



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년09월07일
(11) 등록번호 10-2575725
(24) 등록일자 2023년09월01일

(51) 국제특허분류(Int. Cl.)
B60L 50/50 (2019.01)
(52) CPC특허분류
B60L 53/60 (2019.02)
B60L 53/16 (2019.02)
(21) 출원번호 10-2018-0142020
(22) 출원일자 2018년11월16일
심사청구일자 2021년10월21일
(65) 공개번호 10-2020-0057518
(43) 공개일자 2020년05월26일
(56) 선행기술조사문헌
US20180337957 A1
KR1020170045876 A
KR1020170014460 A
KR1020160134048 A

(73) 특허권자
현대자동차주식회사
서울특별시 서초구 현릉로 12 (양재동)
기아 주식회사
서울특별시 서초구 현릉로 12 (양재동)
(72) 발명자
이돈형
경기도 안양시 동안구 동안로 11, 무궁화코오롱,
건영아파트 710-1002
이정희
서울특별시 관악구 양지길 50-5, 관악우정하이비
전아파트 101-1702
(74) 대리인
특허법인태평양

전체 청구항 수 : 총 16 항

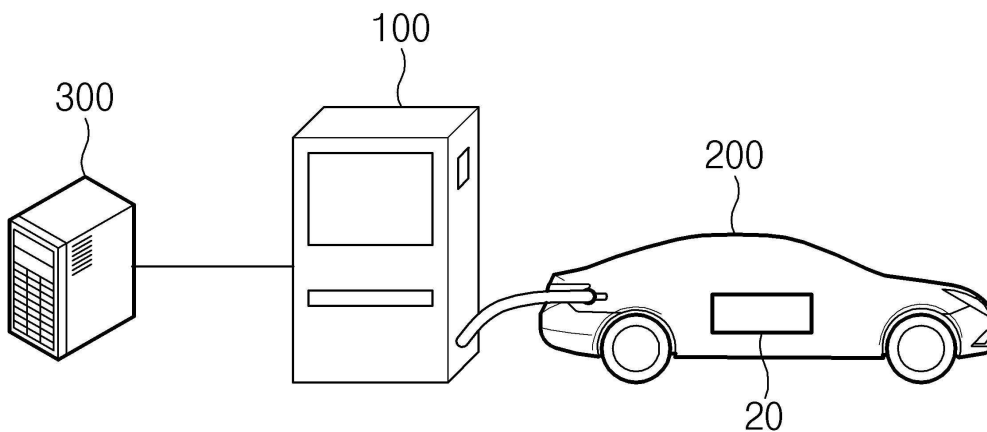
심사관 : 안정환

(54) 발명의 명칭 전기차 충전 제어 장치, 시스템 및 방법

(57) 요약

본 발명의 전기차 충전 제어 시스템은 공개키 암호화 방식을 이용하여 무결성이 확인된 현재 시간 정보를 추출하고, 상기 추출된 현재 시간 정보를 기반으로 충전 계약 인증서가 유효한 것으로 판단하면, 충전 단말기로부터 충전하도록 하는 전기차와, 상기 공개키 암호화 방식을 이용하여 무결성이 확인된 현재 시간 정보를 상기 전기차에 전송하는 서버 및 상기 전기차와 연결되는 충전 단말기를 포함하여, 전력선 통신을 이용한 차량 충전 및 충전 과금 시에 사용되는 인증서의 유효성을 정확하게 판단할 수 있고, 전기차 충전 시 해킹에 대한 보안을 강화할 수 있다.

대표도 - 도1



(52) CPC특허분류

B60L 53/305 (2019.02)

B60Y 2200/91 (2013.01)

Y02T 90/16 (2020.08)

(72) 발명자

김현수

경기도 수원시 장안구 만석로20번길 28, 한라비발
디아파트 633-801

노태선

서울특별시 도봉구 방학로 200, 신동아아파트
114-909

명세서

청구범위

청구항 1

시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하고, 상기 서버로부터 수신되는 암호화된 시간 정보 응답 메시지를 복호화하여 현재 시간 정보를 추출하고, 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하고, 판단 결과에 기초하여 충전 동작을 제어하는 전기차 충전 제어 장치; 및

상기 전기차 충전 제어 장치로부터 수신되는 상기 시간 정보 요청 메시지를 개인키를 이용하여 복호화하고, 상기 현재 시간 정보를 포함하는 시간 정보 응답 메시지를 상기 개인키로 암호화하여 상기 전기차 충전 제어 장치로 전달하는 서버를 포함하는 전기차 충전 제어 시스템.

청구항 2

청구항 1에 있어서,

상기 인증서의 유효성이 판단되면 충전을 수행하는 충전 단말기를 더 포함하는 전기차 충전 제어 시스템.

청구항 3

청구항 2에 있어서,

상기 전기차 충전 제어 장치는 상기 충전 단말기와 전력선 통신하는 전기차 충전 제어 시스템.

청구항 4

청구항 1에 있어서,

상기 전기차 충전 제어 장치는

상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화하는 전기차 충전 제어 시스템.

청구항 5

청구항 1에 있어서,

상기 전기차 충전 제어 장치는

상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화하지 못한 것으로 판단하면, EIM(External Identification Means)방식으로 충전하도록 제어하는 전기차 충전 제어 시스템.

청구항 6

청구항 1에 있어서,

상기 전기차 충전 제어 장치는

상기 현재 시간 정보가 추출되면 프로토콜 암호화를 수행하는 전기차 충전 제어 시스템.

청구항 7

청구항 1에 있어서,

상기 전기차 충전 제어 시스템은

상기 추출된 시간 정보를 기반으로 상기 인증서가 유효하지 않으면 충전을 종료하도록 제어하는 전기차 충전 제어 시스템.

청구항 8

청구항 1에 있어서,

상기 전기차 충전 제어 시스템은

상기 추출된 시간 정보를 기반으로 상기 인증서가 유효한 것으로 판단하면, PnC(Plug and Charge) 방식으로 충전하도록 제어하는 전기차 충전 제어 시스템.

청구항 9

시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하고, 상기 서버로부터 수신되는 암호화된 시간 정보 응답 메시지를 수신하는 통신부; 및

상기 암호화된 시간 정보 응답 메시지를 상기 공개키로 복호화하여 현재 시간 정보를 추출하고, 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하고, 판단 결과에 기초하여 충전 동작을 제어하는 제어부를 포함하는 전기차 충전 제어 장치.

청구항 10

시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하는 단계;

상기 서버로부터 암호화된 시간 정보 응답 메시지를 수신하는 단계;

상기 수신된 시간 정보 응답 메시지를 복호화하여 현재 시간 정보를 추출하는 단계;

상기 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하는 단계; 및

상기 판단 결과에 기초하여 충전 동작을 제어하는 단계를 포함하는 전기차 충전 제어 방법.

청구항 11

청구항 10에 있어서,

상기 서버로부터 암호화된 시간 정보 응답 메시지를 수신하는 단계는

상기 서버에서 상기 암호화된 시간 정보 요청 메시지를 수신하는 단계;

상기 서버에서 개인키로 상기 암호화된 메시지를 암호화 해제하는 단계;

상기 서버에서 시간 정보 응답 메시지를 생성하는 단계;

상기 서버에서 상기 시간 정보 응답 메시지를 상기 개인키를 이용하여 암호화하는 단계; 및

상기 서버에서 암호화된 상기 시간 정보 응답 메시지를 전기차 충전 제어장치로 전송하는 단계를 포함하는 전기차 충전 제어 방법.

청구항 12

청구항 10에 있어서,

상기 수신된 시간 정보 응답 메시지는 상기 공개키를 이용하여 복호화하는 전기차 충전 제어 방법.

청구항 13

청구항 12에 있어서,

상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화하지 못한 것으로 판단하면, EIM(External Identification Means) 방식으로 충전하도록 제어하는 전기차 충전 제어 방법.

청구항 14

청구항 10에 있어서,

상기 현재 시간 정보가 추출되면 프로토콜 암호화를 수행하는 단계를 더 포함하는 전기차 충전 제어 방법.

청구항 15

청구항 10에 있어서,

상기 인증서가 유효성이 판단되지 않으면 충전을 종료하도록 제어하는 전기차 충전 제어 방법.

청구항 16

청구항 10에 있어서,

상기 인증서의 유효성이 판단되면, PnC(Plug and Charge)방식으로 충전하도록 제어하는 전기차 충전 제어 방법.

발명의 설명

기술 분야

[0001] 본 발명은 전기차 충전 제어 장치, 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 최근에는 전기차 충전 방식의 하나로 전력선 통신(PLC:Power Line Communication)을 이용하여 고객인증, 충전, 과금이 동시에 이루어지도록 하는 충전방식이 제안되고 있다. 전력선 방식은 전기차 충전 시 충전케이블을 사용하여 별도의 유무선 장치 설치없이 충전 및 통신이 이루어지도록 하는데, 차량 구매시 운전자가 인증기관(충전 사업소)으로부터 수신한 인증서를 기반으로 차량을 인증하고, 충전에 대한 과금이 자동으로 이루어지도록 할 수 있다.

[0003] 이를 위하여, 차량은 유효한 인증서가 필요한데, 인증서가 유효한지 여부를 판단하기 위해 정확한 시간 정보가 확보되어야 한다.

[0004] 그러나, 현재 차량에는 현재 시간을 판별하기 위한 기준이 설정되기 어려운 실정이다. 차량과 휴대 단말기를 연동하여 현재 시간을 판별할 수 있으나, 음영지역인 경우 시간 정보를 정확하게 확보하기 어렵다.

[0005] 또한, 차량에 RTC(시간연산기)를 적용하여 현재 시간을 판별할 수 있으나, 추가적인 하드웨어 적용에 의한 재료비가 상승하는 문제가 있다.

[0006] 만일, 정확한 시간 정보가 없으면 자동과금을 위해 설치된 인증서의 유효기간이 만료되었는지, 현재 정식으로 배포된 인증서를 이용하고 있는지 확인하기 어려운 문제가 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 일 목적은 무결성이 확보된 시간 정보를 획득하여, 전력선 통신을 이용한 차량 충전 및 충전 과금 시에 사용되는 인증서의 유효성을 정확하게 판단할 수 있는 전기차 충전 제어 장치, 시스템 및 방법을 제공하는 데 있다.

[0008] 본 발명의 일 목적은 전기차 충전 시 해킹에 대한 보안을 강화할 수 있는 전기차 충전 제어 장치, 시스템 및 방법을 제공하는 데 있다.

[0009] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재들로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 본 발명의 일 실시예에 따른 전기차 충전 제어 시스템은 시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하고, 상기 서버로부터 수신되는 암호화된 시간 정보 응답 메시지를 복호화하여 현재 시간 정보를 추출하고, 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하고, 판단 결과에 기초하여 충전 동작을 제어하는 전기차 충전 제어 장치 및 상기 전기차 충전 제어 장치로부터 수신되는 상기 시간 정보 요청 메시지를 개인키를 이용하여 복호화하고, 상기 현재 시간 정보를 포함하는 시간 정보 응답 메시지를 상기 개인키로 암호화하여 상기 전기차 충전 제어 장치로 전달하는 서버를 포함한다.

- [0011] 그리고, 상기 인증서의 유효성이 판단되면 충전을 수행하는 충전 단말기를 더 포함한다.
- [0012] 그리고, 상기 전기차 충전 제어 장치는 상기 충전 단말기와 전력선 통신한다.
- [0013] 그리고, 상기 전기차 충전 제어 장치는 상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화한다.
- [0014] 그리고, 상기 전기차 충전 제어 장치는 상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화하지 못한 것으로 판단하면, EIM(External Identification Means)방식으로 충전하도록 제어한다.
- [0015] 그리고, 상기 전기차 충전 제어 장치는 상기 현재 시간 정보가 추출되면 프로토콜 암호화를 수행한다.
- [0016] 그리고, 상기 전기차 충전 제어 시스템은 상기 추출된 시간 정보를 기반으로 상기 인증서가 유효하지 않으면 충전을 종료하도록 제어한다.
- [0017] 그리고, 상기 전기차 충전 제어 시스템은 상기 추출된 시간 정보를 기반으로 상기 인증서가 유효한 것으로 판단하면, PnC(Plug and Charge) 방식으로 충전하도록 제어한다.
- [0018] 그리고, 본 발명의 일 실시예에 따른 전기차 충전 제어 장치는 시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하고, 상기 서버로부터 수신되는 암호화된 시간 정보 응답 메시지를 수신하는 통신부와, 상기 암호화된 시간 정보 응답 메시지를 상기 공개키로 복호화하여 현재 시간 정보를 추출하고, 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하고, 판단 결과에 기초하여 충전 동작을 제어하는 제어부를 포함한다.
- [0019] 본 발명의 일 실시예에 따른 전기차 충전 제어 방법은 시간 정보 요청 메시지를 공개키로 암호화하여 서버로 전달하는 단계와, 상기 서버로부터 암호화된 시간 정보 응답 메시지를 수신하는 단계와, 상기 수신된 시간 정보 응답 메시지를 복호화하여 현재 시간 정보를 추출하는 단계와, 상기 추출된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하는 단계 및 상기 판단 결과에 기초하여 충전 동작을 제어하는 단계를 포함한다.
- [0020] 그리고, 상기 서버로부터 암호화된 시간 정보 응답 메시지를 수신하는 단계는 상기 서버에서 상기 암호화된 시간 정보 요청 메시지를 수신하는 단계; 상기 서버에서 개인키로 상기 암호화된 메시지를 암호화 해제하는 단계; 상기 서버에서 시간 정보 응답 메시지를 생성하는 단계; 상기 서버에서 상기 시간 정보 응답 메시지를 상기 개인키를 이용하여 암호화하는 단계; 상기 서버에서 암호화된 상기 시간 정보 응답 메시지를 전기차 충전 제어장치로 전송하는 단계를 포함한다.
- [0021] 그리고, 상기 수신된 시간 정보 응답 메시지는 상기 공개키를 이용하여 복호화한다.
- [0022] 그리고, 상기 공개키를 이용하여 상기 시간 정보 응답 메시지를 복호화하지 못한 것으로 판단하면, EIM(External Identification Means)방식으로 충전하도록 제어한다.
- [0023] 그리고, 상기 현재 시간 정보가 추출되면 프로토콜 암호화를 수행하는 단계를 더 포함한다.
- [0024] 그리고, 상기 인증서가 유효성이 판단되지 않으면 충전을 종료하도록 제어한다.
- [0025] 그리고, 상기 인증서의 유효성이 판단되면, PnC(Plug and Charge)방식으로 충전하도록 제어한다.

발명의 효과

- [0026] 본 발명의 일 실시예에 따른 전기차 충전 제어 장치, 시스템 및 방법은 공개키 암호방식을 이용하여 무결성이 확보된 시간 정보를 획득함으로써, 전력선 통신을 이용한 차량 충전 및 충전 과금 시에 사용되는 인증서의 유효성을 정확하게 판단할 수 있고, 전기차 충전 시 해킹에 대한 보안을 강화할 수 있다.

도면의 간단한 설명

- [0027] 도 1은 본 발명의 일 실시예에 따른 전기차 충전 제어 시스템을 나타낸 블록도이다.
- 도 2는 본 발명의 일 실시예에 따른 전기차 충전 제어 장치를 나타낸 블록도이다.
- 도 3은 본 발명의 일 실시예에 따른 전기차 충전 제어 방법을 나타낸 순서도이다.
- 도 4는 본 발명의 일 실시예에 따른 방법을 실행하는 컴퓨팅 시스템의 구성을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0028] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호

를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명의 실시예를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 실시예에 대한 이해를 방해한다고 판단되는 경우에는 그 상세한 설명은 생략한다.

- [0029] 본 발명의 실시예의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 또한, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0030] 도 1은 본 발명의 일 실시예에 따른 전기차 충전 제어 시스템을 나타낸 블록도이다.
- [0031] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 전기차 충전 제어 시스템은 충전 단말기(100), 전기차(200)에 구비된 전기차 충전 제어 장치(20) 및 차량 OEM 서버(300)를 포함할 수 있다.
- [0032] 충전 단말기(100)는 전기차(200)와 전력선 통신할 수 있으며, 충전 단말기(100)는 서버(300)와 전력선 통신할 수 있다.
- [0033] 충전 단말기(100)는 전기차(200)에 전원을 공급할 수 있다.
- [0034] 충전 단말기(100)는 전기차 충전 제어 장치(20)에 설치된 인증서(차량과 전력사업자 간에 이루어진 충전 계약 인증서)를 기반으로 전기차(200)에 공급된 충전량을 정산하여 전기차(200)에 자동과금을 수행할 수 있다.
- [0035] 충전 단말기(100)는 전기차 충전 제어 장치(20)가 인증서의 유효기간을 정확하게 판단하지 못하여, 인증서의 유효기간이 만료되지 않았는데 만료된 것으로 판단하거나, 만료된 유효기간이 아직 만료되지 않은 것으로 판단한 경우, 전기차(200)에 충전을 수행하지 않는다.
- [0036] 즉, 충전 단말기(100)는 전기차 충전 제어 장치(20)가 인증서의 유효기간을 정확하게 판단한 경우, 이를 기반으로 전기차(200)에 충전을 수행할 수 있다.
- [0037] 전기차 충전 제어 장치(20)는 차량 OEM(Original Equipment Manufacturer) 서버(30)로부터 차량 생산 단계에서 인증서 및 공개키를 수신할 수 있으며, 이 인증서는 최초 충전 시 자동과금을 위한 계약체결 시 차량의 무결성을 증명하기 위해 사용된다.
- [0038] 또한, 전기차 충전 제어 장치(20)는 공개키 암호화 방식을 이용하여 차량 OEM 서버(30)로부터 무결성이 확인된 현재 시간 정보를 수신할 수 있다.
- [0039] 전기차 충전 제어 장치(20)는 무결성이 확인된 현재 시간 정보를 차량 OEM 서버(30)로부터 수신하면, 무결성이 확인된 현재 시간 정보를 기반으로 인증서의 유효성을 판단하고, 인증서가 유효한 것으로 판단하면 유효성 확인 결과를 충전 단말기(100) 및 충전 사업자에게 전달하여 충전을 시작하도록 제어할 수 있다.
- [0040] 차량 OEM 서버(30)는 차량 생산 단계에서 전기차 충전 제어 장치(20)에 인증서 및 공개키를 전송할 수 있다.
- [0041] 차량 OEM 서버(30)는 공개키 암호화 방식을 이용하여 무결성이 확인된 현재 시간 정보를 전송할 수 있다.
- [0042] 보다 구체적으로, 차량 OEM 서버(30)는 전기차 충전 제어 장치(20)로부터 암호화된 시간 정보 요청 메시지를 수신하면, 개인키를 이용하여 수신된 시간 정보 요청 메시지의 암호를 해제할 수 있다. 여기서, 시간 정보 요청 메시지는 시간 정보를 요청하는 내용을 포함할 수 있다.
- [0043] 차량 OEM 서버(30)는 개인키를 이용하여 전기차 충전 제어 장치(20)로부터 수신된 시간 정보 요청 메시지의 암호를 해제하면, 전기차 충전 제어 장치(20)로부터 수신한 메시지의 무결성을 확인할 수 있다.
- [0044] 차량 OEM 서버(30)는 개인키를 이용하여 전기차 충전 제어 장치(20)로부터 수신된 메시지의 암호를 해제하지 못하면, 전기차 충전 제어 장치(20)로부터 수신된 메시지는 위조된 정보를 판단할 수 있다.
- [0045] 차량 OEM 서버(30)는 전기차 충전 제어 장치(20)로부터 수신한 메시지의 무결성을 확인하면, 현재 시간에 대한 정보를 개인키를 이용하여 암호화하고, 이를 전기차 충전 제어 장치(20)로 전송할 수 있다.

- [0046] 도 2는 본 발명의 일 실시예에 따른 전기차 충전 제어 장치를 나타낸 블록도이다.
- [0047] 도 2에 도시된 바와 같이, 본 발명의 일 실시예에 따른 전기차는 통신부(21) 및 제어부(22)를 포함할 수 있다.
- [0048] 통신부(21)는 충전 단말기(100) 및 차량 OEM 서버(30)와 통신할 수 있다.
- [0049] 통신부(21)는 충전 단말기(100)와 전력선 통신할 수 있고, 충전 단말기(100)를 이용하여 차량 OEM 서버(30)와 통신할 수 있다. 여기서, 전력선 통신(PLC:Power Line Communication)은 전력을 공급하는 전력선을 이용하여 음성과 데이터를 송수신하는 통신을 의미한다.
- [0050] 통신부(21)는 차량 OEM 서버(30)와 무선통신할 수도 있다. 통신부(21)는 차량 OEM 서버(30)와 무선통신할 수 있으며, 실시예에 따르면 와이브로(Wireless broadband), Wimax(World Interoperability for Microwave Access), 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra Wideband), 지그비(ZigBee)를 통해 무선통신할 수 있다.
- [0051] 통신부(21)는 차량 생산 시 차량 OEM 서버(30)로부터 공개키와 인증서를 수신할 수 있다.
- [0052] 통신부(21)는 충전 단말기(100)와 전력선 통신을 위한 세션 연결 시 통신은 IP 기반으로 수행할 수 있다.
- [0053] 통신부(21)는 충전 단말기(100)로부터 충전을 수행하기 이전, 전기차의 인증서 유효기간을 확인하기 위해 암호화된 시간 정보 요청 메시지를 차량 OEM 서버(30)로 전송할 수 있다.
- [0054] 통신부(21)는 차량 OEM 서버(30)로부터 암호화된 시간 정보 응답 메시지를 수신할 수 있다. 여기서, 암호화된 시간 정보 응답 메시지에는 현재 시간 정보가 포함되어 있다.
- [0055] 통신부(21)는 충전이 수행되면, 충전량 정보를 충전 단말기(100)에 전송하고, 충전 단말기(100)로부터 충전과금 정보를 수신할 수 있다.
- [0056] 제어부(22)는 본 발명의 일 실시예에 따른 전기차의 전반적인 동작을 제어할 수 있다.
- [0057] 제어부(22)는 공개키 암호화 방식을 기반으로 무결성이 입증된 현재 시간 정보를 확인하면, 이를 기반으로 인증서의 유효기간을 판단할 수 있다.
- [0058] 보다 구체적으로, 제어부(22)는 차량 OEM 서버(30)로부터 수신한 공개키를 이용하여 차량 OEM 서버(30)에 시간 정보를 요청하는 시간 정보 요청 메시지를 암호화할 수 있다.
- [0059] 제어부(22)는 메시지 암호화 시에 차량 OEM 서버(30)로부터 수신한 공개키를 이용하기 때문에 전기차 충전 제어 장치로부터 발신된 메시지의 무결성을 입증할 수 있다.
- [0060] 제어부(22)는 공개키를 이용하여 암호화된 시간 정보 요청 메시지를 차량 OEM 서버(30)로 전송하도록 제어할 수 있다. 이후 차량 OEM 서버(30)로 전송된 메시지의 복호화 및 암호화는 다음의 방식으로 수행될 수 있다.
- [0061] 차량 OEM 서버(30)는 도 1을 참조하여 설명한 바와 같이, 차량 OEM 서버의 개인키를 이용하여 전기차 충전 제어 장치(20)로부터 수신된 암호화된 시간 정보 요청 메시지를 복호화할 수 있다. 차량 OEM 서버(30)는 암호화된 시간 정보 요청 메시지가 복호화되면 전기차 충전 제어 장치(20)로부터 수신된 메시지의 내용이 시간 정보를 요청하는 내용임을 확인할 수 있다.
- [0062] 차량 OEM 서버(30)는 전기차 충전 제어 장치(20)로부터 요청받은 시간 정보를 포함하는 시간 정보 응답 메시지를 생성하고, 이를 개인키를 이용하여 암호화한다. 개인키를 이용하여 암호화함으로써 차량 OEM 서버(30)는 시간 정보 응답 메시지의 무결성을 입증할 수 있고, 차량 OEM 서버(30)에서 암호화된 사실을 추후에 부인할 수 없게 할 수 있다.
- [0063] 차량 OEM 서버(30)는 개인키를 이용하여 암호화된 시간 정보 응답 메시지를 전기차 충전 제어 장치(20)에 전송하면, 제어부(22)는 차량 OEM 서버(30)로부터 암호화된 시간 정보 응답 메시지를 수신하도록 제어한다.
- [0064] 제어부(22)는 차량 OEM 서버(30)로부터 암호화된 시간 정보 응답 메시지를 공개키를 이용하여 복호화(암호화 해제)할 수 있다.
- [0065] 제어부(22)는 차량 OEM 서버(30)로부터 암호화된 시간 정보 응답 메시지를 공개키를 이용하여 암호화를 해제하기 때문에 암호화된 시간 정보 응답 메시지가 위조되지 않고 믿을 수 있는 서버로부터 발신된 것임(무결성)을 확인할 수 있으며, 암호화된 시간 정보 응답 메시지 내에 포함된 정확한 현재 시간 정보를 추출할 수 있다.

- [0066] 그러나, 제어부(22)는 암호화된 메시지를 공개키를 이용하여 암호화를 해제할 수 없는 경우 무결성이 입증되지 않은 서버로부터 수신한 메시지로 판단할 수 있으며 이러한 경우 EIM(External Identification Means) 방식으로 충전이 진행되도록 할 수 있다.
- [0067] EIM 방식은 충전 단말기(100)에 구비된 사용자 인터페이스를 이용하여 충전하는 방식으로, 예를들면 터치스크린과 같은 인터페이스를 사용자가 직접 조작하여 충전하고, 충전량이 정산된 금액을 직접 결제하는 방식을 의미한다.
- [0068] 제어부(22)는 무결성이 확인된 현재 시간 정보를 추출하면, 프로토콜 암호화를 수행한다. 제어부(22)는 통신부(21)와 차량 OEM 서버(30) 통신과정에서 도청, 간섭, 위조를 방지하기 위해 프로토콜 암호화를 수행할 수 있다. 프로토콜 암호화는 TLS(Transport Layer Security)로 수행될 수 있다.
- [0069] 제어부(22)는 인증서의 유효기간 정보를 추출할 수 있다.
- [0070] 제어부(22)는 무결성이 입증된 현재 시간 정보를 기반으로 인증서가 유효한지 판단할 수 있다.
- [0071] 제어부(22)는 인증서가 만료되어 유효하지 않은 것으로 판단하면, 충전을 종료하도록 제어할 수 있다.
- [0072] 제어부(22)는 인증서가 유효한 것으로 판단되면 PnC(Plug and Charge) 방식으로 충전이 이루어지도록 제어할 수 있다.
- [0073] PnC 방식은 충전 단말기(100)에서 별도의 사용자 인터페이스 장치가 구비되지 않고, 충전 단말기(100)와 전기차 충전 제어 장치(20) 사이에 통신에 의해 자동으로 충전되고 충전량에 따라 자동과금되는 방식을 의미할 수 있다.
- [0074] 상술한 바와 같이, 본 발명의 일 실시예에 따른 전기차는 차량 OEM 서버(30)로부터 수신한 공개키를 이용하여 무결성이 입증된 메시지를 송수신하는 방식으로 현재 시간 정보를 추출함으로써, GPS 음영지역 등 정확한 시간 정보 획득이 어려운 환경에서도 무결성이 확보된 시간 정보를 획득할 수 있다.
- [0075] 또한, 전기차와 차량 OEM 서버는 공개키 암호화 방식을 이용하여 메시지를 송수신함으로써, 메시지의 무결성 뿐만 아니라 전기차와 서버의 무결성도 입증함으로써 해킹되어 시간이 위변조되는 것을 방지할 수 있다.
- [0076] 도 3은 본 발명의 일 실시예에 따른 전기차 충전 제어 방법을 나타낸 순서도이다.
- [0077] 도 3에 도시된 바와 같이, 충전 단말기(100)와 전기차 충전 제어 장치(20)는 연결된다(S31). S31에서 충전 단말기(100) 및 전기차 충전 제어 장치(20)는 전력선 통신을 수행할 수 있다.
- [0078] 전기차 충전 제어 장치(20)는 공개키를 이용하여 시간 정보 요청 메시지를 암호화한다(S32). S32에서 전기차 충전 제어 장치(20)는 메시지 암호화 시에 차량 OEM 서버(30)로부터 수신한 공개키를 이용하기 때문에 전기차 충전 제어 장치(20)로부터 발신된 메시지의 무결성을 입증할 수 있다.
- [0079] 전기차 충전 제어 장치(20)는 암호화된 메시지를 제어부(22)는 공개키를 이용하여 암호화된 시간 정보 요청 메시지를 차량 OEM 서버(30)로 전송한다(S33).
- [0080] 차량 OEM 서버(30)는 전기차 충전 제어 장치(20)로부터 암호화된 시간 정보 요청 메시지를 수신하면, 차량 OEM 서버의 개인키를 이용하여 복호화(암호화 해제)되었는지 판단한다(S34).
- [0081] 차량 OEM 서버(30)는 개인키를 이용하여 전기차 충전 제어 장치(20)로부터 수신된 시간 정보 요청 메시지가 복호화되면(Y), 전기차 충전 제어 장치(20)로부터 수신된 메시지의 내용이 시간 정보를 요청하는 내용임을 확인하고, 현재 시간 정보를 포함한 시간 정보 응답 메시지를 생성하고, 시간 정보 응답 메시지를 개인키를 이용하여 암호화한다(S35). S35에서 차량 OEM 서버(30)는 개인키를 이용하여 암호화함으로써, 시간 정보 응답 메시지의 무결성을 입증할 수 있고, 암호화한 사실을 추후에 부인할 수 없게 된다.
- [0082] 차량 OEM 서버(30)는 개인키를 이용하여 전기차 충전 제어 장치(20)로부터 수신된 메시지가 복호화되지 않은 것으로 판단하면(N), 전기차 충전 제어 장치(20)의 통신을 종료한다(S36).
- [0083] 차량 OEM 서버(30)는 개인키를 이용하여 암호화된 메시지를 전기차 충전 제어 장치(20)로 전송한다(S37).
- [0084] 전기차 충전 제어 장치(20)는 암호화된 시간 정보 응답 메시지를 차량 OEM 서버(30)로부터 수신하면 공개키를 이용하여 복호화할 수 있는지 판단한다(S38).
- [0085] S38에서 전기차 충전 제어 장치(20)는 공개키를 이용하여 시간 정보 응답 메시지를 암호화 해제할 수 있는 것

로 판단하면(Y), 전기차 충전 제어 장치(20)는 시간 정보 응답 메시지가 위조되지 않고 믿을 수 있는 서버로부터 발신된 것임(무결성)을 확인할 수 있다. 이후, 전기차 충전 제어 장치(20)는 복호화된 시간 정보 응답 메시지 내에 포함된 정확한 현재 시간 정보를 추출한다(S39).

- [0086] S38에서 전기차 충전 제어 장치(20)는 공개키를 이용하여 암호화 해제할 수 없는 것으로 판단하면(N), 무결성이 입증되지 않은 서버로부터 수신된 메시지로 판단하고, EIM(External Identification Means) 방식으로 충전이 진행되도록 한다(S40).
- [0087] S39에서 전기차 충전 제어 장치(20)는 현재 시간 정보를 추출하면, 프로토콜 암호화를 수행한다(S41). S41에서 프로토콜 암호화는 전기차 충전 제어 장치(20)와 차량 OEM 서버(30) 통신과정에서 도청, 간섭, 위조를 방지하기 위해 수행될 수 있으며, 실시예에 따르면 프로토콜 암호화는 TLS(Transport Layer Security)로 수행될 수 있다.
- [0088] 전기차 충전 제어 장치(20)는 인증서의 유효기간 정보를 추출한다(S42).
- [0089] 전기차 충전 제어 장치(20)는 무결성이 입증된 현재 시간 정보와 인증서의 유효기간을 비교하여 인증서 유효성을 판단한다(S43).
- [0090] 제어부(22)는 인증서가 유효성이 판단되면 PnC(Plug and Charge) 방식으로 충전이 이루어지도록 제어한다(S44).
- [0091] PnC 방식은 충전 단말기(100)에서 별도의 사용자 인터페이스 장치가 구비되지 않고, 충전 단말기(100)와 전기차 충전 제어 장치(20) 사이에 통신에 의해 자동으로 충전되고 충전량에 따라 자동과금되는 방식을 의미할 수 있다.
- [0092] 제어부(22)는 인증서가 만료되어 유효하지 않은 것으로 판단하면, 충전을 종료하도록 제어한다(S45).
- [0093] 도 4는 본 발명의 일 실시예에 따른 방법을 실행하는 컴퓨팅 시스템의 구성을 도시한 도면이다.
- [0094] 도 4를 참조하면, 컴퓨팅 시스템(1000)은 버스(1200)를 통해 연결되는 적어도 하나의 프로세서(1100), 메모리(1300), 사용자 인터페이스 입력 장치(1400), 사용자 인터페이스 출력 장치(1500), 스토리지(1600), 및 네트워크 인터페이스(1700)를 포함할 수 있다.
- [0095] 프로세서(1100)는 중앙 처리 장치(CPU) 또는 메모리(1300) 및/또는 스토리지(1600)에 저장된 명령어들에 대한 처리를 실행하는 반도체 장치일 수 있다. 메모리(1300) 및 스토리지(1600)는 다양한 종류의 휘발성 또는 비휘발성 저장 매체를 포함할 수 있다. 예를 들어, 메모리(1300)는 ROM(Read Only Memory) 및 RAM(Random Access Memory)을 포함할 수 있다.
- [0096] 따라서, 본 명세서에 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계는 프로세서(1100)에 의해 실행되는 하드웨어, 소프트웨어 모듈, 또는 그 2 개의 결합으로 직접 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 착탈형 디스크, CD-ROM과 같은 저장 매체(즉, 메모리(1300) 및/또는 스토리지(1600))에 상주할 수도 있다. 예시적인 저장 매체는 프로세서(1100)에 커플링되며, 그 프로세서(1100)는 저장 매체로부터 정보를 판독할 수 있고 저장 매체에 정보를 기입할 수 있다. 다른 방법으로, 저장 매체는 프로세서(1100)와 일체형일 수도 있다. 프로세서 및 저장 매체는 주문형 집적회로(ASIC) 내에 상주할 수도 있다. ASIC는 사용자 단말기 내에 상주할 수도 있다. 다른 방법으로, 프로세서 및 저장 매체는 사용자 단말기 내에 개별 컴포넌트로서 상주할 수도 있다.
- [0097] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다.
- [0098] 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

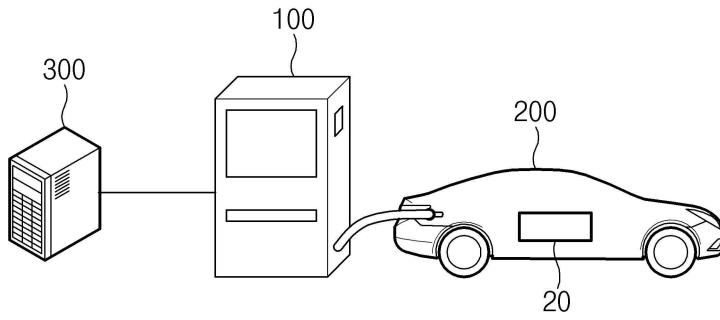
부호의 설명

[0099]	충전 단말기	100
	전기차	200

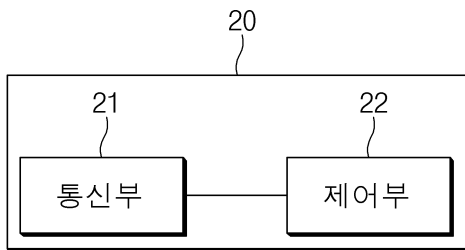
전기차 충전 제어 장치	20
통신부	21
제어부	22
차량 OEM 서버	300

도면

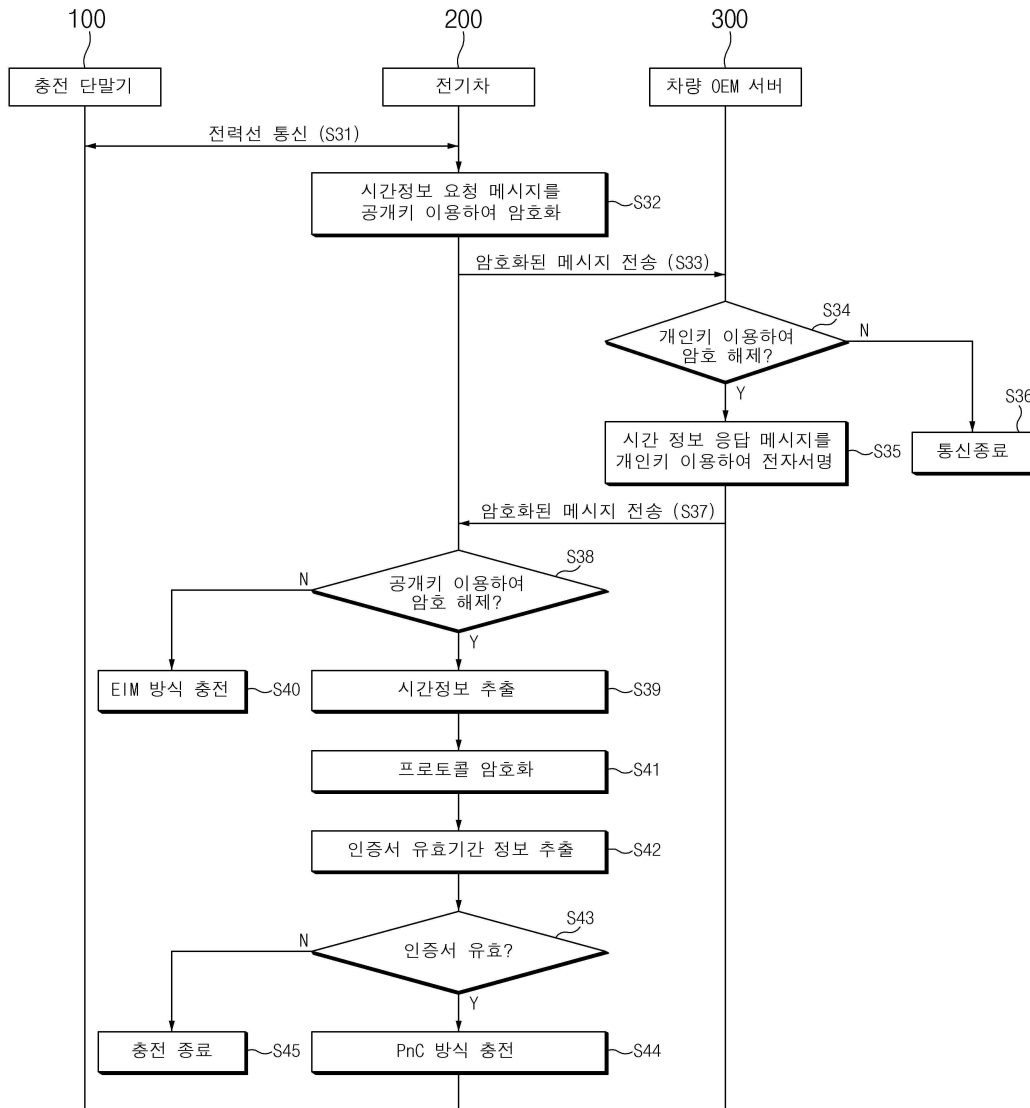
도면1



도면2



도면3



도면4

