



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년04월07일
(11) 등록번호 10-2077659
(24) 등록일자 2020년02월10일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) H04W 12/04 (2009.01)
(21) 출원번호 10-2013-0169307
(22) 출원일자 2013년12월31일
심사청구일자 2018년12월14일
(65) 공개번호 10-2015-0079232
(43) 공개일자 2015년07월08일
(56) 선행기술조사문헌
KR1020020085089 A*
(뒷면에 계속)

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
박재성
서울 서대문구 홍제내길 168, 101동 902호 (홍제동, 홍제남양아파트)
(74) 대리인
유미특허법인

전체 청구항 수 : 총 15 항

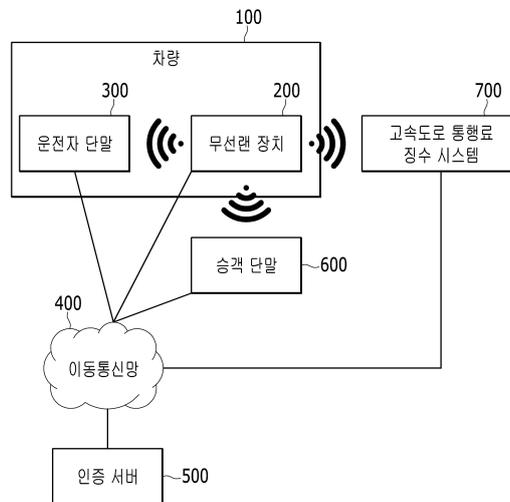
심사관 : 이준석

(54) 발명의 명칭 무선랜 장치 및 상기 무선랜 장치를 이용한 차량 인증 방법

(57) 요약

무선랜 장치 및 상기 무선랜 장치를 이용한 차량 인증 방법이 개시된다. 여기서, 무선랜 장치는 무선랜 통신을 통해 데이터를 송수신하는 무선랜 접속부, 이동통신망을 통해 데이터를 송수신하는 이동통신망 접속부, 상기 무선랜 접속부 및 상기 이동통신망 접속부와 연결되고, 무선랜 통신 반경 내에 위치하는 운전자 단말과 무선랜 통신으로 접속되어 상호 인증하며, 상기 운전자 단말을 통해 제공받은 운전자 정보가 포함된 차량 정보를 상기 무선랜 접속된 승객 단말로 전송하는 프로세서, 그리고 운전자 및 차량, 승객, 통행 장치, 인증 정보를 저장하는 메모리를 포함한다.

대표도 - 도1



(56) 선행기술조사문헌

KR1020070040031 A*

KR1020110071201 A*

KR1020120090445 A*

KR1020130134286 A*

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

무선랜 통신을 통해 데이터를 송수신하는 무선랜 접속부,

이동통신망을 통해 데이터를 송수신하는 이동통신망 접속부, 그리고

상기 무선랜 접속부 및 상기 이동통신망 접속부와 연결되고, 무선랜 통신 환경 내에 위치하는 운전자 단말과 무선랜 통신으로 접속되어 상호 인증하며, 상기 운전자 단말로부터 수신한 운전자 정보가 포함된 차량 정보를 무선랜 통신으로 접속된 승객 단말로 전송하는 프로세서를 포함하고,

상기 차량 정보는,

무선랜 장치의 SSID(Service Set Identifier)에 포함되는, 무선랜 장치.

청구항 2

제1항에 있어서,

상기 프로세서는,

무선랜 장치 공개키 및 무선랜 장치 개인키를 생성하고, 상기 무선랜 장치 공개키를 이동통신망을 통해 접속된 인증 서버에 등록하고, 상기 인증 서버로부터 상기 무선랜 장치 공개키를 이용하여 생성한 무선랜 장치 인증서 및 상기 운전자 단말이 상기 인증 서버에 등록된 운전자 단말 공개키를 이용하여 생성한 운전자 단말 인증서를 수신하는 서비스 등록부,

무선랜 접속된 상기 운전자 단말과 상기 운전자 단말 인증서를 이용하여 인증을 수행하는 단말 인증부, 그리고

상기 무선랜 장치 개인키로 서명한 차량 정보를 생성하여 상기 승객 단말로 전송하는 서비스 실행부

를 포함하는 무선랜 장치.

청구항 3

제2항에 있어서,

상기 단말 인증부는,

랜덤값을 포함하는 확인 요청 메시지를 상기 운전자 단말로 전송하고, 상기 운전자 단말의 운전자 단말 개인키로 서명된 확인 메시지를 상기 운전자 단말로부터 수신하며, 상기 인증 서버로부터 수신한 상기 운전자 단말 공개키로 상기 확인 메시지를 복호하여 상기 랜덤값을 추출하여 상기 랜덤값이 상기 확인 요청 메시지에 포함된 값과 일치하면, 상기 운전자 단말과 인증에 성공하는 무선랜 장치.

청구항 4

제3항에 있어서,

상기 서비스 실행부는,

상기 무선랜 장치의 빈 차량 여부, 운행 구역 및 상기 운전자 단말로부터 수신한 운전자 정보를 포함하는 차량 정보를 생성하고, 상기 무선랜 장치 개인키로 서명하여 상기 승객 단말로 전송하는 무선랜 장치.

청구항 5

제2항에 있어서,

상기 서비스 실행부는,

무선랜 접속된 고속도로 통행료 징수 시스템으로부터 상기 고속도로 통행료 징수 시스템의 제3 개인키로 서명된

결제 정보를 수신하고, 상기 인증 서버로부터 수신한 제3 공개키를 이용하여 상기 결제 정보를 검증하며, 검증에 성공하면, 결제 정보를 상기 운전자 단말로 전송하며, 상기 무선랜 장치 개인키로 결제 요청을 서명한 후, 상기 고속도로 통행료 징수 시스템으로 전송하고,

상기 결제 요청은 상기 인증 서버로 전달되어 상기 무선랜 장치에 통행료 과금 처리하는데 사용되는 무선랜 장치.

청구항 6

차량 내 무선랜 장치에 접속되는 운전자 단말이 차량 인증 서비스를 제공하는 차량 인증 방법으로서,

상기 운전자 단말이 이동통신망을 통해 접속된 인증 서버에 자신이 생성한 공개키를 등록한 후, 상기 인증 서버로부터 인증서를 수신하는 단계, 그리고

상기 인증서를 이용하여, 무선랜을 통해 접속된 상기 무선랜 장치와 상호 인증하는 단계를 포함하고,

상기 무선랜 장치는,

상호 인증된 상기 운전자 단말에게 무선랜 장치의 SSID(Service Set Identifier)를 이용하여 차량 정보를 제공하는, 차량 인증 방법.

청구항 7

제6항에 있어서,

상기 상호 인증하는 단계는,

상기 무선랜 장치로부터 확인 요청 메시지를 수신하는 단계, 그리고

상기 확인 요청 메시지에 포함된 랜덤값 및 운전자 정보가 포함된 확인 메시지를 상기 무선랜 장치로 전송하는 단계를 포함하고,

상기 랜덤값이 일치하고 서명이 검증이 되면, 상기 상호 인증에 성공하는 차량 인증 방법.

청구항 8

제7항에 있어서,

상기 무선랜 장치로 전송하는 단계는,

시간 정보, 운전자 정보, 랜덤값을 포함하는 확인 메시지를 상기 운전자 단말의 개인키로 서명한 후, 상기 무선랜 장치로 전송하고,

상기 확인 메시지는 상기 무선랜 장치가 상기 인증 서버로부터 획득한 상기 운전자 단말의 공개키를 이용하여 복호화되는 차량 인증 방법.

청구항 9

차량 내 무선랜 장치에 접속되는 승객 단말이 차량 인증 서비스를 제공하는 차량 인증 방법으로서,

상기 승객 단말이 상기 무선랜 장치에 접속되는 단계,

상기 무선랜 장치로부터 차량 정보를 수신하는 단계,

상기 차량 정보를 포함하는 차량 탑승 요청을 이동통신망을 통해 접속된 인증 서버로 전송하는 단계, 그리고

상기 인증 서버로부터 상기 차량 내 무선랜 장치에 접속된 운전자 단말이 전송한 차량 도착 정보를 수신하는 단계를 포함하고,

상기 차량 정보는,

상기 무선랜 장치의 SSID(Service Set Identifier)에 포함되는, 차량 인증 방법.

청구항 10

제9항에 있어서,
 상기 차량 도착 정보를 수신하는 단계 이후,
 차량 탑승 확인 정보를 상기 인증 서버로 전송하는 단계
 를 더 포함하는 차량 인증 방법.

청구항 11

제10항에 있어서,
 상기 차량 정보를 수신하는 단계는,
 상기 무선랜 장치의 개인키로 서명된 차량 정보를 수신하는 단계,
 전용 어플리케이션을 실행하여 접속된 인증 서버로부터 상기 무선랜 장치의 공개키를 수신하는 단계, 그리고
 상기 무선랜 장치의 공개키로 상기 서명된 차량 정보를 검증하는 단계
 를 포함하는 차량 인증 방법.

청구항 12

차량 내 무선랜 장치에 접속되는 고속도로 통행료 징수 시스템이 차량 인증 서비스를 제공하는 차량 인증 방법
 으로서,
 상기 고속도로 통행료 징수 시스템이 상기 무선랜 장치에 접속되는 단계,
 자신이 생성한 개인키로 결제 정보를 서명한 후, 상기 무선랜 장치로 전송하는 단계,
 상기 무선랜 장치로부터 결제 요청을 수신하는 단계, 그리고
 상기 결제 요청을 이동통신망을 통해 접속되고 상기 무선랜 장치가 접속된 인증 서버로 전송하는 단계를 포함하
 고,
 상기 무선랜 장치는,
 상호 인증된 운전자 단말에게 무선랜 장치의 SSID(Service Set Identifier)를 이용하여 차량 정보를 제공하는,
 차량 인증 방법.

청구항 13

제12항에 있어서,
 상기 무선랜 장치로부터 결제 요청을 수신하는 단계는,
 상기 무선랜 장치가 자신이 생성한 개인키로 서명한 결제 요청을 수신하는 단계, 그리고
 상기 무선랜 장치의 개인키에 대응하는 공개키를 상기 인증 서버로부터 획득하여 상기 결제 요청을 검증하는 단
 계를 포함하고,
 상기 인증 서버로 전송하는 단계는,
 검증된 결제 요청을 전송하는 차량 인증 방법.

청구항 14

제13항에 있어서,
 상기 무선랜 장치로 전송된 결제 정보는,
 상기 무선랜 장치와 접속된 운전자 단말로 전송되는 차량 인증 방법.

청구항 15

제14항에 있어서,

상기 인증 서버로 전송하는 단계는,
 검증된 결제 요청을 자신의 개인키로 서명한 후, 상기 인증 서버로 전송하고,
 상기 인증 서버로 전송하는 단계 이후,
 상기 인증 서버로 서명된 결제 완료 정보를 수신하여 검증하는 단계를 더 포함하고,
 상기 결제 완료 정보는 상기 운전자 단말로 전송되는 차량 인증 방법.

발명의 설명

기술 분야

[0001] 본 발명은 무선랜 장치 및 상기 무선랜 장치를 이용한 차량 인증 방법에 관한 것이다.

배경 기술

[0002] 운전자의 스마트폰과 차량에 설치된 무선랜 장치, 승객의 스마트폰을 이용하여 차량 탑승 전에 원거리에서 차량과 운전자, 승객, 통행 장치를 상호 인증하는 방법에 관한 것이다.

[0003] 최근에는 차량 안에 설치된 엔에프씨(NFC), 지그비(Zigbee), 블루투스 장치로 차량 정보를 확인하는 방법 등이 사용 또는 제안되고 있다. 하지만 승객이 차량에 탑승하여 차량을 확인하는 것은 안전하지 못하며, 운전자의 정보도 쉽게 확인이 불가능한 실정이다.

[0004] 또한, 승객이 강도로 변하여 운전자를 위협하는 사건이 발생하고 있으며, 차량, 운전자 뿐만 아니라 승객에 대한 확인(인증)도 필요한 실정이다.

[0005] 무선랜은 현재 수십 미터 통신이 가능한 802.11b(11M/bps), 802.11a(54M/bps), 802.11n(300M/bps)을 비롯하여 802.11ac와 같이 빠른 속도(1000M/bps)와 넓은 송신 거리(수Km)가 가능한 기술이 상용화 되고 있는 실정이다.

[0006] 또한, 무선랜 인증 방식은 패스워드 방식(EAP, Extensible Authentication Protocol), 인증서 방식(EAP-TLS, Extensible Authentication Protocol Transport Layer Security), 인증서 패스워드 혼용 방식(PEAP, Protected Extensible Authentication Protocol), SIM(Subscriber Identification Module) 카드 기반 방식(EAP-SIM) 등이 사용되고 있다.

[0007] 현재 인증서 기반 무선랜 인증 방식(EAP-TLS)이 상호 인증을 할 수 있는 가장 안전한 방법이지만 인증서를 안전하게 배포하고 효율적으로 운영할 수 있는 방안이 요구되고 있으며, 기존의 무선랜 인증은 서버(무선랜 장치, AP : Access Point)가 사용자(무선랜 카드)를 인증하기 위한 용도로만 주로 활용되고 있으며, 서버를 인증하기 위한 용도로는 제한적으로 사용되고 있다.

발명의 내용

해결하려는 과제

[0008] 따라서, 본 발명이 이루고자 하는 기술적 과제는 차량 탑승 전에 운전자 및 승객의 단말, 차량내 설치된 무선랜 장치를 이용하여 원거리에서 차량, 운전자, 승객, 통행 장치를 효율적으로 상호 인증하는 무선랜 장치 및 상기 무선랜 장치를 이용한 차량 인증 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 하나의 특징에 따르면, 무선랜 장치는 무선랜 통신을 통해 데이터를 송수신하는 무선랜 접속부, 이동통신망을 통해 데이터를 송수신하는 이동통신망 접속부, 상기 무선랜 접속부 및 상기 이동통신망 접속부와 연결되고, 무선랜 통신 환경 내에 위치하는 운전자 단말과 무선랜 통신으로 접속되어 상호 인증하며, 상기 운전자 단말을 통해 제공받은 운전자 정보가 포함된 차량 정보를 상기 무선랜 접속된 승객 단말로 전송하는 프로세서, 그리고 운전자 및 차량, 승객, 통행 장치, 인증 정보를 저장하는 메모리를 포함한다.

[0010] 상기 프로세서는,

[0011] 무선랜 장치 공개키 및 무선랜 장치 개인키를 생성하고, 상기 무선랜 장치 공개키를 이동통신망을 통해 접속된 인증 서버에 등록하고, 상기 인증 서버로부터 상기 무선랜 장치 공개키를 이용하여 생성한 무선랜 장치 인증서

및 상기 운전자 단말이 상기 인증 서버에 등록된 운전자 단말 공개키를 이용하여 생성한 운전자 단말 인증서를 수신하는 서비스 등록부, 무선랜 접속된 상기 운전자 단말과 상기 운전자 단말 인증서를 이용하여 인증을 수행하는 단말 인증부, 그리고 상기 무선랜 장치 개인키로 서명한 차량 정보를 생성하여 상기 승객 단말로 전송하는 서비스 실행부를 포함할 수 있다.

- [0012] 상기 단말 인증부는,
- [0013] 랜덤값을 포함하는 확인 요청 메시지를 상기 운전자 단말로 전송하고, 상기 운전자 단말의 운전자 단말 개인키로 서명된 확인 메시지를 상기 운전자 단말로부터 수신하며, 상기 인증 서버로부터 수신한 상기 운전자 단말 공개키로 상기 확인 메시지를 복호하여 상기 랜덤값을 추출하여 상기 랜덤값이 상기 확인 요청 메시지에 포함된 값과 일치하면, 상기 운전자 단말과 인증에 성공할 수 있다.
- [0014] 상기 서비스 실행부는,
- [0015] 상기 무선랜 장치의 SSID(Service Set Identifier), 빈 차량 여부, 운행 구역 및 상기 운전자 단말로부터 수신한 운전자 정보를 포함하는 차량 정보를 생성하고, 상기 무선랜 장치 개인키로 서명하여 상기 승객 단말로 전송할 수 있다.
- [0016] 상기 서비스 실행부는,
- [0017] 무선랜 접속된 고속도로 통행료 징수 시스템으로부터 상기 고속도로 통행료 징수 시스템의 제3 개인키로 서명된 결제 정보를 수신하고, 상기 인증 서버로부터 수신한 제3 공개키를 이용하여 상기 결제 정보를 검증하며, 검증에 성공하면, 결제 정보를 상기 운전자 단말로 전송하며, 상기 무선랜 장치 개인키로 결제 요청을 서명한 후, 상기 고속도로 통행료 징수 시스템으로 전송하고,
- [0018] 상기 결제 요청은 상기 인증 서버로 전달되어 상기 무선랜 장치에 통행료 과금 처리하는데 사용된다.
- [0019] 본 발명의 다른 특징에 따르면, 차량 인증 방법은 차량 내 무선랜 장치에 접속되는 운전자 단말이 차량 인증 서비스를 제공하는 차량 인증 방법으로서, 상기 운전자 단말이 이동통신망을 통해 접속된 인증 서버에 자신이 생성한 공개키를 등록한 후, 인증서를 수신하는 단계, 그리고 무선랜에 접속된 상기 무선랜 장치와 상호 인증하는 단계를 포함하고,
- [0020] 상기 상호 인증하는 단계는,
- [0021] 통신사 인증 서버로부터 발급 받은 운전자 및 승객의 스마트폰 인증서, 무선랜 장치, 통행 장치 인증서 가지고 무선랜 인증으로 사용할 수 있다.
- [0022] 상기 상호 인증하는 단계는,
- [0023] 상기 무선랜 장치로부터 확인 요청 메시지를 수신하는 단계, 그리고 상기 확인 요청 메시지에 포함된 랜덤값 및 운전자 정보가 포함된 확인 메시지를 상기 무선랜 장치로 전송하는 단계를 포함하고,
- [0024] 상기 랜덤값이 일치하고 서명이 검증이 되면, 상기 상호 인증에 성공할 수 있다.
- [0025] 상기 무선랜 장치로 전송하는 단계는,
- [0026] 시간 정보, 운전자 정보, 랜덤값을 포함하는 확인 메시지를 상기 운전자 단말의 개인키로 서명한 후, 상기 무선랜 장치로 전송하고,
- [0027] 상기 확인 메시지는 상기 무선랜 장치가 상기 인증 서버로부터 획득한 상기 운전자 단말의 공개키를 이용하여 복호화될 수 있다.
- [0028] 본 발명의 또 다른 특징에 따르면, 차량 인증 방법은 차량 내 무선랜 장치에 접속되는 승객 단말이 차량 인증 서비스를 제공하는 차량 인증 방법으로서, 상기 승객 단말이 상기 무선랜 장치에 접속되는 단계, 상기 무선랜 장치로부터 차량 정보를 수신하는 단계, 상기 차량 정보를 포함하는 차량 탑승 요청을 이동통신망을 통해 접속된 인증 서버로 전송하는 단계, 그리고 상기 인증 서버로부터 상기 차량 내 무선랜 장치에 접속된 운전자 단말이 전송한 차량 도착 정보를 수신하는 단계를 포함한다.
- [0029] 상기 차량 도착 정보를 수신하는 단계 이후,
- [0030] 차량 탑승 확인 정보를 상기 인증 서버로 전송하는 단계를 더 포함할 수 있다.

- [0031] 상기 차량 정보를 수신하는 단계는,
- [0032] 상기 무선랜 장치의 개인키로 서명된 차량 정보를 수신하는 단계, 전용 어플리케이션을 실행하여 접속된 인증 서버로부터 상기 무선랜 장치의 공개키를 수신하는 단계, 그리고 상기 무선랜 장치의 공개키로 상기 서명된 차량 정보를 검증하는 단계를 포함할 수 있다.
- [0033] 본 발명의 또 다른 특징에 따르면, 차량 인증 방법은 차량 내 무선랜 장치에 접속되는 고속도로 통행료 징수 시스템이 차량 인증 서비스를 제공하는 차량 인증 방법으로서, 상기 고속도로 통행료 징수 시스템이 상기 무선랜 장치에 접속되는 단계, 자신이 생성한 개인키로 결제 정보를 서명한 후, 상기 무선랜 장치로 전송하는 단계, 상기 무선랜 장치로부터 결제 요청을 수신하는 단계, 그리고 상기 결제 요청을 이동통신망을 통해 접속되고 상기 무선랜 장치가 접속된 인증 서버로 전송하는 단계를 포함한다.
- [0034] 상기 무선랜 장치로부터 결제 요청을 수신하는 단계는,
- [0035] 상기 무선랜 장치가 자신이 생성한 개인키로 서명한 결제 요청을 수신하는 단계, 그리고 상기 무선랜 장치의 개인키에 대응하는 공개키를 상기 인증 서버로부터 획득하여 상기 결제 요청을 검증하는 단계를 포함하고,
- [0036] 상기 인증 서버로 전송하는 단계는,
- [0037] 검증된 결제 요청을 전송할 수 있다.
- [0038] 상기 무선랜 장치로 전송된 결제 정보는,
- [0039] 상기 무선랜 장치와 접속된 운전자 단말로 전송될 수 있다.
- [0040] 상기 인증 서버로 전송하는 단계는,
- [0041] 검증된 결제 요청을 자신의 개인키로 서명한 후, 상기 인증 서버로 전송하고,
- [0042] 상기 인증 서버로 전송하는 단계 이후,
- [0043] 상기 인증 서버로 서명된 결제 완료 정보를 수신하여 검증하는 단계를 더 포함하고,
- [0044] 상기 결제 완료 정보는 상기 운전자 단말로 전송될 수 있다.

발명의 효과

- [0045] 본 발명의 실시예에 따르면, 차량 탑승 전에 차량 무선랜 장치와 운전자 및 승객의 스마트폰을 이용하여 원거리에서 차량, 운전자, 승객 및 통행 장치를 상호 인증할 수 있다.
- [0046] 또한, 차량 무선랜 장치의 SSID(Service Set Identifier)를 차량 식별 및 인증 ID 정보로 사용함으로써, 쉽게 차량 정보 확인 및 인증이 가능하다.
- [0047] 또한, 차량 무선랜 장치를 활용한 고속도로 통행료 징수 시스템은 빠른 속도로 진입 및 진출하는 다수의 차량을 원거리에서 쉽게 인증 및 결제가 가능하며, 고속도로 통행료 징수 톨게이트를 간단하게 구축할 수 있다.
- [0048] 또한, 통신사 인증 서버를 통해 스마트폰으로 인증서를 쉽게 배포 및 관리하고 해당 인증 정보를 무선랜 인증에 사용함으로써, 기존의 인증서 기반 무선랜 인증 방식(EAP-TLS)의 단점인 인증서 배포, 관리 문제를 효율적으로 해결할 수 있다.

도면의 간단한 설명

- [0049] 도 1은 본 발명의 실시예에 따른 네트워크 구성도이다.
- 도 2는 도 1의 무선랜 장치의 세부적인 구성을 나타낸 블록도이다.
- 도 3은 본 발명의 실시예에 따른 무선랜 장치와 운전자 단말을 인증 서버에 등록하여 인증하는 방법을 나타낸 흐름도이다.
- 도 4는 본 발명의 실시예에 따른 인증 서버를 통해 차량 및 운전자를 인증하는 방법을 나타낸 흐름도이다.
- 도 5는 본 발명의 실시예에 따른 고속도로 통행료 징수 시스템에서 차량 인증 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0050] 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 여러가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0051] 명세서 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.
- [0052] 또한, 명세서에 기재된 "...부", "...모듈" 의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.
- [0053] 이하, 도면을 참조로 하여 본 발명의 실시예에 따른 무선랜 장치 및 상기 무선랜 장치를 이용한 차량 인증 서비스 제공 방법에 대하여 상세히 설명한다.
- [0054] 도 1은 본 발명의 실시예에 따른 네트워크 구성도이고, 도 2는 도 1의 무선랜 장치의 세부적인 구성을 나타낸 블록도이다.
- [0055] 먼저, 도 1을 참조하면, 차량(100)에는 무선랜 장치(200) 및 운전자 단말(300)이 설치된다. 여기서, 차량(100)은 택시, 버스, 렌터카, 셰어링, 개인 차량 등을 포함한다. 그리고 무선랜 장치(200)는 차량(100)내 텔레메틱스 시스템(미도시)에 탑재하거나 또는 스마트폰으로 대체 가능하다. 그리고 차량(100)의 외부에는 무선랜 장치(200)의 설치 여부, 즉, 안심 택시 등을 확인할 수 있는 표식이 설치될 수 있다.
- [0056] 무선랜 장치(200)는 이동통신, 무선랜, 무선 신호 증폭 기능을 동시에 수행할 수 있다. 그리고 무선랜 장치(200)는 와이파이(WIFI) AP 모드 및 와이파이(WIFI) 통신 모드로 사용될 수 있으며, 기타 무선랜 프로토콜을 적용할 수 있다. 즉, 무선랜 장치(200)는 이동통신망(400)을 통해 인증 서버(500)에 접속한다. 여기서, 인증 서버(500)는 차량, 운전자, 승객, 통행 장치를 인증하는 서버로서, 통신 사업자 서버일 수도 있다.
- [0057] 무선랜 장치(200)는 차량 번호 및 운전자 핸드폰 번호를 활용하여 무선랜 SSID(Service Set Identifier) 및 인증 ID로 사용할 수 있다.
- [0058] 무선랜 장치(200)는 등록된 운전자 단말(300)이 무선랜 통신 반경 이내에 존재해야 승객 단말(600)과 인증 절차를 수행할 수 있다. 따라서, 차량이 도난 당해도 해당 차량 운전자 소유의 운전자 단말(300)이 없으면 차량내 무선랜 장치(200)를 인증할 수 없다. 그리고 무선랜 장치(200)가 설치된 차량(100)과 운전자 단말(300)이 모두 도난 당한 경우에도 주기적인 인증 비밀번호 요구, 지문 인식, 운전자 얼굴 확인, 인증서 폐지 등의 과정을 통해 차량 인증을 확인 할 수 있다.
- [0059] 인증 서버(500)는 차량, 운전자, 승객, 통행장치의 인증 정보를 가지고 상호 인증 가능하도록 확인해준다. 또한, 차량의 GPS 위치 정보를 통해 승객 단말(600)로 제공할 수 있다.
- [0060] 승객 단말(600)은 차량(100)에 탑재된 무선랜 장치(200)가 송출하는 차량 정보를 통해 차량 정보에 포함된 차량(100)의 GPS 위치, 승객 탑승 유무, 운행 경로, 승객과의 거리 등을 확인 할 수 있다. 승객 단말(600)은 인증 서버(500)로부터 제공받은 인증 정보를 통해 무선랜 장치(200)를 인증한다. 이때, 무선랜 장치(200)는 무선 채널 간섭 최소화를 위해 차량번호(4자리)를 채널수(4개)로 나눈 집합으로 무선 권장 채널 1, 3, 9, 13 채널을 설정할 수도 있다.
- [0061] 한편, 승객 단말(600)은 인증된 무선랜 장치(200)로 탑승 예약을 요청하면서, 승객의 정보, 즉 현재 위치, 목적지, 주행 요청 경로를 전송할 수 있다. 그리고 승객은 승객 단말(600)을 이용하여 인증된 무선랜 장치(200)가 탑재된 택시를 원거리에서 승차 전에 확인 후 승차할 수 있다. 즉, 승객은 앞에 도착한 택시가 인증된 택시인지를 무선랜을 통해 확인하고 택시에 탑승한다.
- [0062] 승객은 앞에 도착한 택시를 근거리 통신(블루투스 통신) 등을 통해 재확인 할 수 있다.
- [0063] 이때, 차량 탑승 전에 차량 외부 손잡이에 설치된 NFC 장치를 스마트폰 모바일카드로 접촉하여 차량과 운전자 재인증(확인) 및 정보 전송을 할 수 있다.
- [0064] 또한, 운전자 단말(300)과 차량 무선랜 장치(200)는 승객 단말(600)로 운행 정보(현 위치, 운행 경로, 도착 예정 시간)를 제공할 수 있다.

- [0065] 여기서, 차량 인증 서비스는 승객이 차량(100)에 탑승 전에 차량(100)에 설치된 무선랜 장치(200), 운전자 단말(300), 승객 단말(600), 고속도로 통행료 징수 시스템(700) 간에 원거리에서 상호 인증하여 안전하고 편리한 차량 서비스를 제공하는 서비스이다. 이러한 차량 인증 서비스는 택시, 버스, 카셰어링, 하이패스, 주차 관제 등의 서비스에서 활용될 수 있다.
- [0066] 승객 단말(600)은 내장된 무선랜 카드에서 무선랜 장치(200)와의 신호 세기(거리비)를 확인할 수 있다. 즉 신호 세기를 상세화하여 거리로 표시할 수 있다.
- [0067] 무선랜 장치(200)는 무선랜 통신 반경 이내에 접근하거나 또는 위치하는 승객 단말(600) 및 고속도로 통행료 징수 결제 시스템(700)과 연결된다. 이러한 무선랜 장치(200)는 와이파이(WIFI) 장치일 수 있다.
- [0068] 차량 운전자는 관계 서비스 사업자, 예컨대 통신사에 차량 인증 서비스를 가입한다. 이때, 차량 인증 서비스는 'WIFI 안심 택시 서비스'일 수 있다. 가입시 단말 가입 정보 및 차량 등록 정보를 제출하고 신분 증명을 한 후, 사업자로부터 인증된 무선랜 장치(200)를 제공받거나 또는 무선랜 장치(200) 및 무선랜 장치 인증서를 제공받아 차량(100)에 설치한다.
- [0069] 운전자 단말(300), 승객 단말(600), 고속도로 통행료 징수 시스템(700) 역시 인증 서버(500)에 접속하여 차량 인증 서비스 등록을 한다.
- [0070] 즉, 무선랜 장치(200) 및 운전자 단말(300)은 인증 서버(500)에 등록되어 사전에 인증을 받는다. 그리고 무선랜 장치(200)와 운전자 단말(300)간 무선 통신으로 해당 차량에 해당 운전자가 탑승했는지 여부를 인증한다. 이는 서비스 유형에 따라 생략 가능하다.
- [0071] 또한, 승객 단말(600)은 전용 어플리케이션을 통해 무선 통신(WIFI)으로 검색된 근처의 차량, 즉 무선랜 장치(200)를 인증 서버(500)에서 제공받은 인증 정보(인증서 등)와 비교하여 승차 전에 차량을 인증하고 운전자 정보를 확인한다. 또한, 운전자 단말(300)과 승객 단말(600)이 무선랜 장치(200)에 접속되면 운전자와 승객이 상호 인증할 수 있다.
- [0072] 승객 단말(600)이 무선랜 장치(200)에 접속하면 인증 서버(500)로부터 인증된 차량 정보 및 운전자 정보를 제공받는다. 그리고 무선랜 장치(200)로 운전자에게 원하는 목적지, 경로 정보를 제공하면, 무선랜 장치(200)는 이러한 정보를 운전자 단말(300)로 전송할 수 있다.
- [0073] 또한, 인증 서버(500)는 차량 및 운전자 정보(상태, 위치 등)를 승객 단말(600)로 전송할 수 있다.
- [0074] 고속도로 통행료 징수 시스템(700)의 무선랜 장치는 SSID를 통해 통행료 징수 시스템 ID 및 인증 ID를 차량으로 제공하고, 이때, 차량 무선랜 장치(200)는 고속도로 통행료 징수 시스템(700) 무선랜 장치에 접속하여 해당 접속 정보를 신뢰되고 허용된 AP인지를 인증 서버(500)를 통해 확인할 수 있다.
- [0075] 여기서 고속도로 통행료 징수 시스템(700)은 구현 방식에 따라 하이패스 시스템 뿐만 아니라 차량 주문 시스템, 주차 관리 시스템 등으로 구현 될 수 있다.
- [0076] 차량 인증 서비스 등록 이후, 무선랜 장치(200), 운전자 단말(300), 승객 단말(600), 고속도로 통행료 징수 시스템(700)은 상호 인증 후, 차량 인증 서비스를 제공받는다.
- [0077] 여기서, 무선랜 장치(200)는 세부적으로 도 2와 같이 구성될 수 있다. 도 2를 참조하면, 무선랜 장치(200)는 무선랜 접속부(210), 이동통신망 접속부(230), 메모리(250) 및 프로세서(270)를 포함한다.
- [0078] 무선랜 접속부(210)는 무선랜 통신을 통해 데이터를 송수신하며, AP 모드 및 무선 통신 모드로 동작 될 수 있다.
- [0079] 이동통신망 접속부(230)는 이동통신망(400)에 접속하여 이동통신망(400)을 통해 데이터를 송수신한다. 여기서, 이동통신망(400)은 3G망, LTE(Long Term Evolution)망일 수 있다.
- [0080] 메모리(250)는 동적 랜덤 액세스 메모리(Dynamic Random Access Memory, DRAM), 램버스 DRAM(Rambus Dynamic Random Access Memory, RDRAM), 동기식 DRAM(Synchronous Dynamic Random Access Memory, SDRAM), 정적 RAM(Static Random Access Memory, SRAM) 등의 RAM, SDRAM, DISK, USIM, 보안토큰과 같은 매체로 다중으로 구현될 수 있다. 이러한 메모리(250)는 무선랜 장치(200)의 SSID, 인증 정보, 차량 정보, 운전자 정보 등을 저장한다.
- [0081] 여기서, SSID는 차량 번호 대신 차량(100)의 식별정보로 사용된다. SSID에 차량 정보를 포함시키는 예는 다음과

같다. 즉, SSID가 0_3372_33가_모범_서울_경기일 때, 탑승가능여부OX_차량번호4자리_차량나머지번호_운전자정보_운행구역_운행구역 등이 포함될 수 있다.

- [0082] 또한, 인증 정보는 인증서 정보를 포함하여 안전하게 저장될 수 있는 하드웨어 기반, 즉, USIM(Universal Subscriber Identity Module), 보안 토큰 등의 저장 방식이 사용될 수 있다.
- [0083] 프로세서(270)는 중앙처리 유닛(central processing unit, CPU)이나 기타 칩셋, 마이크로프로세서 등으로 구현될 수 있다. 프로세서(270)는 서비스 등록부(271), 단말 인증부(273) 및 서비스 실행부(275)를 포함한다.
- [0084] 서비스 등록부(271)는 인증 서버(500)에 차량 인증 서비스를 위한 정보를 등록한다. 단말 인증부(273)는 운전자 단말(300)과 상호 인증한다. 서비스 실행부(275)는 무선랜 통신으로 차량 정보 및 운전자 정보, 인증 정보를 전송한다.
- [0085] 다시, 도 1을 참조하면, 고속도로 통행료 징수 시스템(700)이 양방향으로 설치되는 경우 무선랜 장치(200)가 진입 및 진출을 혼동하지 않도록 무선통신 통신 거리를 조정하거나, 무선 통신 신호의 세기 증가율에 따라 방향을 확인하거나, 구역을 이중으로 하여 재차 확인하거나, 차량 상태(진입정보, 위치 등)를 확인하여 인증 및 결제가 가능하도록 할 수 있다.
- [0086] 이때, 고속도로 통행료 징수 시스템(700)이 설치된 톨게이트를 통과하는 차량 내 무선랜 장치(200), 운전자 단말(300), 고속도로 통행료 징수 시스템(700)은사전에 인증 서버(500)로부터 인증을 받는다. 그리고 인증 서버(500)는 고속도로 통행료 징수 시스템(700)에 신뢰된 인증정보를 배포하고, 차량(100)이 고속도로 통행료 징수 시스템(700)을 지나갈 때 무선 통신으로 안전하게 인증 및 결제를 한다. 인증 서버(500)는 결제가 완료되면 운전자 단말(300)로 결제 정보를 제공한다.
- [0087] 고속도로 통행료 징수 시스템(700)은 SSID로 통행료 징수 구역 정보를 차량 무선랜 장치(200)로 제공할 수 있다. 즉, 무선랜 장치(200)는 고속도로 톨게이트 정보를 고속도로 통행료 징수 시스템(700)으로부터 전달 받고, 차량 진입 및 진출 정보를 무선랜 통신을 통해 고속도로 통행료 징수 시스템(700)에 전달한다. 그리고 고속도로 통행료 징수 시스템(700)은 인증 서버(500)에 차량 확인 및 결제를 요청하고 인증 서버(500)로부터 응답 받는다. 고속도로 통행료 징수 시스템(700)은 차량에 탑재된 무선랜 장치(200)에게 진입 및 진출 처리 결과를 전달하고, 무선랜 장치(200)는 자신의 차량 상태를 고속도로 진입 또는 진출 상태로 변경할 수 있다.
- [0088] 도 1 및 도 2의 구성을 토대로 차량 인증 서비스를 제공하는 일련의 과정을 실시예 별로 설명하면 다음과 같다. 이때, 도 1 및 도 2의 구성 요소에 대한 설명은 동일한 도면 부호를 사용한다.
- [0089] 먼저, 도 3은 본 발명의 실시예에 따른 무선랜 장치와 운전자 단말을 인증 서버에 등록하여 인증하는 방법을 나타낸 흐름도이다.
- [0090] 도 3을 참조하면, 무선랜 장치(200)의 이동통신망 접속부(230)는 이동통신망(400)을 통해 인증 서버(500)에 접속한다(S101).
- [0091] 무선랜 장치(200)의 서비스 등록부(271)는 무선랜 장치 공개키 및 무선랜 장치 개인키를 생성(S103). 그리고 서비스 등록부(271)는 무선랜 장치 공개키를 인증 서버(500)에 등록한다(S105).
- [0092] 한편, 운전자 단말(300)은 이동통신망(400)을 통해 인증 서버(500)에 접속한다(S107). 운전자 단말(300)은 운전자 단말 공개키 및 운전자 단말 개인키를 생성(S109). 그리고 운전자 단말 공개키를 인증 서버(500)에 등록한다(S111).
- [0093] 인증 서버(500)는 S105 단계에서 수신된 무선랜 장치 공개키를 이용하여 무선랜 장치 인증서를 생성하고, 운전자 단말 공개키를 이용하여 운전자 단말 인증서를 생성한다(S113). 그리고 무선랜 장치 인증서 및 운전자 단말 인증서를 무선랜 장치(200)에게 전송한다(S115). 그리고 운전자 단말(300)에게는 운전자 단말 인증서를 전송한다(S117).
- [0094] 여기서, 무선랜 장치 인증서는 차량번호 기반의 차량 인증서이고, 운전자 단말 인증서는 핸드폰 번호 기반의 운전자 인증서일 수 있다. 그리고 무선랜 장치(200)와 운전자 단말 인증서의 위변조를 차단하기 위해 통신사는 무선랜 장치 등록과 스마트폰 인증서 등록 시 신원 확인을 한다. 이는 기존의 통신사에서 제공했던 USIM을 통해 쉽게 배포될 수 있다.
- [0095] 무선랜 장치(200)는 생성한 랜덤값을 포함하는 확인 요청 메시지를 생성하여 운전자 단말(300)에게 전송한다(S119).

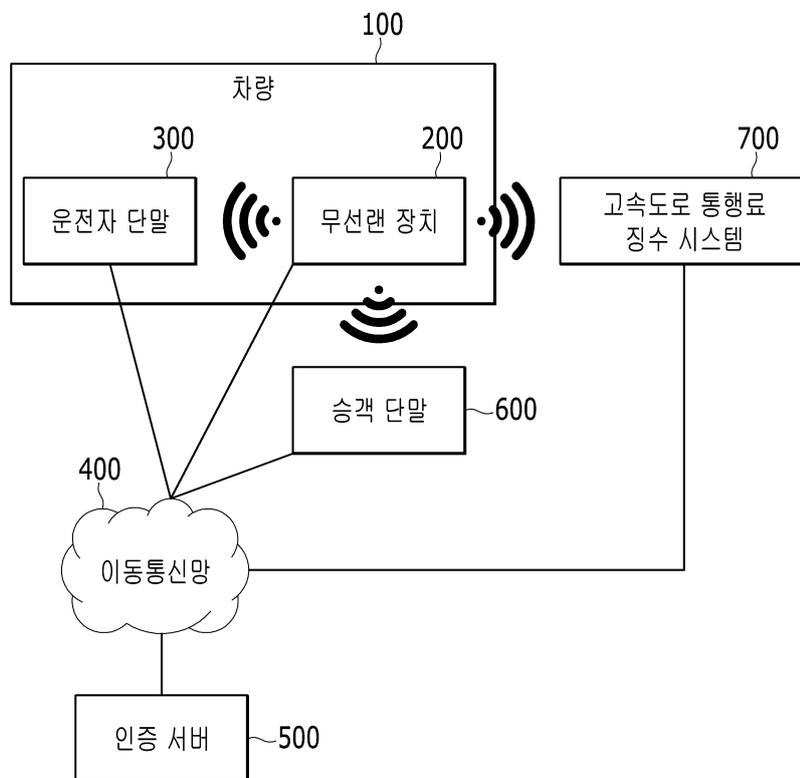
- [0096] 운전자 단말(300)은 시간 정보, 운전자 정보 및 랜덤값을 포함하는 확인 메시지를 생성하는데, S109 단계에서 생성한 운전자 단말 개인키로 서명한 확인 메시지를 생성한다(S121). 그리고 무선랜 장치(200)에게 확인 메시지를 전송한다(S123).
- [0097] 무선랜 장치(200)의 단말 인증부(273)는 인증 서버(500)로 운전자 단말 인증서를 검증 요청하여 응답을 수신(S125)하여 확인 메시지를 검증한다(S127).
- [0098] 이때, 확인 메시지를 복호하여 시간 정보, 운전자 정보 및 랜덤값을 추출한다. 그리고 랜덤값이 S119 단계에서 전송된 값과 일치하는지 판단한다(S129). 일치하면 검증에 성공한 경우로 판단하여 운전자 단말 인증을 완료한다(S131). 반면, 일치하지 않으면 검증에 실패한 경우로 판단하여 운전자 단말 인증 실패 처리한다(S133).
- [0099] 이후, 무선랜 장치(200)의 단말 인증부(273)는 S131 단계, S133 단계에서의 운전자 인증 결과를 인증 서버(400)로 전송한다(S135).
- [0100] 도 4는 본 발명의 실시예에 따른 인증 서버를 통해 차량 및 운전자를 인증하는 방법을 나타낸 흐름도이다.
- [0101] 도 4를 참조하면, 무선랜 장치(200)의 무선랜 접속부(210)는 무선랜 통신으로 차량(100)내 운전자 단말(300)과 무선랜 통신으로 접속한다(S201). 그리고 무선랜 장치(200)의 이동통신망 접속부(230)는 이동통신망(400)을 통해 인증 서버(500)에 접속한다(S203).
- [0102] 무선랜 장치(200)의 서비스 실행부(275)는 메모리(250)로부터 획득한 SSID, 빈 차량 여부, 운행 구역, 운전자 정보를 포함하는 차량 정보를 생성한다(S205). 이때, 빈 차량 여부, 운행 구역, 운전자 정보는 운전자 단말(300)을 통해 획득된 정보일 수 있다.
- [0103] 여기서, 운전자는 운전자 단말(300)을 통해 인증 서버(500)로 운행 시작 정보를 등록한다. 공유 차량을 시간대 별로 다른 운전자가 운전할 수 있으므로 해당 차량에 해당 운전자를 등록할 수 있다.
- [0104] 무선랜 장치(200)의 서비스 실행부(275)는 S205 단계에서 생성한 차량 정보를 무선랜 장치 개인키로 서명한다(S207).
- [0105] 이후, 승객 단말(600)은 사전에 인증 서버(500)에 접속하여 다운로드한 전용 어플리케이션을 실행한다(S209).
- [0106] 승객 단말(600)은 무선랜 장치(200)의 무선랜 통신 반경 이내에 진입하거나 또는 위치하면, 차량 무선랜 장치(200)의 무선랜 정보를 확인한다(S211). 그러면, 무선랜 장치(200)의 서비스 실행부(275)는 S207 단계에서 서명한 차량 정보를 승객 단말(600)로 전송한다(S213).
- [0107] 승객 단말(600)은 이동통신망(400)을 통해 인증 서버(500)에 무선랜 장치 공개키를 요청하여 수신한다(S215). 그리고 S217 단계에서 수신한 무선랜 장치 공개키로 차량 정보를 검증한다(S217). 즉, 차량 정보를 무선랜 장치 공개키로 복호하여 무선랜 장치(200)가 설치된 차량(100)의 정보, 즉, 빈차량 여부, 운전자 정보를 확인한다.
- [0108] 승객 단말(600)은 무선랜 장치(200)와 운전자, 차량, 승객 정보를 교환한다(S219).
- [0109] 도 5는 본 발명의 실시예에 따른 고속도로 통행료 징수 시스템에서 차량 인증 방법을 나타낸 흐름도이다.
- [0110] 도 5를 참조하면, 도 3과 같은 과정을 통해 무선랜 장치(200)가 운전자 단말(200)과 인증 절차가 완료(S301)된 상태에서 고속도로 통행료 징수 시스템(700)이 설치된 톨게이트 구간에서 근접하면, 무선 통신(WIFI)로 고속도로 통행료 징수 시스템에 접속된다(S303).
- [0111] 그러면, 고속도로 통행료 징수 시스템(700)은 자신이 생성한 고속도로 통행료 징수 시스템 개인키로 결제 정보를 서명(S305)한 후, 무선랜 장치(200)로 전송한다(S307).
- [0112] 무선랜 장치(300)의 서비스 실행부(275)는 이동통신망(400)을 통해 인증 서버(500)로 접속하여 고속도로 통행료 징수 시스템 공개키로 결제 정보를 검증한다(S309). 즉, 결제 정보를 복호화하여 결제 정보를 획득한다.
- [0113] 무선랜 장치(300)의 서비스 실행부(275)는 무선랜 장치 개인키로 결제 정보를 서명하여 운전자 단말(300)로 전송한다(S311).
- [0114] 그러면, 운전자 단말(300)은 인증 서버(500)에 요청하여 획득한 무선랜 장치 공개키로 결제 정보를 검증 즉, 복호화하여 결제 정보를 추출한다.
- [0115] 한편, 무선랜 장치(300)의 서비스 실행부(275)는 S307 단계에서 수신한 결제 정보를 수락할 것인지 판단한다(S313). 즉, 운전자가 무선랜 장치(300)에 장착된 터치 입력부 또는 입력 수단을 통해 수락 여부를 입력하면,

입력된 내용에 기초하여 수락 여부를 판단한다.

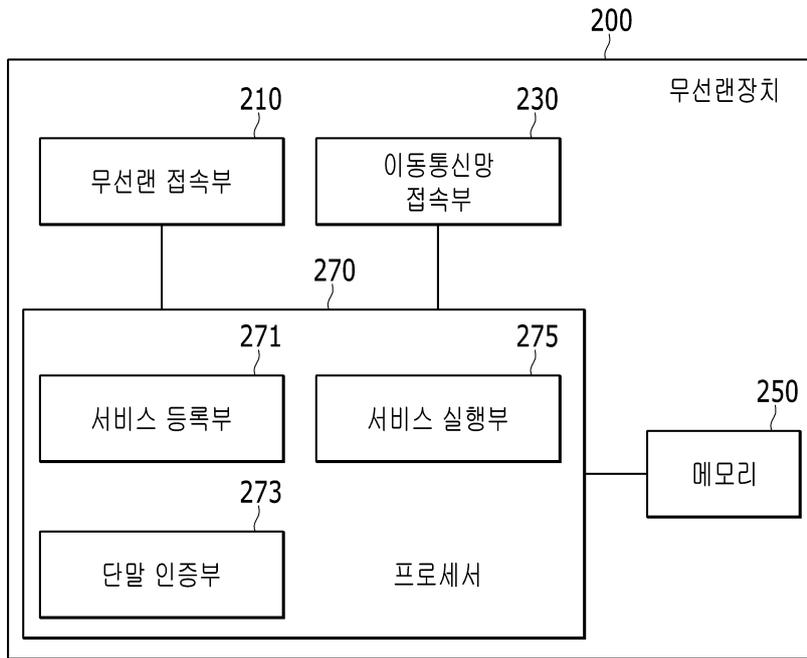
- [0116] 이때, 결제 수락이 선택되지 않으면, 결제 불승인을 고속도로 통행료 징수 시스템(700)으로 전송한다(S315).
- [0117] 반면, 결제 수락이 선택되면, 무선랜 장치 개인키로 결제 요청을 서명(S317)한 후, 고속도로 통행료 징수 시스템(700)으로 전송한다(S319).
- [0118] 고속도로 통행료 징수 시스템(700)은 S319 단계에서 수신된 결제 요청을 인증 서버(500)로부터 획득한 무선랜 장치 공개키로 검증(S321)한다. 즉, 결제 요청 정보를 획득한다. 그러면, 획득한 결제 요청을 다시 고속도로 통행료 징수 시스템 개인키로 서명(S323)한 후, 인증 서버(500)로 전송한다(S325).
- [0119] 그러면, 인증 서버(500)는 결제 요청을 고속도로 통행료 징수 시스템(700) 공개키로 검증하여 결제 요청 정보를 획득한 후, 결제 프로세스를 수행한다(S327). 즉, 결제 프로세스는 과금을 수행한다. 이때, 과금 식별 정보로는 결제 정보에 포함된 무선랜 장치(200)의 SSID가 포함될 수 있다.
- [0120] 인증 서버(500)는 결제 프로세스가 완료되면, 결제 완료 정보를 자신이 생성한 인증 서버 개인키로 서명하여 고속도로 통행료 징수 시스템(700)으로 전송한다(S329). 그러면, 고속도로 통행료 징수 시스템(700)은 사전에 수신한 인증서 또는 인증 서버(500)에서 수신한 인증 서버 공개키로 복호화하여 결제 완료 정보를 획득한다.
- [0121] 한편, 인증 서버(500)는 결제 정보를 운전자 단말(300)에게 전송한다(S331).
- [0122] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.
- [0123] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

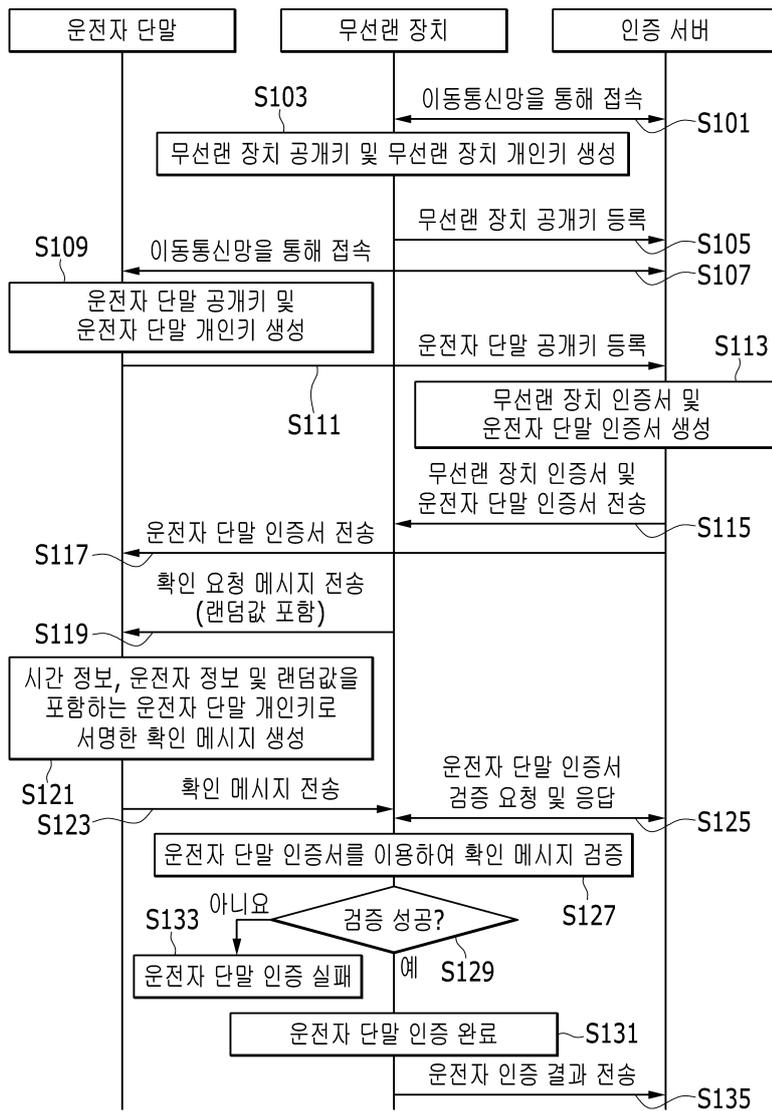
도면1



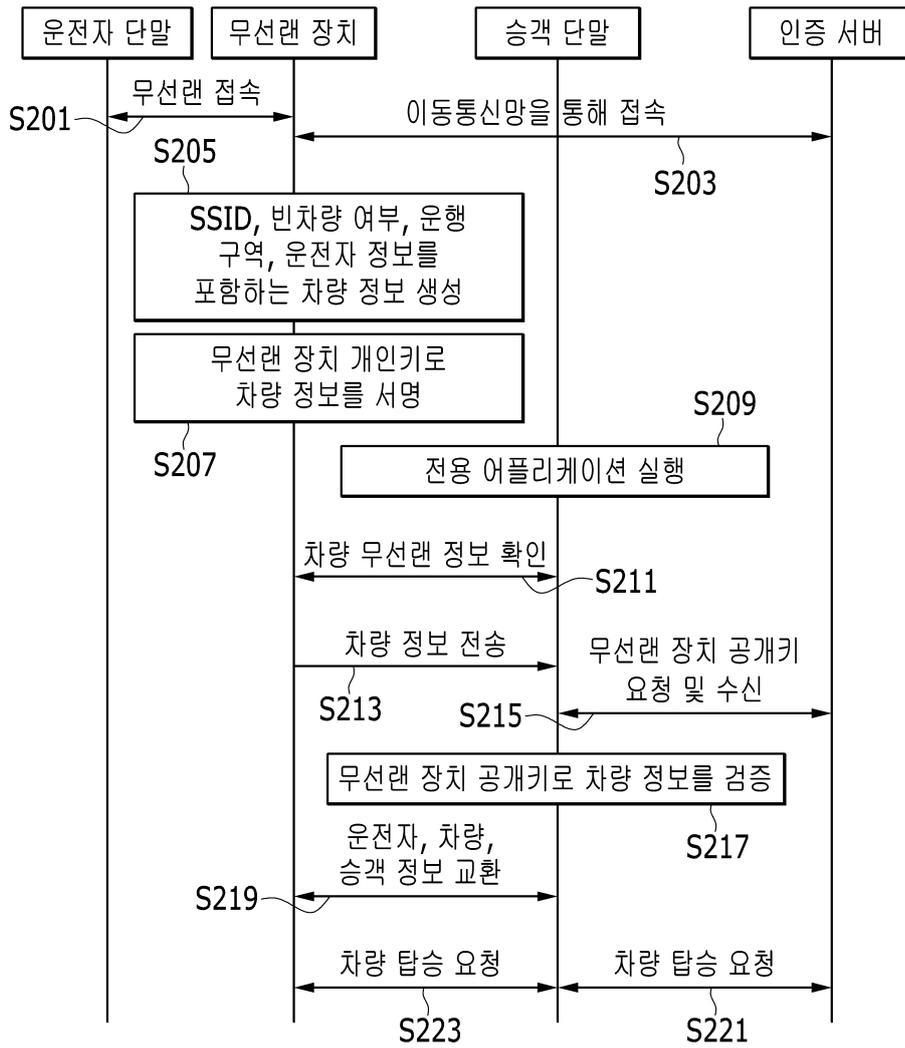
도면2



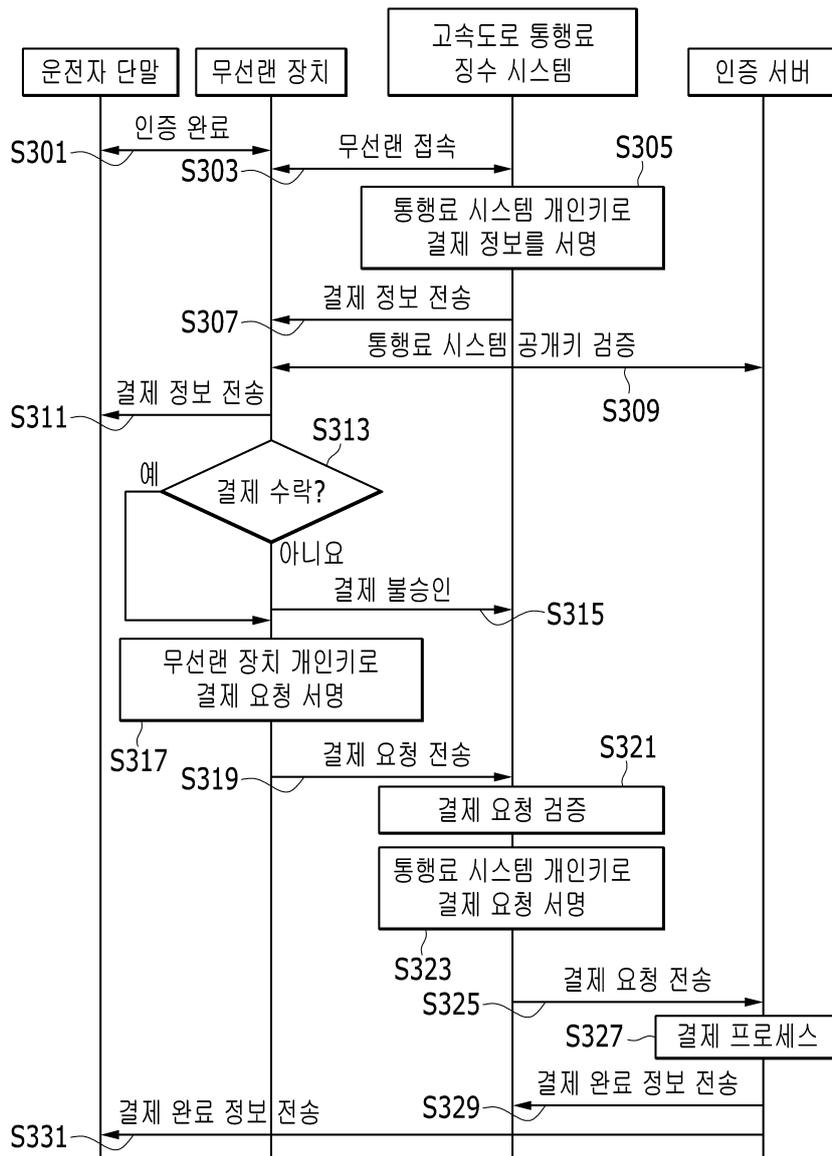
도면3



도면4



도면5



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항12

【변경전】

상기 운전자 단말에게 ~

【변경후】

운전자 단말에게 ~

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항1

【변경전】

상기 무선랜 장치의 SSID~

【변경후】

무선랜 장치의 SSID~