(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년07월23일
(11) 등록번호 10-1881167
(24) 등록일자 2018년07월17일

(51) 국제특허분류(Int. Cl.)
B60W 50/08 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2011-0056748
(22) 출원일자 2011년06월13일
심사청구일자 2016년06월07일
(65) 공개번호 10-2012-0137729
(43) 공개일자 2012년12월24일
(56) 선행기술조사문헌
JP4539246 B2*
US20020135466 A1*
KR1020090100818 A*
KR1020090060506 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이민구
경기도 성남시 분당구 판교로 430, 건영아파트 106동 801호 (이매동, 아름마을)
김동완
서울특별시 중구 다산로 32, 10동 604호 (신당동, 남산타운)
(뒷면에 계속)
(74) 대리인
유미특허법인

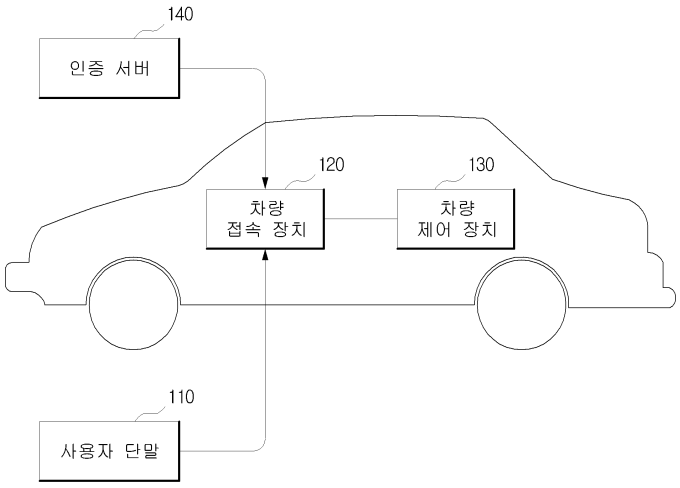
전체 청구항 수 : 총 8 항 심사관 : 한동기

(54) 발명의 명칭 **차량 제어 시스템**

(57) 요 약

차량 제어 시스템이 개시된다. 차량 내부에 차량의 전자적 제어를 위해 구비되는 차량 제어 장치(ECU: electronic control unit)와 연동되어 차량을 제어하는 시스템은, 사용자 단말의 단말 정보 및 차량 식별 정보 중 적어도 하나를 이용하여 사용자 단말에 대해 차량 접속 인증을 수행하여 인증 결과를 생성하는 인증 서버; 및 차량 제어 장치와 차량 내부 네트워크를 통해 직접 연결되고, 인증 서버를 통해 획득된 사용자 단말의 인증 결과에 따라 사용자 단말의 차량 제어를 위한 차량 제어 요청을 차량 제어 장치로 중계할지 여부를 결정하는 차량 접속 장치를 포함할 수 있다.

대 표 도 - 도1



(72) 발명자

박순향

경기도 안양시 동안구 학의로 390, 인덕원대우아파트 105동 1503호 (평촌동)

박종한

서울특별시 구로구 고척로16가길 7-9, 2층 (오류동)

정원영

서울특별시 송파구 송파대로32길 15, 금호아파트 104동 1003호 (가락동)

명 세 서

청구범위

청구항 1

차량 내부에 차량의 전자적 제어를 위해 구비되는 차량 제어 장치(ECU: electronic control unit)와 연동되어 차량을 제어하는 시스템에 있어서,

사용자 단말의 단말 정보 및 차량 식별 정보 중 적어도 하나를 이용하여 사용자 단말에 대해 차량 접속 인증을 수행하여 인증 결과를 생성하는 인증 서버; 및

상기 차량 제어 장치와 차량 내부 네트워크를 통해 직접 연결되고, 상기 인증 서버를 통해 획득된 상기 사용자 단말의 인증 결과, 상기 인증 서버와의 통신 연결 상태, 그리고 상기 인증 서버와의 통신 연결이 불가능한 경우를 위해 등록된 비상 제어 단말 유무를 기초로, 정상 모드, 비상 모드 그리고 비정상 운행 모드를 포함하는 복수의 모드들 중에서 차량 제어 상태 모드를 결정하고, 결정한 상기 차량 제어 상태 모드에 따라 상기 사용자 단말의 차량 제어를 위한 차량 제어 요청을 상기 차량 제어 장치로 중계할지 여부를 결정하는 차량 접속 장치를 포함하고,

상기 차량 접속 장치는

상기 인증 서버와의 통신 연결이 불가능하고, 상기 사용자 단말이 비상 제어 단말로 등록된 경우, 상기 차량 제어 상태 모드를 상기 비상 모드로 설정하고, 상기 사용자 단말의 제어 범위를 시동 제어로 한정하며,

상기 인증 서버로부터 인증 성공에 따른 인증 결과를 획득한 후 재획득된 인증 결과가 인증 실패이면, 상기 차량 제어 상태 모드를 상기 비정상 운행 모드로 변경하고, 상기 차량 제어 장치로 통보하며,

상기 비정상 운행 모드는 차량이 비정상적인 상태로 운행되고 있음을 나타내는 모드인, 차량 제어 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1 항에 있어서,

상기 비상 모드는 상기 사용자 단말의 제한된 차량 제어 요청을 상기 차량 제어 장치로 중계하는 것을 특징으로 하는 차량 제어 시스템.

청구항 5

삭제

청구항 6

제1 항에 있어서,

상기 차량 접속 장치는 상기 사용자 단말에 대한 인증 결과를 획득한 이후 일정 주기마다 상기 인증 서버로 상기 사용자 단말에 대한 차량 접속 인증을 요청하여 인증 결과를 획득하는 것을 특징으로 하는 차량 제어 시스템.

청구항 7

삭제

청구항 8

제1 항에 있어서,

상기 비정상 운행 모드는 최고 속도 제한, 비상등 점멸 및 경적음 발생 중 적어도 하나로 상기 차량이 운행되도록 제어하는 모드인 것을 특징으로 하는 차량 제어 시스템.

청구항 9

제1 항에 있어서,

상기 차량 접속 장치는,

상기 차량 제어 상태 모드를 상기 비정상 운행 모드로 변경시, 상기 사용자 단말에 대해 등록된 인증 정보를 삭제하고, 이후 상기 사용자 단말의 차량 제어를 위한 접속 요청시 연결을 차단하는 것을 특징으로 하는 차량 제어 시스템.

청구항 10

삭제

청구항 11

제1 항에 있어서,

상기 인증 서버는 차량 식별정보를 포함하는 도난 차량 등록 요청 수신시, 상기 차량 식별정보에 대응하는 차량의 상태를 도난 상태로 설정하고, 상기 차량 식별정보를 포함하는 도난 차량 정보를 상기 차량 접속 장치로 전송하고,

상기 차량 접속 장치는 상기 도난 차량 정보에 따라 상기 차량 제어 상태 모드를 도난 모드로 변경하여 상기 차량 제어 장치로 전송하는 것을 특징으로 하는 차량 제어 시스템.

청구항 12

제11 항에 있어서,

상기 도난 모드인 경우, 상기 차량 접속 장치는 일정 주기마다 상기 차량 접속 장치의 위치 정보를 획득하여 상기 인증 서버로 전송하되,

상기 인증 서버는 상기 위치 정보를 경찰 시스템으로 전송하는 것을 특징으로 하는 차량 제어 시스템.

청구항 13

제1 항에 있어서,

상기 차량 접속 장치는 제1 통신 방식을 통해 상기 사용자 단말과 연결되고, 제2 통신방식을 통해 상기 인증 서버와 연결되는 것을 특징으로 하는 차량 제어 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 제어에 관한 것으로, 보다 상세하게 사용자 단말을 이용하여 차량을 제어할 수 있는 시스템에 관한 것이다.

배 경 기 술

[0002] 경제 발전에 힘입어 자동차의 보급이 보편화되고 있다. 이에 따라, 자동차를 이용한 사용자의 편의성을 증진시키기 위한 다양한 기술들이 연구 개발되고 있는데, 이중 한 분야가 스마트키 시스템 분야이다. 스마트키 시스템은 운전자 또는 자동차의 소유자가 기계적인 제어 장치의 삽입 또는 조작에 의해 자동차의 시동을 제어하는 것이 아니라, 무선 통신 기술을 이용하여 자동차에 근접하여 원격으로 자동차 시동을 제어하고, 경보기를 설정할 수 있는 시스템이다.

[0003] 이와 같은 종래의 스마트키 시스템은 사용자가 별도의 스마트키를 구비해야만 하는 번거로운 단점이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 사용자 단말을 이용하여 차량을 제어할 수 있는 시스템을 제공하기 위한 것이다.

[0005] 또한, 본 발명은 차량 제어를 위한 별도의 스마트키를 구비할 필요가 없으며, 차량 도난의 경우 시스템을 통해 차량 제어를 위한 접근을 차단 또는/및 제어할 수 있는 차량 제어 시스템을 제공하기 위한 것이다.

[0006] 또한, 본 발명은 시스템을 통해 차량의 위치를 파악하여 차량에 대한 위치 추적 등에 대한 정보를 제공할 수 있는 차량 제어 시스템을 제공하기 위한 것이다.

과제의 해결 수단

[0007] 본 발명의 일 측면에 따르면, 차량 내부에 차량의 전자적 제어를 위해 구비되는 차량 제어 장치(ECU: electronic control unit)와 연동되어 차량을 제어하는 시스템이 제공된다.

[0008] 본 발명의 일 실시예에 따르면, 차량 내부에 차량의 전자적 제어를 위해 구비되는 차량 제어 장치(ECU: electronic control unit)와 연동되어 차량을 제어하는 시스템에 있어서, 사용자 단말의 단말 정보 및 차량 식별 정보 중 적어도 하나를 이용하여 사용자 단말에 대해 차량 접속 인증을 수행하여 인증 결과를 생성하는 인증 서버; 및 상기 차량 제어 장치와 차량 내부 네트워크를 통해 직접 연결되고, 상기 인증 서버를 통해 획득된 상기 사용자 단말의 인증 결과에 따라 상기 사용자 단말의 차량 제어를 위한 차량 제어 요청을 상기 차량 제어 장치로 중계할지 여부를 결정하는 차량 접속 장치를 포함하는 차량 제어 시스템이 제공될 수 있다.

발명의 효과

[0009] 본 발명의 일 실시예에 따르면, 스마트키를 대체하여 사용자 단말을 통해 차량을 제어할 수 있는 이점이 있다.

[0010] 또한, 본 발명은 차량 제어를 위한 별도의 스마트키를 구비할 필요가 없으며, 차량 도난의 경우 시스템을 통해 차량 제어를 위한 접근을 차단 또는/및 제어할 수 있다.

[0011] 또한, 본 발명은 시스템을 통해 차량의 위치를 파악하여 차량에 대한 위치 추적 등에 대한 정보를 제공할 수 있다.

도면의 간단한 설명

[0012] 도 1은 사용자 단말을 이용하여 차량을 제어하는 차량 제어 시스템을 개략적으로 도시한 블록도.

도 2는 차량 제어 시스템에서 사용자 단말의 차량 제어 요청에 따라 해당 사용자 단말에 대한 접속 인증을 수행하는 방법을 나타낸 흐름도.

도 3은 EAP-AKA 인증 방식에 따른 접속 인증 방법을 나타낸 흐름도.

도 4는 차량 접속 장치로 비상 모드에 따른 차량 제어가 가능한 비상 제어 대상 단말을 등록하는 방법을 나타낸 순서도.

도 5는 차량 접속 장치가 인증 서버와 일정 시간 동안 통신 연결이 불가능한 경우, 차량 제어 방법을 나타낸 흐름도.

도 6은 차량 제어 시스템에서 비상 모드에서 정상 모드로 변경시, 사용자 단말에 대한 접속 인증이 실패한 경우 차량 제어 방법을 나타낸 흐름도.

도 7은 차량 제어 시스템에서 차량 도난 신고에 따른 차량 제어 방법을 나타낸 흐름도.

도 8은 본 발명의 다른 실시예에 따른 차량 제어 시스템의 구성을 개략적으로 도시한 블록도.

도 9는 차량 접속 장치의 내부 구성을 개략적으로 도시한 블록도.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0014] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0015] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0016] 이하, 본 발명의 실시예를 첨부한 도면들을 참조하여 상세히 설명하기로 한다.

[0017] [도 1 설명]

[0018] 도 1은 사용자 단말을 이용하여 차량을 제어하는 차량 제어 시스템을 개략적으로 도시한 블록도이다.

[0019] 도 1을 참조하면, 차량 제어 시스템은 사용자 단말(110), 차량 접속 장치(120), 차량 제어 장치(130) 및 인증 서버(140)를 포함하여 구성된다. 여기서, 도 1에 도시된 바와 같이, 차량 접속 장치(120) 및 차량 제어 장치(130)는 차량 내부에 구비되거나 내장되는 장치이다.

[0020] 사용자 단말(110)은 근거리 무선 통신을 통해 차량 접속 장치(120)에 접속하여 차량 제어를 위한 접속 인증 결과에 따라 해당 차량 접속 장치(120)를 통해 차량 제어 장치(130)와 연결되어 차량을 제어하거나 해당 차량에 대한 다양한 정보(예를 들어, 차량 상태 정보)를 제공받을 수 있는 장치이다.

[0021] 이하, 본 명세서에서 별도의 설명이 없더라도 사용자 단말(110)에 차량 제어를 위한 별도의 어플리케이션이 설치되어 있으며, 해당 어플리케이션을 통해 차량 제어를 위한 차량 제어 요청을 차량 접속 장치(120)로 전송하는 것으로 이해되어야 할 것이다.

[0022] 예를 들어, 사용자 단말(110)은 이동통신 단말기, PDA, 스마트 폰 등과 같이, 근거리 무선 통신 기능을 구비한 휴대용 장치인 경우에는 모두 동일하게 적용될 수 있다.

[0023] 차량 접속 장치(120)는 차량 내부에 탑재되며, 차량의 전자적 제어를 담당하는 차량 제어 장치(130)와 차량 내부 네트워크를 통해 연결된다. 또한, 차량 접속 장치(120)는 사용자 단말(110)의 접속 인증 결과에 따라 해당 사용자 단말(110)의 차량 제어를 위한 차량 제어 요청을 차량 제어 장치(130)로 중계할지 여부를 결정하는 장치이다. 예를 들어, 차량 접속 장치(120)는 인증 서버(140)와의 통신 연결 상태 및 사용자 단말(110)의 접속 인증 결과 중 적어도 하나에 따라 차량 제어 상태 모드를 결정하고, 해당 결정된 차량 제어 상태 모드에 따라 차량이 운행되도록 이를 차량 제어 장치(130)로 통보하거나 사용자 단말(110)의 차량 제어 요청을 제한적으로 중계할 수 있다. 이에 대해서는 하기에서 관련 도면을 참조하여 보다 상세히 설명하기로 한다.

[0024] 또한, 차량 접속 장치(120)는 제1 통신 방식을 통해 사용자 단말(110)과 연결되고 제2 통신 방식을 통해 인증 서버(140)와 연결될 수 있다. 여기서, 제1 통신 방식은 근거리 통신 방식이고, 제2 통신 방식은 광역 통신 방식일 수 있다.

[0025] 결과적으로, 차량 접속 장치(120)는 차량을 전자적으로 제어하는 차량 제어 장치(130)와 직접 연동되어 사용자 단말(110)과 차량 제어 장치(130) 사이에서 게이트웨이 기능을 수행하기 위한 장치이다.

[0026] 예를 들어, 차량 접속 장치(120)는 사용자 단말(110)로부터 단말 정보를 포함하는 접속 인증을 요청받고, 차량 제어 장치(130)로부터 차량 식별 정보를 수신한 후 단말 정보 및 차량 식별 정보를 포함하는 인증 요청을 인증 서버(140)로 전송하여 사용자 단말(110)에 대한 인증을 요청할 수 있다. 이어, 차량 접속 장치(120)는 인증 서버(140)로부터 인증 결과를 수신하고, 수신된 인증 결과에 따라 사용자 단말(110)과 차량 제어 장치(130)간의 게이트웨이 기능을 수행하여 사용자 단말(110)이 차량을 제어하거나 차량 상태 정보를 제공받도록 중계할 수 있다.

[0027] 차량 제어 장치(130)는 차량에 탑재되는 전자 제어 장치(ECU: Electronic Control Unit)이다. 차량 제어 장치는 엔진, 자동 변속기, ABS 등의 상태를 제어하는 전자 제어 장치로, 차량 제어 장치를 통해 차량을 제어하거나 차량의 상태 정보를 획득하는 방법은 당업자에게는 자명한 사항이므로 이에 대한 별도의 설명은 생략하기로 한다. 여기서, 차량 제어 장치(130)는 차량 접속 장치(120)와 별도의 보안 채널(Secure Channel)을 통해 연결되며, 유선 또는 무선 차량 내부 네트워크를 통해 직접 연결된다.

[0028] 인증 서버(140)는 차량 접속 장치(120)와 연동되어 사용자 단말(110)에 대한 차량의 접속 권한을 인증하기 위한 장치이다.

[0029] 예를 들어, 인증 서버(140)는 차량 접속 장치(120)로부터 사용자 단말(110)에 대한 단말 정보와 차량에 대한 차량 식별 정보 중 적어도 하나를 포함하는 인증 요청을 수신할 수 있다. 여기서, 단말 정보는 예를 들어, 전화번호, IMSI(International Mobile Subscriber Identity)일 수 있다. 물론, 단말 정보는 이외에도 사용자 단말(110)을 식별할 수 있는 정보(예를 들어, MAC)인 경우에는 모두 동일하게 적용될 수 있음은 당연하다.

[0030] 이에 따라, 인증 서버(140)는 해당 인증 요청에 포함된 단말 정보 및 차량 식별 정보 중 적어도 하나를 이용하여 기등록된 인증 정보와 비교하여 해당 사용자 단말(110)이 해당 차량에 대한 제어 권한이 있는지에 대해 인증하여 인증 결과를 차량 접속 장치(120)로 전송할 수 있다. 여기서, 인증 결과는 인증 성공 또는 인증 실패일 수 있다.

[0031] 또한, 인증 서버(140)는 차량 접속 장치(120)와의 연동이 불가능한 경우를 대비하여, 차량 접속 장치(120)로 인증 결과와 함께 등록된 단말 정보를 함께 전송할 수도 있다.

[0032] 이하, 도 2에서는 차량 접속 장치를 통해 사용자 단말을 인증하는 방법에 대해 설명하기로 한다.

[0033] [도 2 및 도 3 설명]

[0034] 도 2는 차량 제어 시스템에서 사용자 단말의 차량 제어 요청에 따라 해당 사용자 단말에 대한 접속 인증을 수행하는 방법을 나타낸 흐름도이고, 도 3은 EAP-AKA 인증 방식에 따른 접속 인증 방법을 나타낸 흐름도이다.

[0035] 전술한 바와 같이, 차량 접속 장치(120)는 사용자 단말(110)과는 근거리 무선 통신을 통해 연결되고, 차량 접속 인증을 수행하는 인증 서버(140)와는 광역 통신을 통해 연결될 수 있다. 또한, 차량 접속 장치(120)는 차량 내부에 탑재되는 전자 제어 장치()와는 차량 내부 네트워크를 통해 직접 연결될 수 있다.

[0036] 단계 210에서 사용자 단말(110)은 차량 내부에 탑재된 차량 접속 장치(120)의 통신 가능 거리 이내에 위치되면,

차량 제어를 위한 접속 요청을 해당 차량 접속 장치(120)로 전송한다.

[0037] 예를 들어, 차량 접속 장치(120)와 사용자 단말(110)이 Wi-Fi로 연결되는 경우, 사용자 단말(110)은 차량 접속 장치에서 일정 주기로 송신하는 RF 신호를 감지하고, 해당 RF 신호에 따라 차량 접속 장치(120)와 통신 가능 거리 이내에 위치한 것으로 판단할 수 있다. 이에 따라, 사용자 단말(110)은 접속 요청을 위해 EAP-Start 메시지를 차량 접속 장치(120)로 전송할 수 있다.

[0038] 단계 215에서 차량 접속 장치(120)는 사용자 단말(110)의 접속 요청에 따라 인증 서버(140)와 연동되어 해당 사용자 단말(110)에 대한 접속 인증을 수행하고, 인증 서버(140)로부터 인증 결과를 수신한다. 여기서, 인증 결과는 인증 성공 또는 인증 실패일 수 있다.

[0039] 이하, 도 3에서는 사용자 단말(110)과 차량 접속 장치(120)가 Wi-Fi로 연결되는 것을 가정하여 EAP-AKA 인증 방식에 따라 인증하는 방법에 대해 설명하기로 한다. 본 명세서에서는 차량 접속 장치(120)가 인증 서버(140)와 연동되어 사용자 단말(110)에 대해 EAP-AKA 방식에 따라 접속 인증을 수행하는 것을 중심으로 설명하나 차량 접속 장치(120)와 사용자 단말(110)이 연결되는 방식이 상이해지는 경우 인증 방식도 상이해질 수 있음은 당연하다.

[0040] 단계 310에서 차량 접속 장치(120)는 사용자 단말(110)의 접속 요청에 따라 인증을 위해 필요한 식별 정보 요청(예를 들어, EAP-Request(Identity)메시지)을 사용자 단말(110)로 전송한다.

[0041] 단계 315에서 사용자 단말(110)은 차량 접속 장치(120)의 식별정보 요청에 따라 인증을 위해 필요한 식별정보를 차량 접속 장치(120)로 전송한다. 예를 들어, 사용자 단말(110)은 EAP-Response(Identity) 메시지를 이용하여 인증 정보를 차량 접속 장치(120)로 전송할 수 있다. 여기서, 인증 정보는 예를 들어, IMSI일 수 있다. 본 명세서에서는 AKA 인증을 예로 들어 설명하므로, 사용자 단말(110)이 인증 정보로 IMSI를 차량 접속 장치(120)로 전달하는 것을 가정하여 설명하고 있으나, 사용자 단말(110)과 차량 접속 장치(120)간에 인증 방식이 상이해지는 경우, 사용자 단말(110)에서 차량 접속 장치(120)로 전송하는 인증 정보 또한 상이해질 수 있음은 당연하다.

[0042] 단계 320에서 차량 접속 장치(120)는 사용자 단말(110)로부터 수신한 인증 정보를 인증 서버(140)로 전송한다. 여기서, 차량 접속 장치(120)와 인증 서버(140)는 RADIUS 프로토콜을 이용하여 통신을 수행하는 것을 가정하기로 한다. 즉, 차량 접속 장치(120)는 RADIUS(EAP-Response(Identity) 메시지)를 통해 인증 정보를 인증 서버(140)로 전송할 수 있다.

[0043] 물론, 차량 접속 장치(120)와 인증 서버(140)는 RADIUS 프로토콜 이외에도 DIAMETER 프로토콜을 통해 통신을 수행할 수도 있음은 당연하다.

[0044] 단계 325에서 인증 서버(140)는 차량 접속 장치(120)를 통해 사용자 단말(110)에 대한 인증 정보 수신에 따라 해당 인증 정보를 이용하여 인증 벡터를 생성하고, 생성된 인증 벡터를 차량 접속 장치(120)를 통해 사용자 단말(110)로 전송한다.

[0045] 예를 들어, 인증 서버(140)는 RADIUS(EAP-Request(AKA-Challenge(RAND, AUTH, MAC)) 메시지를 통해 차량 접속 장치(120)로 전송하고, 차량 접속 장치(120)는 EAP-Request(AKA-Challenge(RAND, AUTH, MAC))를 통해 인증 벡터를 사용자 단말(110)로 전송할 수 있다. 여기서, 인증 벡터는 랜덤식별변수값(RAND), 인증필드(AUTH), 메시지 인증 코드(MAC: message authentication code)를 포함한다.

[0046] 이에 따라, 단계 330에서 사용자 단말(110)은 인증벡터를 이용하여 서버 인증을 수행하고, 인증값을 생성하고, 이를 차량 접속 장치(120)를 통해 인증 서버(140)로 전송한다.

[0047] 예를 들어, 사용자 단말(110)은 생성된 인증값(예를 들어, RES)과 메시지 인증 코드를 AKA-Challenge로 캡슐화하고 EAP-Response 메시지를 통해 차량 접속 장치(120)로 전송하며, 차량 접속 장치(120)는 RADIUS 프로토콜을 통해 해당 EAP-Response 메시지를 인증 서버(140)로 전송할 수 있다.

[0048] 이때, 차량 접속 장치(120)는 당해 차량 접속 장치(120)에 저장된 차량 식별정보를 RADIUS 프로토콜에 더 포함하여 인증 서버(140)로 전송할 수 있다. 여기서, 차량 식별정보는 당해 차량 접속 장치(120)에 저장된 차량 엔진번호 및 차대 번호 중 어느 하나일 수 있다. 물론, 차량 식별정보는 차량 접속 장치(120)에 부여된 유일한 식별정보로 예를 들어, MAC일 수도 있다.

[0049] 단계 335에서 인증 서버(140)는 차량 접속 장치(120)를 통해 수신된 인증값 및 차량 식별정보 중 적어도 하나를 이용하여 해당 사용자 단말(110)이 차량에 대한 접속 인증을 수행하여 인증 결과를 차량 접속 장치(120)로 전송

한다.

[0050] 다시 도 2를 참조하여, 단계 220에서 차량 접속 장치(120)는 인증 서버(140)로부터 수신된 인증 결과가 인증 성공인지 여부를 판단한다.

[0051] 만일 인증 결과가 인증 실패이면, 단계 225에서 차량 접속 장치(120)는 인증 실패 메시지(EAP-Failure)를 사용자 단말(110)로 전송하고, 차량 제어 장치(130)와의 네트워크를 차단한다.

[0052] 이와 같이, 사용자 단말(110)에 대한 접속 인증에 대한 인증 결과가 인증 실패이면, 차량 접속 장치(120)는 이후 사용자 단말(110)로부터의 차량 제어 요청을 차량 제어 장치(130)로 중계하지 않고 차단하여 사용자 단말(110)에서 차량 제어가 불가능하도록 할 수 있다.

[0053] 그러나 만일 인증 결과가 인증 성공이면, 단계 230에서 차량 접속 장치(120)는 인증 성공 메시지(EAP-Success)를 사용자 단말(110)로 전송하고, 이어 인증 완료 통보 메시지를 차량 제어 장치(130)로 전송한다.

[0054] 이에 따라 이후, 차량 접속 장치(120)는 사용자 단말(110)로부터 차량에 대한 특정 제어 명령을 포함하는 차량 제어 요청이 수신되면, 이를 차량 제어 장치(130)로 전송하여 사용자 단말(110)을 통해 차량 제어가 가능하도록 할 수 있다.

[0055] 물론, 인증 결과가 인증 성공이면, 차량 접속 장치(120)는 사용자 단말(110)에서 차량 제어 장치(130)로의 차량 제어 명령 전송을 위해 차량 제어 장치(130)와 사용자 단말(110)간 보안 무선 채널 확보를 위한 과정을 더 수행할 수도 있다. 여기서, 차량 제어 장치(130)는 상술한 도 3의 접속 인증 수행에서 획득한 MSK를 이용하여 무선 보안 채널 확보 과정을 수행할 수 있다.

[0056] [도 4 설명]

[0057] 도 4는 차량 접속 장치로 비상 모드에 따른 차량 제어가 가능한 비상 제어 대상 단말을 등록하는 방법을 나타낸 순서도이다. 이하에서는 인증 서버(140)에서의 정상적인 접속 인증이 완료된 사용자 단말이 차량 접속 장치(120)를 통해 비상 제어 단말을 등록하는 절차에 대해 설명하기로 한다.

[0058] 도 4에서는 이해와 설명의 편의를 도모하기 위해 사용자 단말(110)이 차량 접속 장치(120)와의 접속을 통해 비상 제어 단말을 등록하는 것을 가정하여 설명하나 비상 제어 단말을 등록하는 대상은 정당한 권한이 있는 관리자 등이 사용자 정보(예를 들어, 아이디 및 패스워드 중 적어도 하나)를 이용하여 소지한 단말을 통해 차량 접속 장치(120)에 접속하여 등록할 수도 있음은 당연하다.

[0059] 단계 410에서 사용자 단말(110)은 단말 등록 요청을 차량 접속 장치(120)로 전송한다. 여기서, 단말 등록 요청은 사용자 단말(110)의 단말 정보 및 사용자 정보 중 적어도 하나를 포함할 수 있다. 사용자 정보는 사용자 식별정보 및 패스워드 중 적어도 하나일 수 있다.

[0060] 단계 415에서 차량 접속 장치(120)는 단말 등록 요청에 포함된 단말 정보 및 사용자 정보 중 적어도 하나를 이용하여 사용자 단말(110)에 대한 권한 인증을 수행한다. 여기서, 권한 인증은 사용자 단말(110) 또는 관리자가 차량 접속 장치(120)를 통해 비상 제어 단말을 등록할 정당한 권한이 존재하는지를 검증하기 위한 인증 절차이다.

[0061] 예를 들어, 차량 접속 장치(120)는 단말 정보 및 사용자 정보 중 적어도 하나가 기등록되어 있는지와 해당 단말 정보 및 사용자 정보 중 적어도 하나에 대해 설정된 권한이 단말 등록이 가능한 권한인지를 확인하여 해당 사용자 단말(110)에 상응하는 권한 인증을 수행할 수 있다.

[0062] 단계 420에서 차량 접속 장치(120)는 사용자 단말(110)에 대한 등록 권한 인증 결과가 인증 성공인지 여부를 판단한다.

[0063] 만일 인증 실패이면, 단계 425에서 차량 접속 장치(120)는 등록 권한 인증 실패 메시지를 생성하여 사용자 단말(110)로 전송한다.

[0064] 그러나 만일 인증 성공이면, 단계 430에서 차량 접속 장치(120)는 비상 제어 단말에 대한 인증을 위해 필요한 단말 정보 등록 요청을 사용자 단말(110)로 전송하여 획득한다. 여기서, 단말 정보(이하, 이해와 설명의 편의를 도모하기 위해 비상 제어 단말 정보라 칭하기로 함)는 비상 제어 단말을 식별하기 위한 정보로, MAC 어드레스, IMSI 및 전화번호 중 적어도 하나일 수 있다. 여기서, 비상 제어 단말은 사용자 단말(110)을 포함할 수도 있다.

[0065] 단계 435에서 차량 접속 장치(120)는 비상 제어 단말 등록 정보를 해당 차량 식별정보에 대응하여 등록한 후, 등록 완료 메시지를 사용자 단말(110)로 전송한다.

[0066] 단계 440에서 차량 접속 장치(120)는 사용자 단말(110)로부터 비상 제어 단말 조회 요청이 수신되었는지를 확인한다. 여기서, 비상 제어 단말 조회 요청은 사용자 단말(110)의 단말 정보 또는 관리자 정보나 차량 식별정보 중 적어도 하나를 포함할 수 있다.

[0067] 만일 비상 제어 단말 조회 요청이 수신되면, 단계 445에서 차량 접속 장치(120)는 해당 사용자 단말(110)에 상응하여 등록된 비상 제어 단말 정보를 데이터베이스에서 추출한 후 사용자 단말(110)로 전송한다. 이에 따라, 사용자 단말(110)은 해당 비상 제어 단말 정보를 이용하여 비상 등록된 단말 정보를 디스플레이할 수 있다.

[0068] 그러나 만일 비상 제어 단말 조회 요청이 미수신된 경우, 단계 440에서 대기한다.

[0069] 단계 450에서 차량 접속 장치(120)는 사용자 단말(110)로부터 비상 제어 단말 삭제 요청이 수신되었는지 여부를 판단한다. 여기서, 비상 제어 단말 삭제 요청은 적어도 하나의 삭제 대상 단말 정보, 사용자 단말(110)의 단말 정보 또는 관리자 정보 및 차량 식별정보 중 적어도 하나일 수 있다.

[0070] 만일 비상 제어 단말 삭제 요청이 수신된 경우, 단계 455에서 차량 접속 장치(120)는 해당 비상 제어 단말 삭제 요청에 포함된 삭제 대상 단말 정보에 상응하는 비상 제어 단말 정보를 삭제한다. 이어, 차량 접속 장치(120)는 삭제 완료 메시지를 사용자 단말(110)로 전송한다.

[0071] 그러나, 만일 비상 제어 단말 삭제 요청이 미수신된 경우 단계 350에서 대기한다.

[0072] 도 4에서는 사용자 단말(110)에 대해 한번의 권한 인증을 통해 단말 등록, 단말 조회 및 단말 삭제 중 하나 이상이 가능한 것을 중심으로 설명하였으나, 구현 방법에 따라 단말 등록, 단말 조회 및 단말 삭제 각각의 기능 수행시마다 차량 접속 장치(120)는 사용자 단말(110)에 상응하여 권한 인증을 수행할 수도 있다.

[0073] [도 5 설명]

[0074] 도 5는 차량 접속 장치가 인증 서버와 일정 시간 동안 통신 연결이 불가능한 경우, 차량 제어 방법을 나타낸 흐름도이다. 이하에서는 차량 접속 장치(120)와 인증 서버(140)와의 통신 연결이 불가능한 상태에서, 차량 접속 장치(120)가 사용자 단말에 대해 비상 접속 인증을 수행하는 절차에 대해 설명하기로 한다.

[0075] 단계 510에서 차량 접속 장치(120)는 사용자 단말(110)로부터 접속 요청을 수신한다.

[0076] 단계 515에서 차량 접속 장치(120)는 인증 서버(140)와의 통신 연결을 시도하고, 통신 연결이 가능한 상태인지 여부를 판단한다.

[0077] 만일 통신 연결이 가능한 경우에는 도 2 및 도 3에서 설명한 바와 동일하게 사용자 단말에 대해 접근 인증을 수행하므로 이에 대한 별도의 설명은 생략하기로 한다.

[0078] 그러나 만일 통신 연결이 불가능한 경우, 단계 520에서 차량 접속 장치(120)는 차량 제어 상태 모드를 비상 모드로 설정한다.

[0079] 본 명세서에서 비상 모드에서는 사용자 단말(110)의 차량 제어를 위한 접속 인증에 대해 단방향으로 인증을 수행하는 모드로, 차량에 대한 정상적인 제어가 불가능하고, 단지 시동 제어만 가능한 제어 상태를 나타낸다. 이에 따라, 차량 접속 장치(120)가 차량 제어 상태 모드를 비상 모드로 설정하는 경우, 사용자 단말(110)은 차량의 상태 조회, 비상등 점멸 등과 같은 시동 제어를 제외한 다른 기능들은 제어가 불가능하게 된다.

[0080] 단계 525에서 차량 접속 장치(120)는 사용자 단말(110)에 대한 인증을 위해 단말 정보를 요청하여 획득한다. 여기서, 단말 정보는 당해 사용자 단말(110)의 MAC 어드레스, IMSI 및 전화번호 중 적어도 어느 하나일 수 있다.

[0081] 단계 530에서 차량 접속 장치(120)는 사용자 단말(110)을 통해 획득된 단말 정보가 등록된 단말정보와 일치하는지 확인하여 해당 사용자 단말(110)에 대해 인증을 수행한 후 인증 결과가 인증 성공인지 여부를 판단한다.

[0082] 물론, 차량 접속 장치(120)는 구현 방법에 따라 단말 정보 이외에 사용자 단말(110)로 기등록된 인증을 위해 필요한 사용자 정보(예를 들어, 아이디 및 패스워드)를 더 획득한 후 인증에 더 이용할 수도 있다.

[0083] 차량 접속 장치(120)는 이와 같이, 인증 서버(140)와의 통신 연결이 불가능한 상태에서는 단방향으로 해당 사용

자 단말(110)에 대한 접속 인증을 수행할 수 있다.

[0084] 만일 인증 결과가 인증 성공이면, 단계 535에서 차량 접속 장치(120)는 비상 인증 완료 메시지를 생성하여 차량 제어 장치(130)로 전송한다. 이어, 차량 접속 장치(120)는 비상 인증 성공 메시지를 생성하여 사용자 단말(110)로 전송한다.

[0085] 이후, 단계 540에서 사용자 단말(110)은 차량 접속 장치(120)로부터의 비상 인증 성공 메시지 수신에 따라 차량 접속 장치(120)를 통해 차량 제어 장치(130)로 제한된 차량 제어 요청을 전송한다.

[0086] 예를 들어, 사용자 단말(110)은 당해 사용자 단말(110)상에 차량 제어를 위한 어플리케이션의 차량 제어 기능들 중에서 비상 모드에 따른 비상 인증에 따라 차량 시동 제어와 같이 제한된 제어 기능만 활성화시키고 나머지 차량 제어 기능들은 모두 비활성화시킬 수 있다. 이와 같은 경우, 사용자에 의해 비활성화된 차량 제어 기능이 선택되는 것을 미연에 방지할 수 있는 이점이 있다.

[0087] 예를 들어, 사용자 단말(110)상에 비상 모드에 따라 활성화되는 차량 제어 기능은 시동 제어 기능일 수 있으며, 비활성화되는 차량 제어 기능은 차량 상태 조회, 비상키 등록 기능 등일 수 있다.

[0088] 물론, 사용자 단말(110)은 해당 어플리케이션상의 차량 제어 기능 중 일부를 비활성화시키지 않을 수 있다. 이와 같은 경우, 차량 접속 장치(120)가 사용자 단말(110)로부터 비상 모드에 허용되지 않은 차량 제어 요청이 수신되는 경우, 이를 차량 제어 장치(130)로 중계하여 전송하지 않을 수 있다.

[0089] 그러나 만일 단계 530의 인증 결과가 인증 실패이면, 단계 545에서 차량 접속 장치(120)는 차량 제어 장치(130)와의 네트워크를 차단한다. 이로 인해, 차량 접속 장치(120)는 사용자 단말(110)이 당해 차량 접속 장치(120)를 통해 차량 제어 장치(130)에 접속하는 것을 차단한다.

[0090] 이와 같이, 사용자 단말(110)이 차량 접속 장치(120)와의 비상 접속 인증을 통해 비상 모드에서 차량을 제한적으로 제어하고 있는 상태에서, 차량 접속 장치(120)와 인증 서버(140)간의 통신이 가능해지는 경우에는 도 2 및 도 3에서 설명한 바에 따라 사용자 단말(110)에 대한 정상 접속 인증을 수행할 수 있다. 이와 같은 경우, 차량 접속 장치(120)는 차량 제어 상태 모드를 비상 모드에서 정상 모드로 변경한 후 도 2 및 도 3에서 설명한 바에 따른 접속 인증을 수행할 수 있다.

[0091] [도 6 설명]

[0092] 도 6은 차량 제어 시스템에서 비상 모드에서 정상 모드로 변경시, 사용자 단말에 대한 접속 인증이 실패한 경우 차량 제어 방법을 나타낸 흐름도이다.

[0093] 도 6에서는 차량 접속 장치(120)와 인증 서버(140)간의 통신 연결이 불가능한 상태에서 차량 접속 장치(120)가 인증 서버(140)와의 연동 없이 단방향으로 사용자 단말(110)에 대해 비상 접속 인증을 수행한 이후, 인증 서버(140)와의 통신 연결이 가능해지는 경우의 접속 인증 방법에 대해 설명하기로 한다.

[0094] 단계 610에서 차량 접속 장치(120)는 비상 모드에 따른 비상 접속 인증을 수행한 이후, 일정 주기마다 인증 서버(140)와의 통신 연결을 시도하여 통신 연결이 가능한 상태인지 여부를 판단한다.

[0095] 만일 통신 연결이 가능하지 않은 경우, 단계 610으로 진행한다.

[0096] 그러나 만일 통신 연결이 가능한 경우, 단계 615에서 차량 접속 장치(120)는 인증 서버(140)로 사용자 단말(110)에 대한 접속 인증을 요청하여 사용자 단말(110)에 대한 접속 인증을 수행한다. 이는 이미 도 2 및 도 3에서 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0097] 단계 620에서 차량 접속 장치(120)는 인증 서버(140)로부터 접속 인증에 따른 인증 결과를 수신하여 인증 결과가 인증 성공인지 여부를 판단한다.

[0098] 만일 인증 결과가 인증 성공이면, 단계 625에서 차량 접속 장치(120)는 차량 제어 상태 모드를 비상 모드에서 정상 모드로 변경하고, 차량 접속 장치(120)는 사용자 단말(110)이 정상적으로 차량 제어가 가능하도록 차량 제어 장치(130)로 중계할 수 있다.

[0099] 반면, 인증 결과가 인증 실패이면, 단계 630에서 차량 접속 장치(120)는 사용자 단말(110)에 대한 인증 정보(즉, 단말 정보)를 폐기하거나 블랙 리스트에 등록한다.

[0100] 단계 635에서 차량 접속 장치(120)는 인증 실패 메시지를 사용자 단말(110)로 전송한다.

[0101] 이어, 단계 640에서 차량 접속 장치(120)는 차량 제어 상태 모드를 비정상 운행 모드로 설정하고, 차량 제어 장치(130)로 비정상 운행 모드를 통보한다.

[0102] 이에 따라, 단계 645에서 차량 제어 장치(130)는 비정상 운행 모드에 상응하여 미리 설정된 차량이 비정상 모드로 운행되도록 제어한다.

[0103] 본 명세서에서 비정상 모드로의 운행은 차량의 최고 속도 제한, 비상등 점멸 및 경적음 발생 등과 같이, 차량이 비정상적인 상태로 운행되고 있음을 표출하는 방식으로 제어한다. 또한, 비정상 운행 모드의 경우, 차량 제어 장치(130)는 차량이 정차 또는 주차된 상태에서 차량 운행이 불가능하도록 처리할 수도 있다.

[0104] 또 다른 예를 들어, 차량이 비정상 모드로 운행중인 상태에서, 차량 제어 장치(130)는 일정 시간 동안 차량이 운행되도록 제어한 후 점차적으로 차량의 속도를 줄여서 정차되도록 제어할 수도 있다. 물론, 이와 같은 경우, 차량 제어 장치(130)는 차량이 정차할 것임을 알리는 메시지를 사용자 단말(110)로 전송할 수도 있다.

[0105] [도 7 설명]

[0106] 도 7은 차량 제어 시스템에서 차량 도난 신고에 따른 차량 제어 방법을 나타낸 흐름도이다. 이하에서는 차량이 정상적인 인증을 통해 운행되고 있는 상태에서 차량 도난 신고에 따른 차량 제어 방법에 대해 설명하기로 한다.

[0107] 단계 710에서 인증 서버(140)는 관리자로부터 도난 차량 식별정보를 포함하는 도난 차량 등록 요청을 수신하여 도난 차량을 등록한다. 즉, 인증 서버(140)는 도난 차량 식별정보에 상응하는 차량 식별정보의 차량 상태를 도난 차량으로 변경하여 설정할 수 있다.

[0108] 이어, 단계 715에서 인증 서버(140)는 도난 차량 정보를 차량 접속 장치(120)로 전송한다.

[0109] 인증 서버(140)는 차량 식별정보와 차량 접속 장치(120)에 대한 정보를 데이터베이스에 저장하고 있다. 이에 따라 인증 서버(140)는 도난 차량에 탑재된 차량 접속 장치(120)로 도난 차량 정보를 전송할 수 있다.

[0110] 단계 720에서 차량 접속 장치(120)는 인증 서버(140)로부터의 도난 차량 정보 수신에 따라 차량 제어 상태 모드를 도난 모드로 설정한다.

[0111] 이때, 차량 접속 장치(120)는 RADIUS 또는 DIAMETER의 클라이언트-서버간 P2P(Peer to Peer)간 보안 채널을 기반으로 해당 인증 서버(140)에 대한 인증을 수행한 후 차량 제어 상태 모드를 도난 모드로 설정 변경할 수 있다.

[0112] 단계 725에서 차량 접속 장치(120)는 도난 모드 설정에 상응하여 해당 차량 접속 장치(120)의 위치 정보를 획득한 후 인증 서버(140)로 전송한다. 인증 서버(140)는 획득된 위치 정보를 해당 경찰 시스템(미도시)으로 전송하여 해당 도난 차량에 대한 실시간 위치 추적이 가능하도록 할 수 있다.

[0113] 단계 730에서 차량 접속 장치(120)는 도난 모드 설정에 상응하여 차량 제어 장치(130)로 도난 모드를 통보한다.

[0114] 이에 따라 단계 735에서 차량 제어 장치(130)는 도난 모드로 차량이 운행되도록 제어할 수 있다. 본 명세서에서 차량의 도난 모드로의 운행은 차량의 최고 속도를 제한하고, 비상등을 점멸하고, 경적음을 발생하여 운행되도록 제어하는 것을 나타낸다.

[0115] 이어, 차량 접속 장치(120)에 의해 차량이 도난 모드로 설정되는 경우, 이후, 사용자 단말(110)은 시동 정지 제어만 가능하며 나머지 차량 제어 기능은 이용이 불가능한 상태로 변경된다.

[0116] 도난 모드에서 사용자 단말(110)에 의해 차량이 시동 정지되는 경우, 차량 접속 장치(120)는 이후 사용자 단말(110)에 의해 차량 시동 제어 요청이 수신되더라도 이를 차량 제어 장치(130)로 중계하여 전송하지 않을 수 있다. 이에 따라, 이후 차량 접속 장치(120)는 사용자 단말(110)에 의해 차량이 시동되지 않도록 제어할 수 있다.

[0117] [도 8 설명]

[0118] 도 8은 본 발명의 다른 실시예에 따른 차량 제어 시스템의 구성을 개략적으로 도시한 블록도이다.

[0119] 도 8을 참조하면, 차량 제어 시스템은 사용자 단말(810), 차량 접속 장치(820), 차량 제어 장치(830), 통신망

시스템(840) 및 인증 서버(850)를 포함하여 구성된다.

[0120] 여기서, 사용자 단말(810), 차량 접속 장치(820), 차량 제어 장치(830) 및 인증 서버(840)는 도 1에서 설명한 바와 동일하므로 중복되는 설명은 생략하며 상이한 구성에 대해서만 설명하기로 한다.

[0121] 도 1에서는 인증 서버(850)가 통신망 시스템(840) 내부에 위치되는 경우의 차량 제어 시스템의 구성을 설명한 것이다.

[0122] 도 8은 인증 서버(850)가 통신망 시스템(840) 내부에 위치되는 것이 아니라 별도로 위치되는 경우의 구성이다.

[0123] 이에 따라 차량 접속 장치(820)는 통신망 시스템(840)과 RADIUS 혹은 DIAMETER 프로토콜을 이용하여 통신하고, 통신망 시스템(840)은 인증 서버(850)가 외부의 네트워크에 별도로 구비되는 경우이므로 프록싱(proxying)을 통해 통신망 시스템(840)은 메시지를 인증 서버(850)로 전송하여 인증 서버(850)는 프록시(proxy) 형태로 접속 인증을 수행할 수 있다.

[0124] 이를 위해, 통신망 시스템(840)은 도메인 라우팅 기능을 수행하여, 차량 접속 장치(820)에 접속하는 사용자 단말(810)에 대해 각 차량 제조사별로 구분된 도메인을 붙여 접속 인증을 요청할 수 있다.

[0125] 예를 들어, 차량 접속 장치(820)는 사용자 단말(810)로부터 단말정보가 수신시, 단말정보에 차량 제조사별로 구분된 도메인을 붙여 통신망 시스템(840)으로 전송할 수 있다. 이에 따라 통신망 시스템(840)은 프록싱을 통해 상응하는 차량 제조사의 인증 서버(850)로 단말정보를 전송하여 접속 인증을 요청할 수 있다.

[0126] 즉, 차량 접속 장치(820)에서 통신망 시스템(840)으로 차량 제조사별로 구분된 도메인을 붙여 접속 인증을 요청하거나, 차량임대사업자 별 도메인을 붙여 접속인증을 요청하는 등 사업장에 따라 도메인을 붙이고, 통신망 시스템(840)은 프록싱을 통해 인증 서버(850)로 접속한다는 점 이외에 도 2 및 도 3에서 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0127] [도 9 설명]

[0128] 도 9는 차량 접속 장치의 내부 구성을 개략적으로 도시한 블록도이다.

[0129] 도 9을 참조하면, 차량 접속 장치는 통신부(910), 설정부(915), 인증부(920), 등록부(925), 저장부(930) 및 제어부(935)를 포함하여 구성된다.

[0130] 통신부(910)는 복수의 통신 모듈을 구비하여 각 통신 모듈을 통해 각각의 장치와 데이터를 송수신하기 위한 수단이다.

[0131] 예를 들어, 통신부(910)는 제1 통신 모듈 및 제2 통신 모듈을 구비할 수 있으며, 여기서, 제1 통신 모듈은 근거리 통신 방식에 따라 데이터를 송수신하고, 제2 통신 모듈은 광역 통신 방식에 따라 데이터를 송수신할 수 있다.

[0132] 설정부(915)는 당해 차량 접속 장치(120, 820)가 탑재 또는 구비되는 차량에 대한 차량 제어 상태 모드를 설정하기 위한 수단이다. 예를 들어, 설정부(915)는 인증부(920)의 인증 결과 및 통신부(910)를 통한 인증 서버(140, 850)와의 통신 연결 상태 중 적어도 어느 하나에 따라 차량 제어 상태 모드를 설정할 수 있다. 물론, 설정부(915)는 인증 서버(140, 850)로부터의 차량 정보(예를 들어, 도난 차량 정보)에 따라 해당 차량 제어 상태 모드를 설정할 수도 있다.

[0133] 차량 제어 상태 모드는 이미 전술한 바와 같이, 정상 모드, 비상 모드, 비정상 운행 모드 및 도난 모드 중 하나 이상을 포함할 수 있다. 각각의 모드에 대해서는 이미 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0134] 인증부(920)는 인증 서버(140, 850)와의 통신 연결 상태에 따라 인증 서버(140, 850)와 연동되어 사용자 단말(110)에 대한 차량 접속 인증을 수행하거나 인증 서버(140, 850)와의 연동없이 비상 접속 인증을 수행하기 위한 수단이다.

[0135] 예를 들어, 인증 서버(140, 850)와의 통신 연결이 가능한 상태이면, 인증부(920)는 사용자 단말(110, 810)의 단말 정보 및 해당 차량 제어 장치(130, 830)를 통해 획득된 차량 식별정보 중 적어도 하나를 포함하는 차량 접속 인증을 인증 서버(140, 850)로 요청하여 인증 결과를 획득할 수 있다.

[0136] 다른 예를 들어, 인증 서버(140, 850)와의 통신 연결이 불가능한 상태이면, 인증부(920)는 사용자 단말(110, 810)로부터 단말 정보 및 사용자 정보 중 적어도 하나를 획득하고, 해당 단말 정보 및 사용자 정보 중 적어도 하나와 기등록된 비상 단말 정보를 이용하여 해당 사용자 단말(110, 810)에 대한 비상 접속 인증을 수행하여 인증 결과를 생성하여 제어부(935)로 출력할 수 있다.

[0137] 등록부(925)는 인증 서버(140)와 정상적인 통신 연결이 가능한 상태에서, 해당 인증 서버(140)로부터 정상적으로 권한 인증이 수행된 사용자 단말(110, 810)로부터 비상시에 해당 차량 운행이 가능한 비상 단말 정보를 입력받아 등록하기 위한 수단이다. 이는 이미 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0138] 저장부(930)는 본 발명의 일 실시예에 따른 차량 접속 장치를 운용하기 위해 필요한 다양한 알고리즘을 저장한다. 또한, 저장부(930)는 등록부(925)를 통해 등록된 비상 단말 정보를 저장한다.

[0139] 제어부(935)는 본 발명의 일 실시예에 따른 차량 접속 장치의 내부 구성 요소들(예를 들어, 통신부(910), 설정부(915), 인증부(920), 등록부(925), 저장부(930) 등)을 제어하기 위한 수단이다.

[0140] 또한, 제어부(935)는 설정부(915)를 통해 설정된 차량 제어 상태 모드에 따라 사용자 단말(110, 810)의 차량 제어 요청을 제한적으로 중계할 수 있다. 이 또한 이미 전술한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0141] 한편, 본 발명의 실시예에 따른 사용자 단말을 이용한 차량 제어 방법은 다양한 전자적으로 정보를 처리하는 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 저장 매체에 기록될 수 있다. 저장 매체는 프로그램 명령, 데이터 파일, 데이터 구조등을 단독으로 또는 조합하여 포함할 수 있다.

[0142] 저장 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 소프트웨어 분야 당업자에게 공지되어 사용 가능한 것일 수도 있다. 저장 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media) 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 또한 상술한 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 전자적으로 정보를 처리하는 장치, 예를 들어, 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0143] 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0144] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0145] 110: 사용자 단말

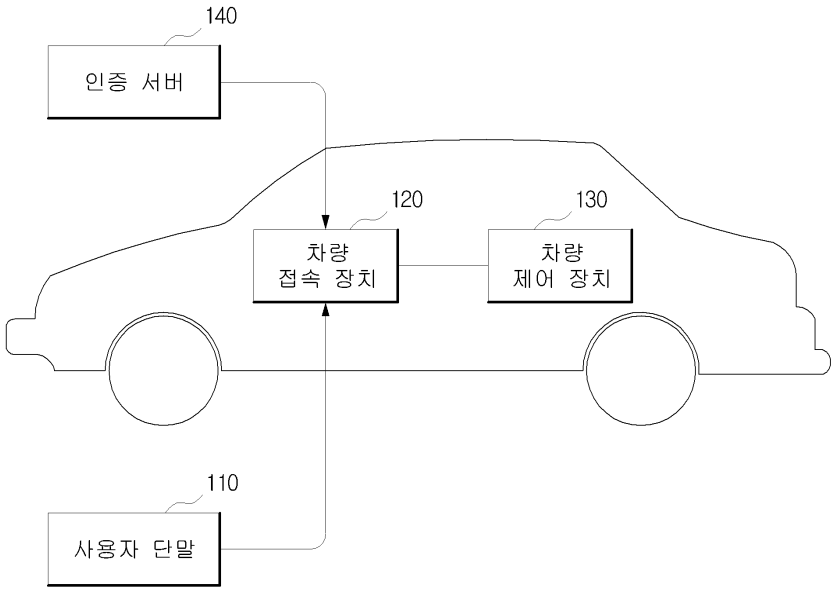
120: 차량 접속 장치

130: 차량 제어 장치

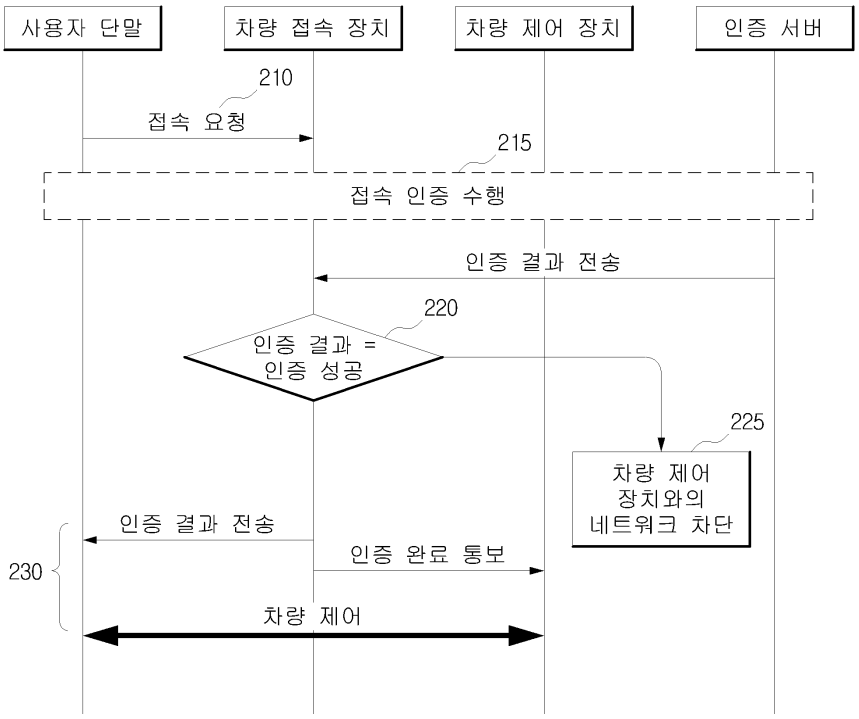
140: 인증 서버

도면

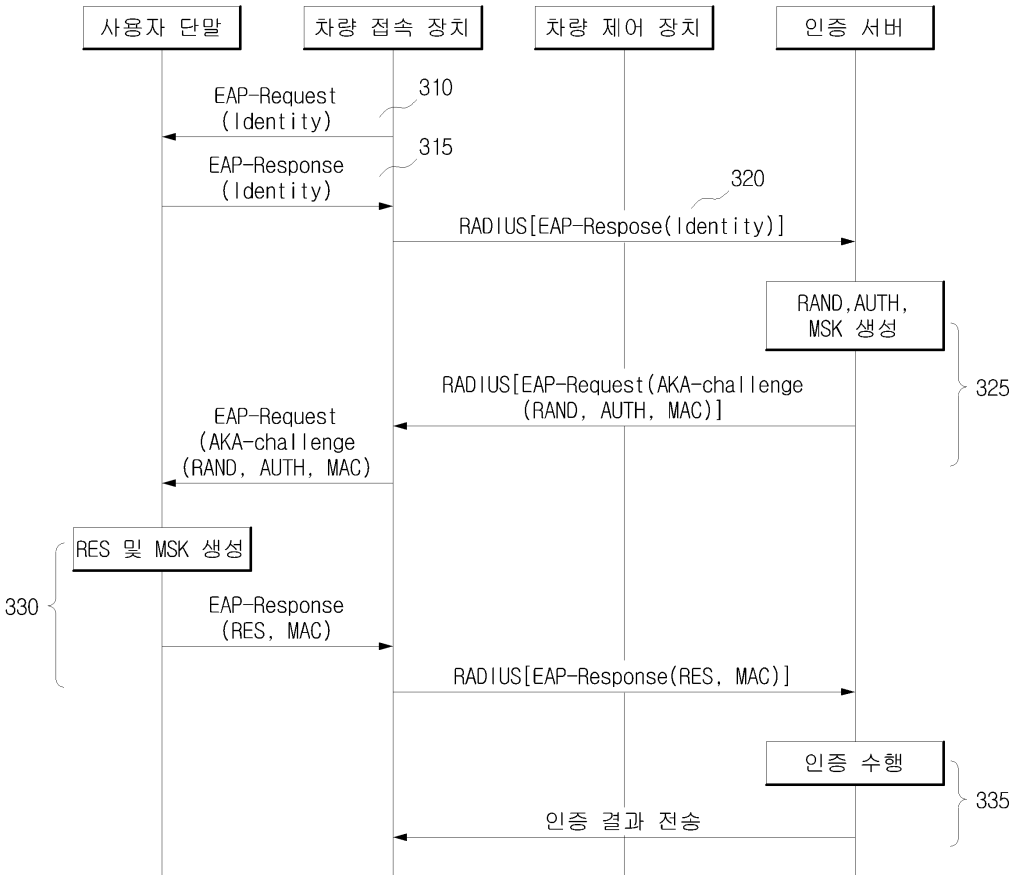
도면1


140
인증 서버
120
차량
접속 장치
130
차량
제어 장치
110
사용자 단말

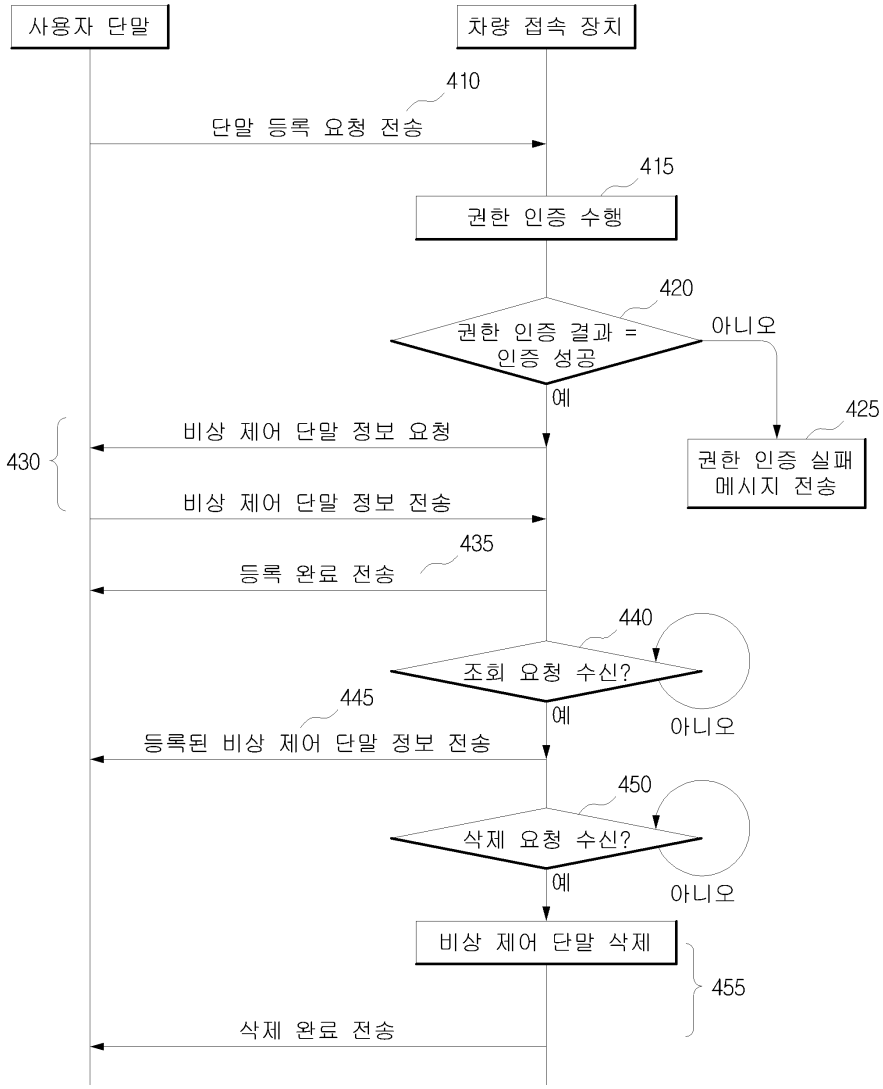
도면2


사용자 단말
차량 접속 장치
차량 제어 장치
인증 서버
210
접속 요청
215
접속 인증 수행
인증 결과 전송
220
인증 결과 =
인증 성공
225
차량 제어
장치와의
네트워크 차단
인증 결과 전송
230
인증 완료 통보
차량 제어

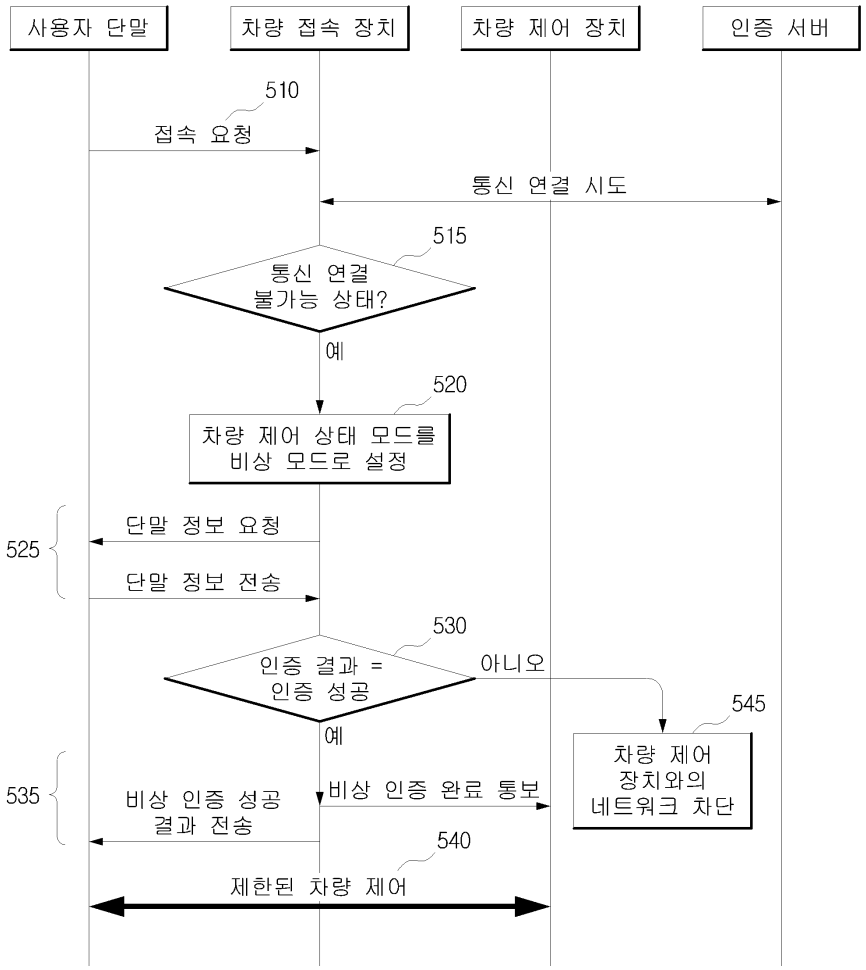
도면3


사용자 단말
차량 접속 장치
차량 제어 장치
인증 서버
310
EAP-Request
(Identity)
315
EAP-Response
(Identity)
320
RADIUS[EAP-Respose(Identity)]
RAND,AUTH,
MSK 생성
325
RADIUS[EAP-Request(AKA-challenge
(RAND, AUTH, MAC)]
EAP-Request
(AKA-challenge
(RAND, AUTH, MAC)
RES 및 MSK 생성
330
EAP-Response
(RES, MAC)
RADIUS[EAP-Response(RES, MAC)]
인증 수행
335
인증 결과 전송

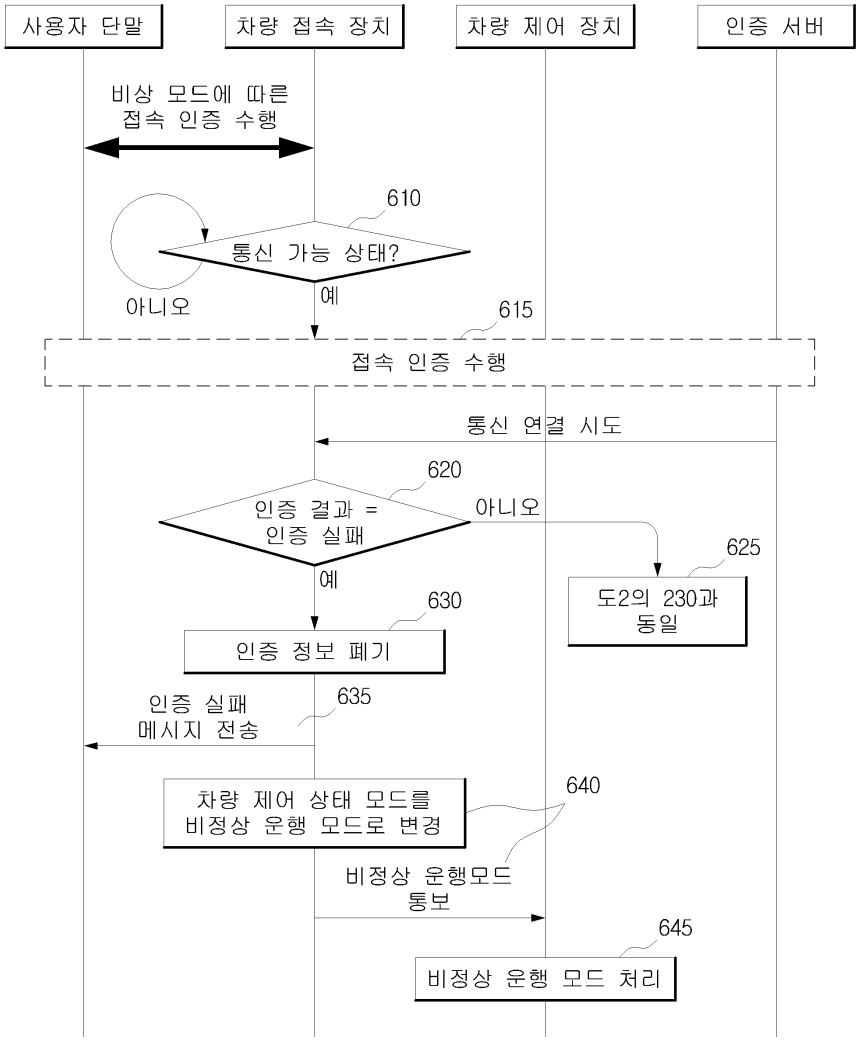
도면4


사용자 단말
차량 접속 장치
410
단말 등록 요청 전송
415
권한 인증 수행
420
권한 인증 결과 = 인증 성공
아니오
예
425
권한 인증 실패 메시지 전송
430
비상 제어 단말 정보 요청
비상 제어 단말 정보 전송
435
등록 완료 전송
440
조회 요청 수신?
아니오
예
445
등록된 비상 제어 단말 정보 전송
450
삭제 요청 수신?
아니오
예
비상 제어 단말 삭제
455
삭제 완료 전송

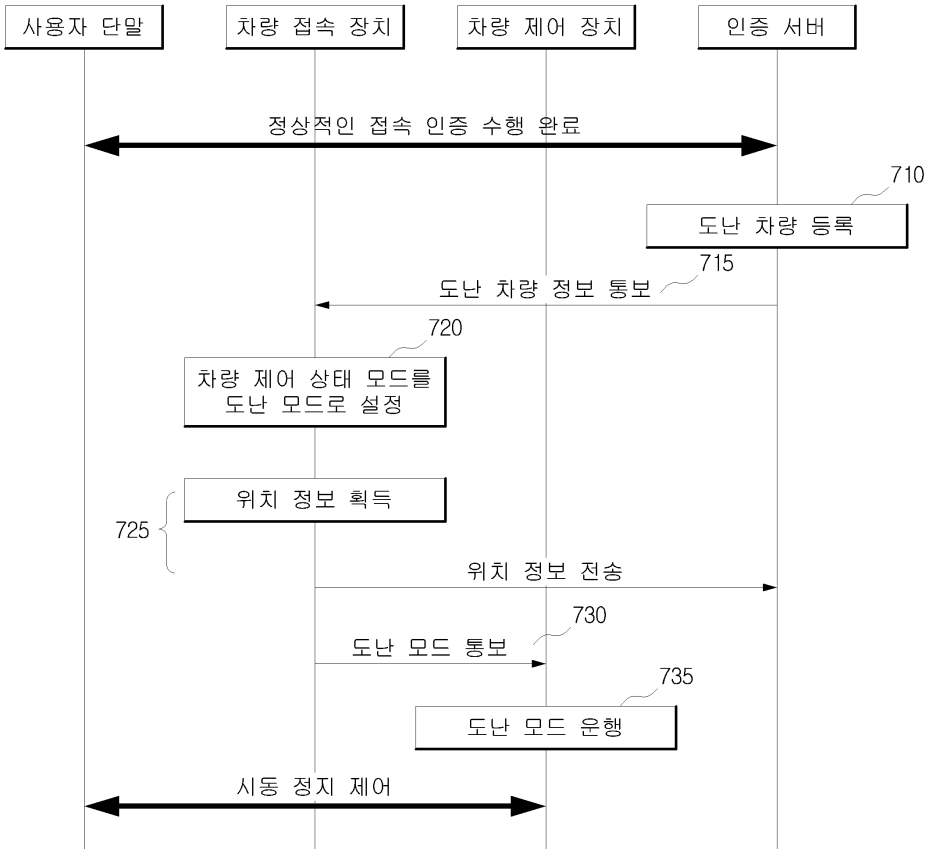
도면5


사용자 단말
차량 접속 장치
차량 제어 장치
인증 서버
510
접속 요청
통신 연결 시도
515
통신 연결
불가능 상태?
예
520
차량 제어 상태 모드를
비상 모드로 설정
525
단말 정보 요청
단말 정보 전송
530
인증 결과 =
인증 성공
아니오
545
차량 제어
장치와의
네트워크 차단
예
535
비상 인증 성공
결과 전송
비상 인증 완료 통보
540
제한된 차량 제어

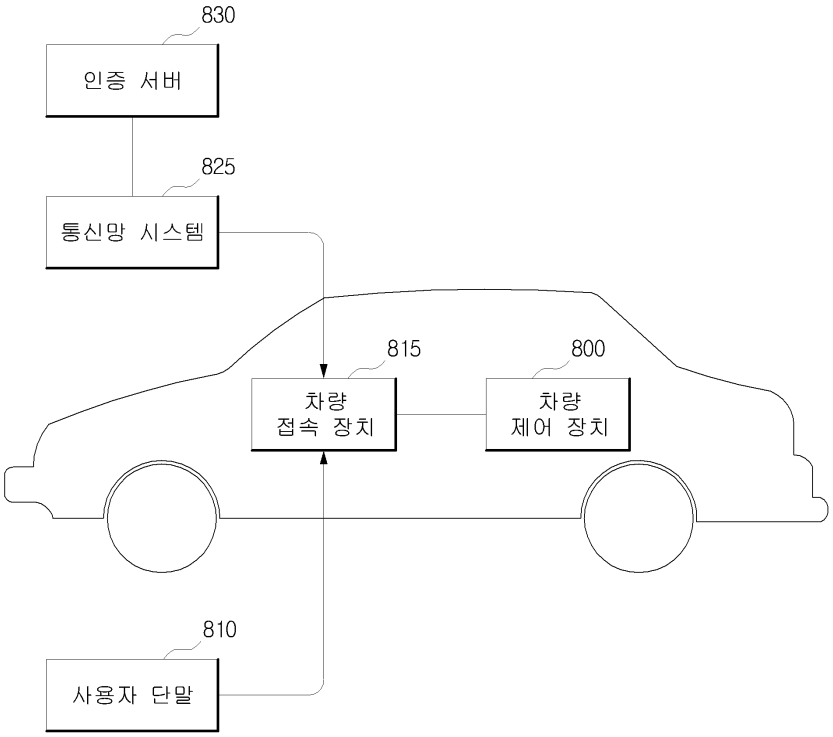
도면6


사용자 단말
차량 접속 장치
차량 제어 장치
인증 서버
비상 모드에 따른
접속 인증 수행
610
통신 가능 상태?
아니오
예
615
접속 인증 수행
통신 연결 시도
620
인증 결과 =
인증 실패
아니오
625
도2의 230과
동일
예
630
인증 정보 폐기
인증 실패
메시지 전송
635
차량 제어 상태 모드를
비정상 운행 모드로 변경
640
비정상 운행모드
통보
645
비정상 운행 모드 처리

도면7


사용자 단말
차량 접속 장치
차량 제어 장치
인증 서버
정상적인 접속 인증 수행 완료
710
도난 차량 등록
715
도난 차량 정보 통보
720
차량 제어 상태 모드를
도난 모드로 설정
위치 정보 획득
725
위치 정보 전송
730
도난 모드 통보
735
도난 모드 운행
시동 정지 제어

도면8


830
인증 서버
825
통신망 시스템
815
800
차량
접속 장치
차량
제어 장치
810
사용자 단말

도면9