정보의 데이터 값이 추가적으로 포함된 경우, 비신뢰망 접속 장치(200)의 식별 정보의 데이터 값과 사용자 단말(100)의 접속 정보의 데이터 값은"_"을 이용하여 구분한다.

[0087] 추가된 데이터 값은 ":"으로 끝난다.

[0088] 예를 들면, 사용자 단말(100)의 위치 정보로서 비신뢰망 접속 장치(200)의 식별 정보와 사용자 단말(100)의 GPS 정보가 포함된 경우, IDi의 포맷은 다음과 같은 포맷을 예시로 가질 수 있다.

[0089] *<IMSI>@12-45-67-89_3735.0079.6646: nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

[0090] 상기 예시에서 추가된 데이터 값 "12-45-67-89_3735.0079.6646"을 살펴보면, 전단의 "12-45-67-89"는 비신뢰망 접속 장치(200)의 식별 정보에 대한 데이터 값의 예시이며, 후단의 "3735.0079.6646"은 사용자 단말(100)의 GPS 정보에 대한 데이터 값의 예시이다. 사용자 단말(100)이 접속한 비신뢰망 접속 장치(200)의 식별 정보에 대한 데이터 값과 사용자 단말(100)의 GPS 정보에 대한 데이터 값은"_"로 구분한다.

[0091] 이 후, 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 포함한 IKEv2_AUTH_REQ 메시지를 진화된 패킷 데이터 게이트웨이(310)에 전송한다.

[0092] IKEv2_AUTH_REQ 메시지를 수신한 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)의 위치 정보를 추출하고, 사용자 단말(100)의 위치 정보를 포함하는 DER 메시지를 인증 서버(320)로 전송한다(S240).

[0093] 인증 서버(320)는 DER 메시지에 포함된 사용자 단말(100)의 위치 정보에 기초하여, 사용자 단말(100)이 사설망(500)으로 접속이 허용된 단말인지 인증한다(S250).

[0094] 구체적으로, 인증 서버(320)는 EAP-MSCHAPv2 인증 방식으로 사용자 단말(100)과 상호 인증 과정을 수행하되, 사용자 단말(100)의 위치 정보와 사설망(500)으로의 접속이 허용된 위치 정보가 대응하는지 추가적으로 결정한다.

[0095] 만일 사용자 단말(100)의 위치 정보가 사설망(500)으로 접속이 허용된 지역의 위치 정보인 경우, 인증 서버(320)는 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정한다.

[0096] 사용자 단말(100)의 위치 정보가 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 또는 사용자 단말(100)의 GPS 정보를 포함하는 상기 예시에서, 인증 서버(320)는 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 및/또는 사용자 단말(100)의 GPS 정보가 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 사설망(500)으로 접속이 허용된 GPS 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정할 수 있다.

[0097] 사용자 단말(100)의 인증이 성공적으로 완료되면, 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)로 DEA 메시지를 전송한다(S260).

[0098] DEA 메시지를 수신한 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)로 IKEv2_AUTH_RESP 메시지를 전송한다(S270). 상기 단계들을 통해, 사용자 단말(100)과 인증 서버(320) 사이에 EAP-MSCHAPv2를 통한 상호 인증 절차가 완료된다.

[0099] 상호 인증 절차가 완료되면 사용자 단말(100)과 진화된 패킷 데이터 게이트웨이(310) 사이에 IPSec 터널이 생성되고, 진화된 패킷 데이터 게이트웨이(310)와 패킷 데이터 네트워크 게이트웨이(400) 사이에 GRE 터널 또는 GTP 터널이 생성된다(S280).

[0100] 터널이 생성되면, 사용자 단말(100)은 생성된 터널을 통해 사설망(500)과 데이터를 송수신한다(S290).

[0101] 이제, 도 4 내지 도 10을 참고하여, 사용자 단말 접속 제어 시스템(300)이 사용자 단말(100)의 위치 정보에 기초하여 사용자 단말(100)의 재인증을 수행하는 실시예를 설명한다.

[0102] 도 4는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 환경을 도시하는 도면이다.

[0103] 도 1 내지 도 3에 따라 사용자 단말(100)의 사설망(500)으로의 접속이 허용된 경우에도, 사용자 단말 접속 제어 시스템(300)은 사용자 단말(100)을 재인증함으로써, 사용자 단말(100)의 사설망(500)으로의 접속을 실시간으로 제어할 수 있다.

[0104] 도 4를 참고하면, 제1 비신뢰망 접속 장치(210)를 통해 사설망(500)으로 접속한 사용자 단말(100)은 사용자가 이동함에 따라 제1 비신뢰망 접속 장치(210)와의 연결을 해제하고, 제2 비신뢰망 접속 장치(220)를 통해 사설망(500)으로 접속할 수 있다.

[0105] 이 경우, 사용자 단말(100)은 사설망(500)과의 접속을 유지하기 위해 재인증 절차를 거칠 수 있고, 재인증이 성공적으로 완료되면 사용자 단말(100)과 사설망(500)과의 접속이 유지된다.

[0106] 또한, 사용자 단말(100)은 사용자 단말(100) 또는 인증 서버(320)에 설정된 주기마다 재인증 절차를 거칠 수 있고, 재인증이 성공적으로 완료되면 사용자 단말(100)과 사설망(500)과의 접속이 유지된다.

[0107] 도 5는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

[0108] 도 5를 참고하면, 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)를 통해 사용자 단말(100)로 재인증 요청을 전송한다(S300).

[0109] 한 실시예에서, 인증 서버(320)는 재인증 요청을 사용자 단말(100)로 주기적으로 전송할 수 있다.

[0110] 재인증 요청을 수신한 사용자 단말(100)은 진화된 패킷 데이터 게이트웨이(310)를 통해 인증 서버(320)로 사용자 단말(100)의 위치 정보를 포함하는 재인증 응답을 전송한다(S310).

[0111] 구체적으로, 사용자 단말(100)은 최초 인증 이후 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 또는 사용자 단말(100)의 GPS 정보를 사용자 단말(100)의 위치 정보로서 획득할 수 있다.

[0112] 또한, 사용자 단말(100)은 재인증 응답의 비어있는 슬롯 상에 획득한 위치 정보를 포함시킬 수 있다.

[0113] 인증 서버(320)는 재인증 응답에 포함된 사용자 단말(100)의 위치 정보에 기초하여, 사용자 단말(100)이 사설망(500)으로 접속이 허용된 단말인지 재인증한다(S320).

[0114] 예를 들면, 인증 서버(320)는 재인증 응답에서 추출한 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 또는 사용자 단말(100)의 GPS 정보가 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 GPS 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정한다.

[0115] 사용자 단말(100)의 재인증이 성공적으로 완료되면, 인증 서버(320)는 사용자 단말(100)의 사설망(500)으로의 접속을 유지한다. 이 경우, 사용자 단말(100)은 기존에 생성된 터널을 통해 사설망(500)과 데이터를 계속 송수신한다(S330).

[0116] 도 6은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 사용자 단말의 재인증을 수행하는 다른 방법을 나타낸 흐름도이다.

[0117] 도 6을 참고하면, 사용자 단말(100)은 진화된 패킷 데이터 게이트웨이(310)를 통해 인증 서버(320)로 사용자 단말(100)의 위치 정보를 포함하는 재인증 요청을 전송한다(S400).

[0118] 한 실시예에서, 사용자 단말(100)은 주기적으로 재인증 요청을 인증 서버(320)로 전송할 수 있다.

[0119] 다른 실시예에서, 사용자 단말(100)에 핸드오버가 발생하여 사용자 단말(100)이 다른 비신뢰망 접속 장치에 접속한 경우, 사용자 단말(100)은 접속한 비신뢰망 접속 장치가 변경된 것을 알리는 메시지를 재인증 요청으로서 인증 서버(320)로 전송할 수 있다.

[0120] 또한, 사용자 단말(100)은 도 5에서 설명한 방법으로 사용자 단말(100)의 위치 정보를 획득하고, 획득한 위치 정보를 재인증 요청에 포함시킬 수 있다.

[0121] 인증 서버(320)는 도 5에서 설명한 방법으로 사용자 단말(100)의 재인증 절차를 수행한다(S410).

[0122] 사용자 단말(100)의 재인증이 성공적으로 완료되면, 인증 서버(320)는 사용자 단말로 사설망(500)으로의 접속이 유지됨을 알리는 재인증 응답을 전송한다(S420). 이 경우, 사용자 단말(100)은 기존에 생성된 터널을 통해 사설망(500)과 데이터를 계속 송수신한다(S430).

[0123] 도 7은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 EAP-MSCHAPv2 인증 방식을 통해 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

[0124] 비록 도 7에서는 사용자 단말 접속 제어 시스템(300)이 사용자 단말(100)의 재인증을 수행하는 방법을 구체적으로 설명하기 위해 EAP-MSCHAPv2 인증방식에 한정하였으나, 다른 인증방식을 통해 사용자 단말(100)의 재인증을 수행할 수 있다.

[0125] 도 7을 참고하면, 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 포함하는 IKEv2 INFORMATIONAL Exchange Request 메시지를 진화된 패킷 데이터 게이트웨이(310)로 전송한다(S500).

[0126] 구체적으로, 사용자 단말(100)은 최초 인증 이후 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 또는 사용자 단말(100)의 GPS 정보를 사용자 단말(100)의 위치 정보로서 획득할 수 있다.

[0127] 이후, 사용자 단말(100)은 획득한 위치 정보를 IKEv2 INFORMATIONAL Exchange Request 메시지에 포함시킨다.

[0128] 구체적으로, 사용자 단말 접속 제어 시스템(300)이 IKE 프로토콜을 이용하는 경우, IKEv2의 공급자 아이디 페이로드(Vendor ID Payload)는 IKEv2의 모든 메시지에 포함될 수 있다. 따라서, 사용자 단말(100)은 사용자 단말(100)의 식별 정보의 데이터 포맷을 변경하여 사용자 단말(100)의 식별 정보에 사용자 단말(100)의 업데이트된 위치 정보를 추가할 수 있다. 나아가, 사용자 단말(100)은 사용자 단말(100)의 식별 정보를 공급자 아이디 페이로드에 실어 IKEv2 정보 교환 요청 메시지에 포함시킬 수 있다.

[0129] 진화된 패킷 데이터 게이트웨이(310)는 IKEv2 INFORMATIONAL Exchange Request 메시지에서 사용자 단말(100)의 위치 정보를 추출하고, 추출된 위치 정보가 포함된 Re-Auth-Request 메시지를 인증 서버(320)로 전송한다(S510).

[0130] 인증 서버(320)는, 도 5에서 설명한 방법으로, Re-Auth-Request 메시지에 포함된 사용자 단말(100)의 위치 정보에 기초하여, 사용자 단말(100)이 사설망(500)으로 접속이 허용된 단말인지 재인증한다(S520).

[0131] 사용자 단말(100)의 재인증이 성공적으로 완료되면, 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)로 Re-Auth-Answer 메시지를 전송한다(S530).

[0132] 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)로 IKEv2 INFORMATIONAL Exchange Answer 메시지를 전송한다(S540).

[0133] 이 경우, 사용자 단말은 기존에 생성된 터널을 통해 사설망(500)과 데이터를 계속 송수신한다(S550).

[0134] 도 8은 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 핸드오버 발생시 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

[0135] 사용자 단말(100)이 새로운 비신뢰망 접속 장치를 통해 사설망으로 접속하는 경우, MOBIKE에 의해 핸드오버가 발생한다(S600).

[0136] 이 경우, 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 획득하고, 도 7에서 설명한 방법으로 획득한 위치 정보를 MOBIKE 메시지에 포함시킨다.

[0137] 사용자 단말(100)의 위치 정보는 새로운 비신뢰망 접속 장치의 식별 정보 또는 최초 인증 이후 사용자 단말(100)의 GPS 정보를 포함할 수 있다.

[0138] 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 포함하는 MOBIKE 메시지를 재접속 요청으로서 진화된 패킷 데이터 게이트웨이(310)로 전송한다(S610).

[0139] 진화된 패킷 데이터 게이트웨이(310)는 MOBIKE 메시지에서 사용자 단말(100)의 위치 정보를 추출하고, 사용자 단말(100)의 위치 정보를 포함하는 Re-AUTH-Request 메시지를 인증 서버(320)로 전송한다(S620).

[0140] 인증 서버(320)는 Re-AUTH-Request 메시지에 포함된 사용자 단말(100)의 위치 정보에 기초하여, 사용자 단말(100)의 재인증 절차를 수행한다(S630).

[0141] 구체적으로, 인증 서버(320)는 새로운 비신뢰망 접속 장치의 식별 정보 또는 최초 인증 이후 사용자 단말(100)의 GPS 정보가 사설망(500)으로 접속이 허용된 비신뢰망 접속 장치의 식별 정보 또는 GPS 정보인 경우, 사용자 단말(100)의 인증이 성공적으로 완료된 것으로 결정한다.

[0142] 사용자 단말(100)의 재인증이 성공적으로 완료되면, 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)로

Re-AUTH-Answer 메시지를 전송한다(S640).

[0143] 이 경우, 사용자 단말(100)이 새로운 비신뢰망 접속 장치에 대해 사용자 단말(100)과 진화된 패킷 데이터 게이트웨이(310) 사이에 IPSec 터널이 생성되고, 진화된 패킷 데이터 게이트웨이(310)와 패킷 데이터 네트워크 게이트웨이(400) 사이에 GRE 터널 또는 GTP 터널이 생성된다(S650). 상기 과정을 통해, 사용자 단말(100)은 사설망(500)에 재접속한다.

[0144] 터널이 생성되면, 사용자 단말(100)은 생성된 터널을 통해 사설망(500)과 데이터를 송수신한다(S660).

[0145] 도 9는 본 발명의 한 실시예에 따른 사용자 단말 접속 제어 시스템이 고객 관리 서버와 연동하는 환경을 도시하는 도면이다.

[0146] 도 9를 참고하면, 고객 관리 서버(600)는 사용자 단말(100) 및 인증 서버(320)와 데이터 전송 프로토콜을 통해 연결된다. 예를 들면, 고객 관리 서버(600)는 사용자 단말(100) 및 인증 서버(320)와 IKEv2 프로토콜과 같은 인증 프로토콜이 아닌 HTTPS 프로토콜을 통해 연결될 수 있다.

[0147] 도 10은 사용자 단말 접속 제어 시스템이 고객 관리 서버와 연동하여 사용자 단말의 재인증을 수행하는 방법을 나타낸 흐름도이다.

[0148] 사용자 단말(100)은 사용자 단말(100)의 위치 정보를 포함하는 재인증 요청을 고객 관리 서버(600)를 통해 인증 서버(320)로 전송한다(S700).

[0149] 구체적으로, 사용자 단말(100)은 최초 인증 이후 사용자 단말(100)이 접속한 비신뢰망 접속 장치의 식별 정보 또는 사용자 단말(100)의 GPS 정보를 사용자 단말(100)의 위치 정보로서 획득할 수 있다.

[0150] 또한, 사용자 단말(100)은 도 5에서 설명한 방법으로, 획득한 위치 정보를 재인증 응답에 포함시킬 수 있다.

[0151] 고객 관리 서버(600)는 사용자 단말(100)의 위치 정보를 저장함으로써, 사용자 단말(100)의 실시간 이용 정보를 저장할 수 있다.

[0152] 인증 서버(320)는 도 5에서 설명한 방법으로 사용자 단말(100)의 재인증 절차를 수행한다(S710).

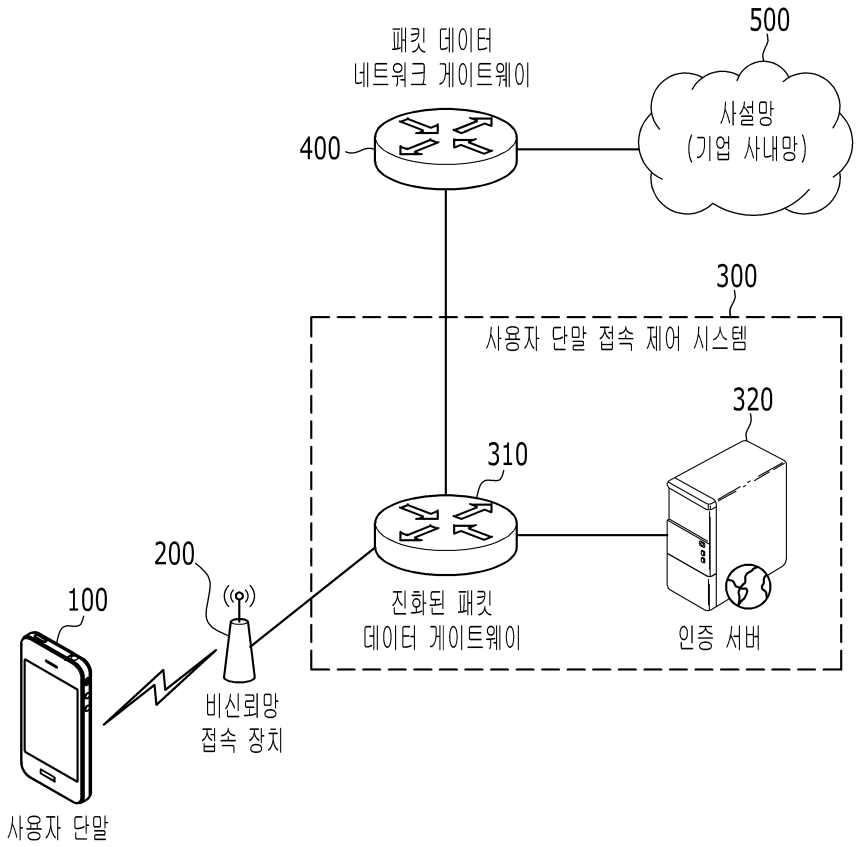
[0153] 사용자 단말(100)의 재인증이 성공적으로 완료되면, 인증 서버(320)는 진화된 패킷 데이터 게이트웨이(310)로 재인증 성공을 알리는 재인증 응답 메시지를 전송한다(S720). 이 경우, 진화된 패킷 데이터 게이트웨이(310)는 사용자 단말(100)과 사설망(500)의 접속을 유지하며, 사용자 단말(100)은 기존에 생성된 터널을 통해 사설망(500)과 데이터를 계속 송수신한다(S730).

[0154] 본 발명에 따르면, 사용자 단말이 접속한 비신뢰망 접속 장치의 식별 정보에 기초하여 사용자 단말의 인증/재인증 과정을 수행함으로써, 더욱 정교한 보안 솔루션을 제공할 수 있다.

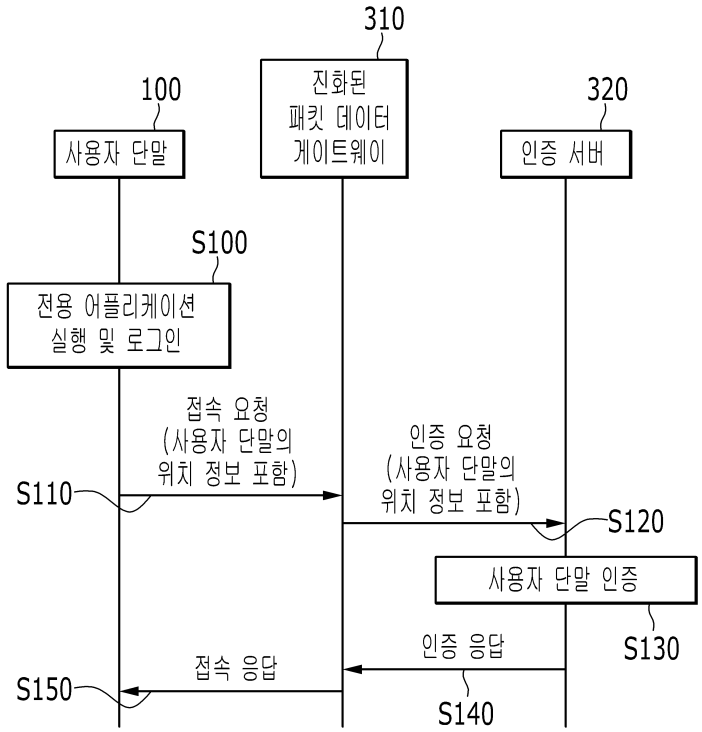
[0155] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

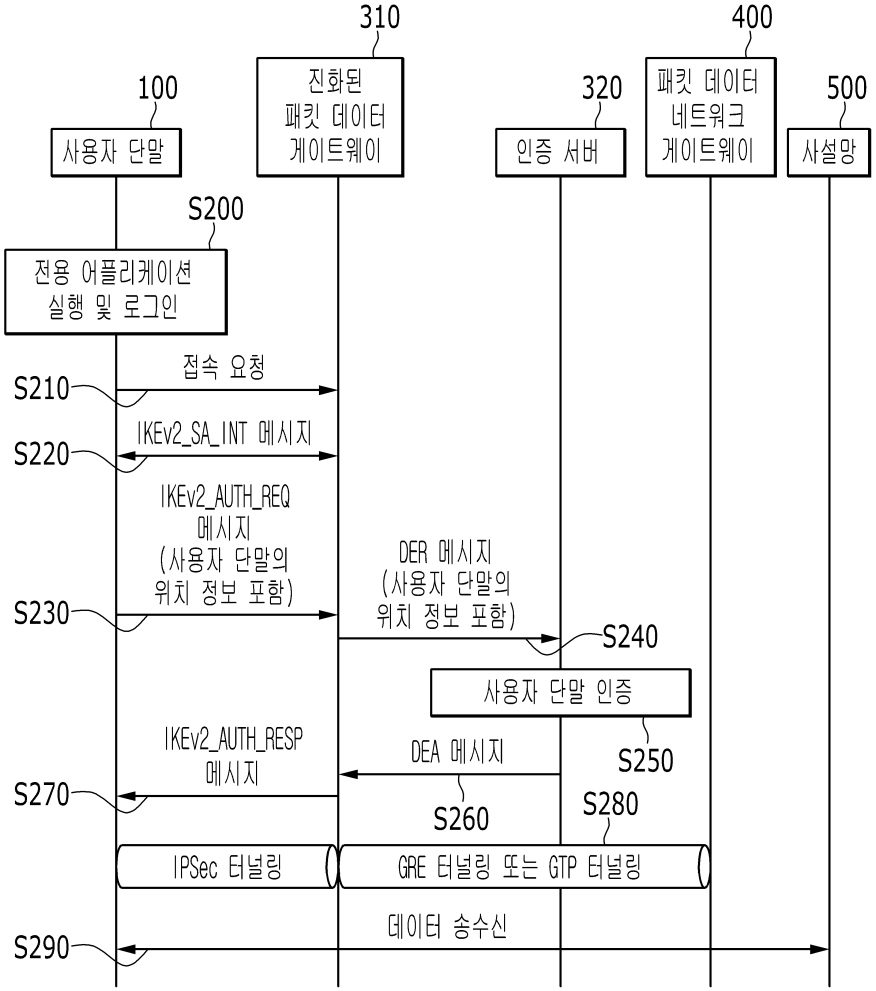
도면1


패킷 데이터
네트워크 게이트웨이
400
500
사설망
(기업 사내망)
300
사용자 단말 접속 제어 시스템
320
310
200
100
진화된 패킷
데이터 게이트웨이
인증 서버
비신뢰망
접속 장치
사용자 단말

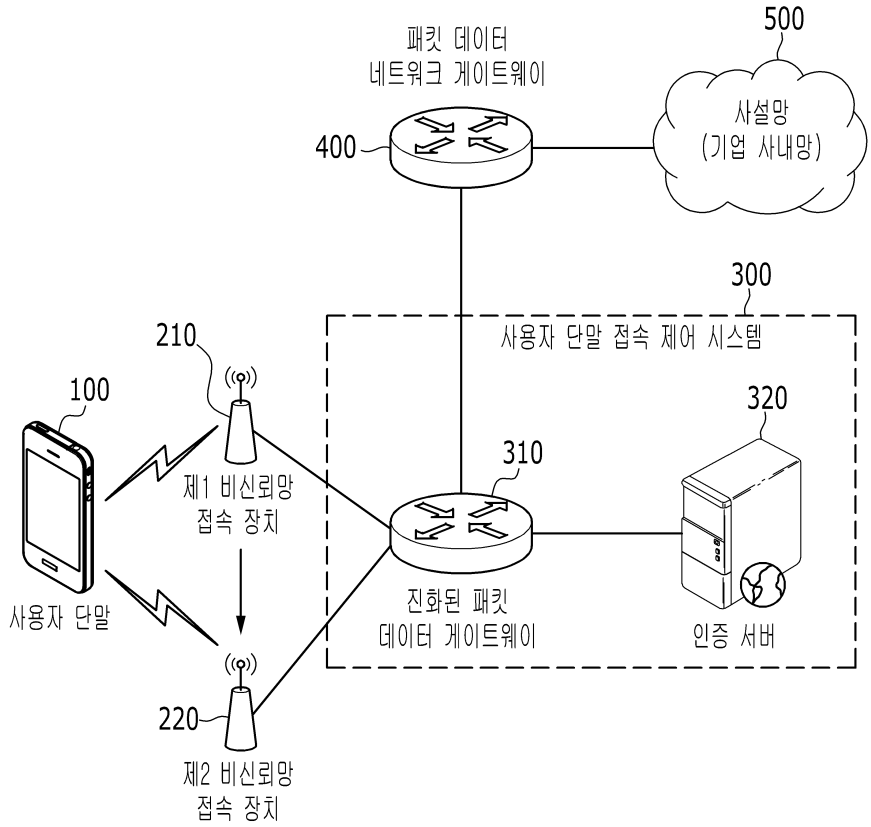
도면2


310
진화된
패킷 데이터
게이트웨이
100
사용자 단말
320
인증 서버
S100
전용 어플리케이션
실행 및 로그인
접속 요청
(사용자 단말의
위치 정보 포함)
S110
인증 요청
(사용자 단말의
위치 정보 포함)
S120
사용자 단말 인증
S130
인증 응답
S140
접속 응답
S150

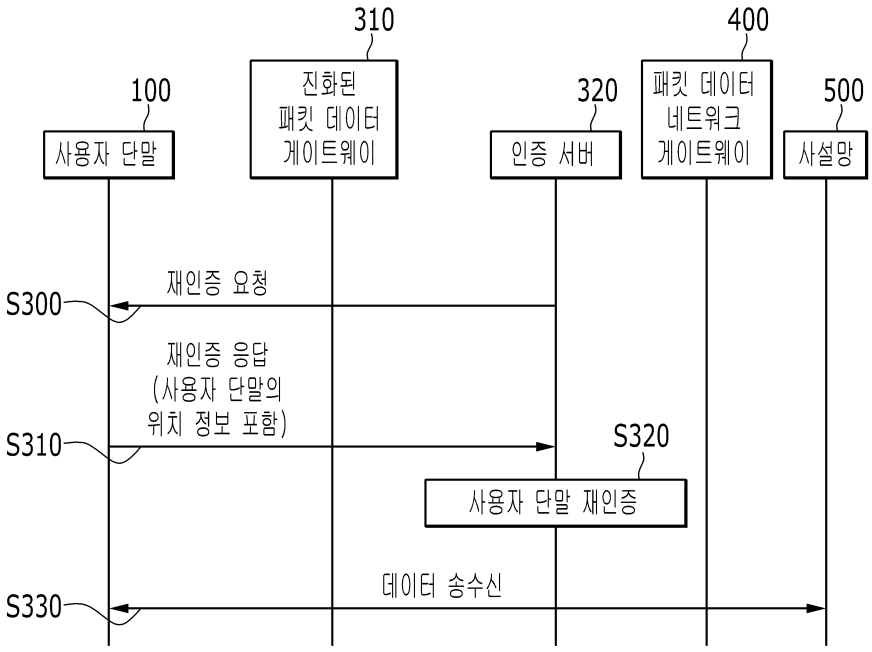
도면3


310
400
100
진화된
패킷 데이터
게이트웨이
320
패킷 데이터
네트워크
게이트웨이
500
사용자 단말
인증 서버
사설망
S200
전용 어플리케이션
실행 및 로그인
접속 요청
S210
IKEv2_SA_INT 메시지
S220
IKEv2_AUTH_REQ
메시지
(사용자 단말의
위치 정보 포함)
DER 메시지
(사용자 단말의
위치 정보 포함)
S230
S240
사용자 단말 인증
S250
IKEv2_AUTH_RESP
메시지
DEA 메시지
S270
S260
S280
IPSec 터널링
GRE 터널링 또는 GTP 터널링
데이터 송수신
S290

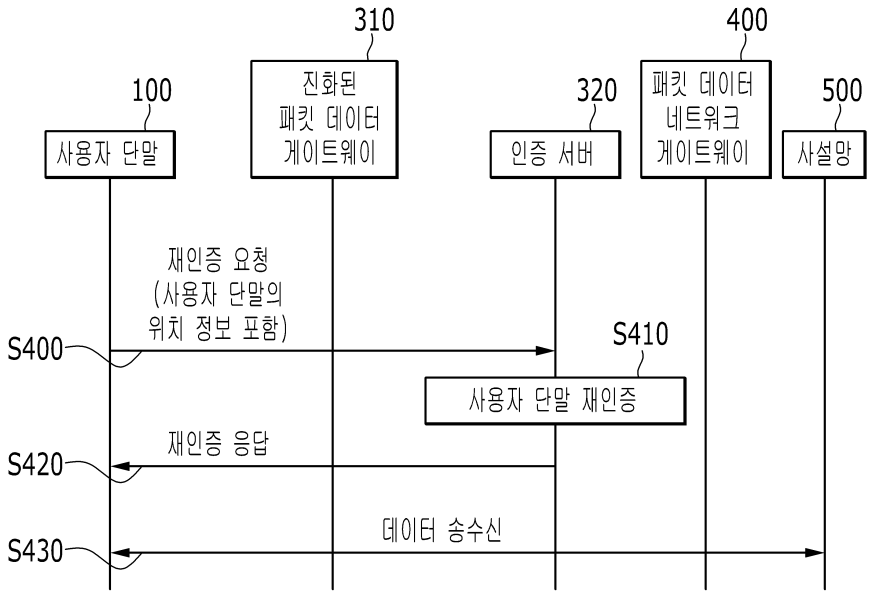
도면4


패킷 데이터
네트워크 게이트웨이
400
500
사설망
(기업 사내망)
300
사용자 단말 접속 제어 시스템
210
100
320
310
제1 비신뢰망
접속 장치
사용자 단말
진화된 패킷
데이터 게이트웨이
인증 서버
220
제2 비신뢰망
접속 장치

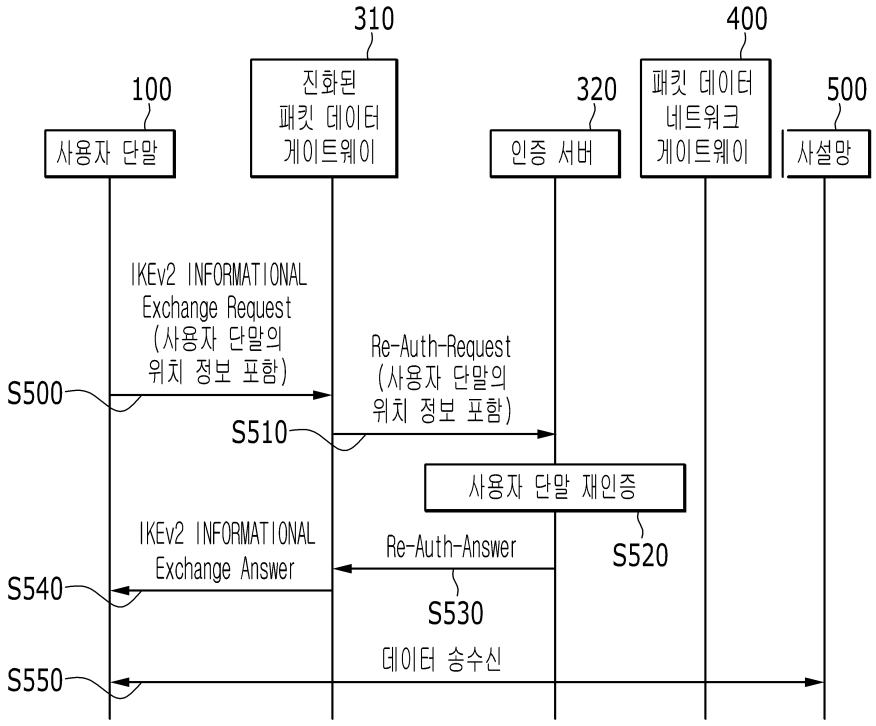
도면5


310
400
100
진화된
패킷 데이터
게이트웨이
320
패킷 데이터
네트워크
게이트웨이
500
사용자 단말
인증 서버
사설망
재인증 요청
S300
재인증 응답
(사용자 단말의
위치 정보 포함)
S310
S320
사용자 단말 재인증
데이터 송수신
S330

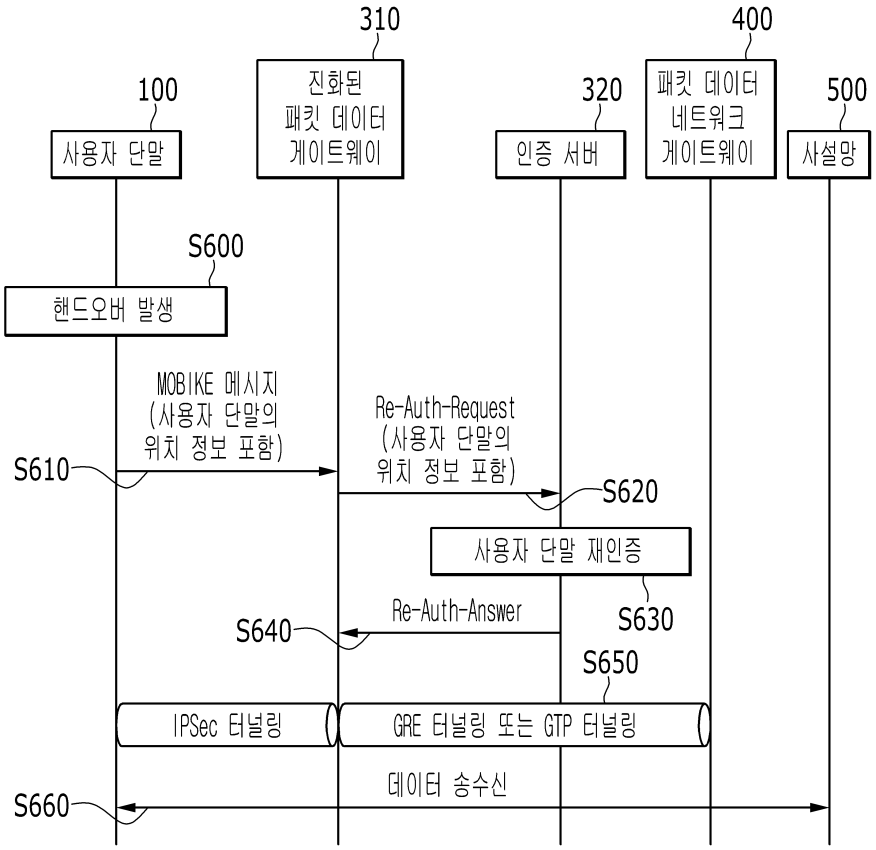
도면6


310
400
100
진화된
패킷 데이터
게이트웨이
320
패킷 데이터
네트워크
게이트웨이
500
사용자 단말
인증 서버
사설망
재인증 요청
(사용자 단말의
위치 정보 포함)
S400
S410
사용자 단말 재인증
재인증 응답
S420
데이터 송수신
S430

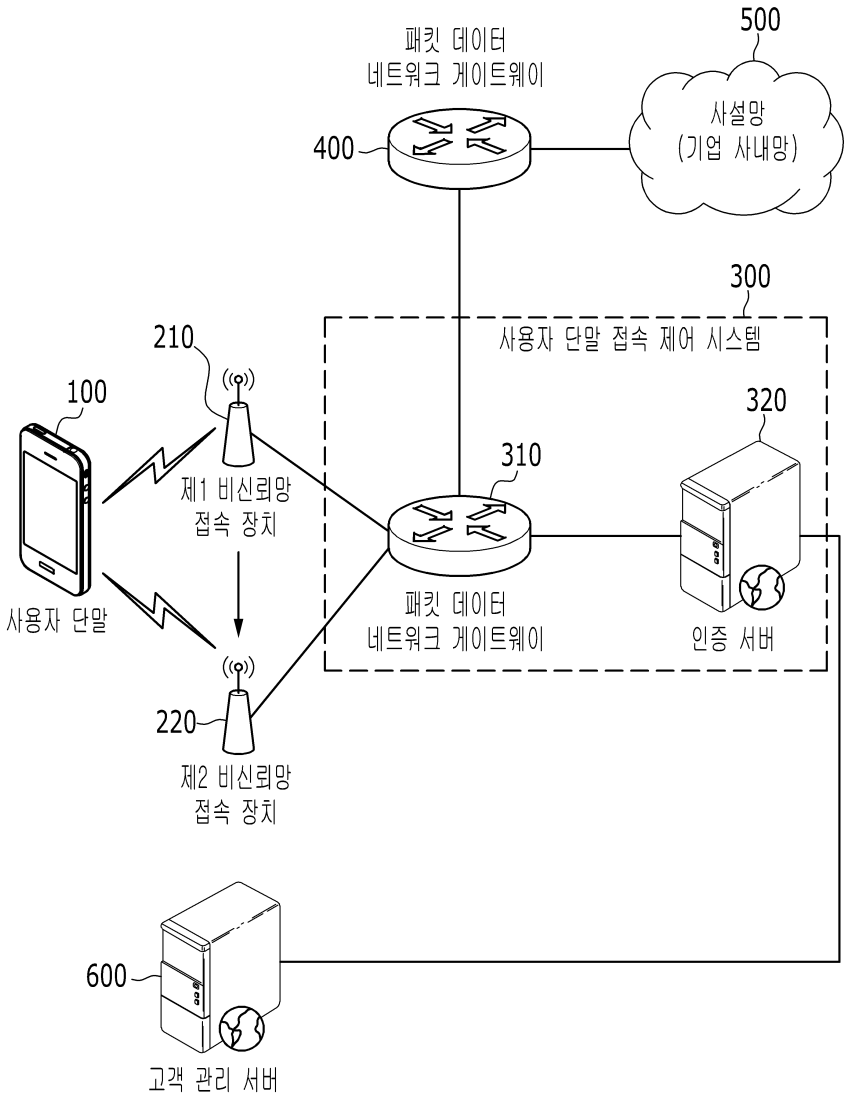
도면7


310
400
100
진화된
패킷 데이터
게이트웨이
320
패킷 데이터
네트워크
게이트웨이
500
사용자 단말
인증 서버
사설망
IKEv2 INFORMATIONAL
Exchange Request
(사용자 단말의
위치 정보 포함)
Re-Auth-Request
(사용자 단말의
위치 정보 포함)
S500
S510
사용자 단말 재인증
S520
IKEv2 INFORMATIONAL
Exchange Answer
Re-Auth-Answer
S530
S540
데이터 송수신
S550

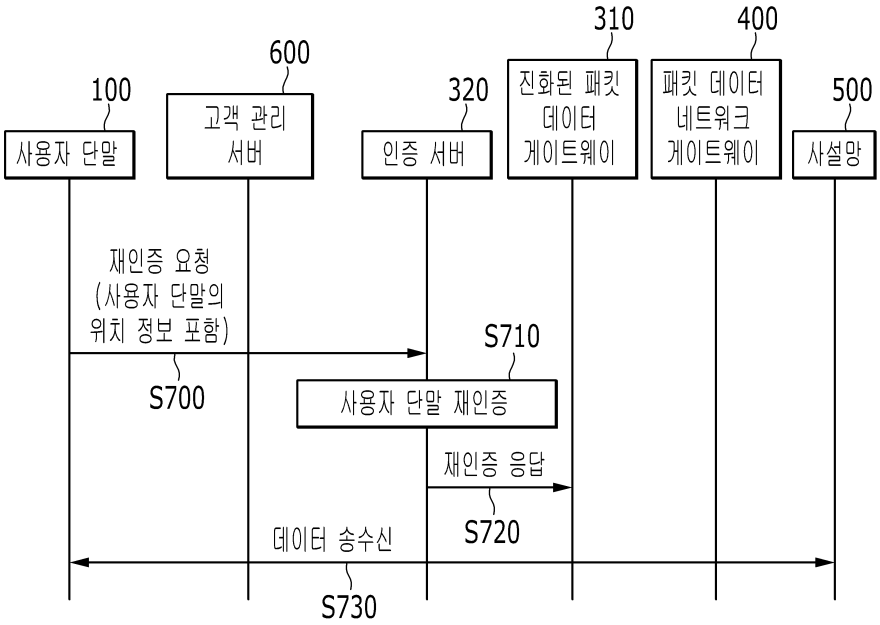
도면8


310
400
100
진화된
패킷 데이터
게이트웨이
320
패킷 데이터
네트워크
게이트웨이
500
사용자 단말
인증 서버
사설망
S600
핸드오버 발생
MOBIKE 메시지
(사용자 단말의
위치 정보 포함)
Re-Auth-Request
(사용자 단말의
위치 정보 포함)
S610
S620
사용자 단말 재인증
S630
Re-Auth-Answer
S640
S650
IPSec 터널링
GRE 터널링 또는 GTP 터널링
데이터 송수신
S660

도면9


패킷 데이터
네트워크 게이트웨이
400
500
사설망
(기업 사내망)
300
사용자 단말 접속 제어 시스템
210
100
320
310
제1 비신뢰망
접속 장치
사용자 단말
패킷 데이터
네트워크 게이트웨이
인증 서버
220
제2 비신뢰망
접속 장치
600
고객 관리 서버

도면10


100
사용자 단말
600
고객 관리 서버
320
인증 서버
310
진화된 패킷 데이터 게이트웨이
400
패킷 데이터 네트워크 게이트웨이
500
사설망
재인증 요청 (사용자 단말의 위치 정보 포함)
S700
S710
사용자 단말 재인증
재인증 응답
S720
데이터 송수신
S730