



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2022-0133149  
(43) 공개일자 2022년10월04일

(51) 국제특허분류(Int. Cl.) H04L 9/40 (2022.01) B60L 53/30 (2019.01) H04L 47/6275 (2022.01) H04L 69/08 (2022.01) (52) CPC특허분류 H04L 63/166 (2013.01) B60L 53/305 (2019.02) (21) 출원번호 10-2022-0117131(분할) (22) 출원일자 2022년09월16일 심사청구일자 2022년09월16일 (62) 원출원 특허 10-2018-0073315 원출원일자 2018년06월26일 심사청구일자 2021년04월20일	(71) 출원인 한국전력공사 전라남도 나주시 전력로 55(빛가람동) (72) 발명자 임유석 대전광역시 유성구 문지로 105 박기준 대전광역시 유성구 송림로 20 206-2301 (뒷면에 계속) (74) 대리인 특허법인아주
--	---

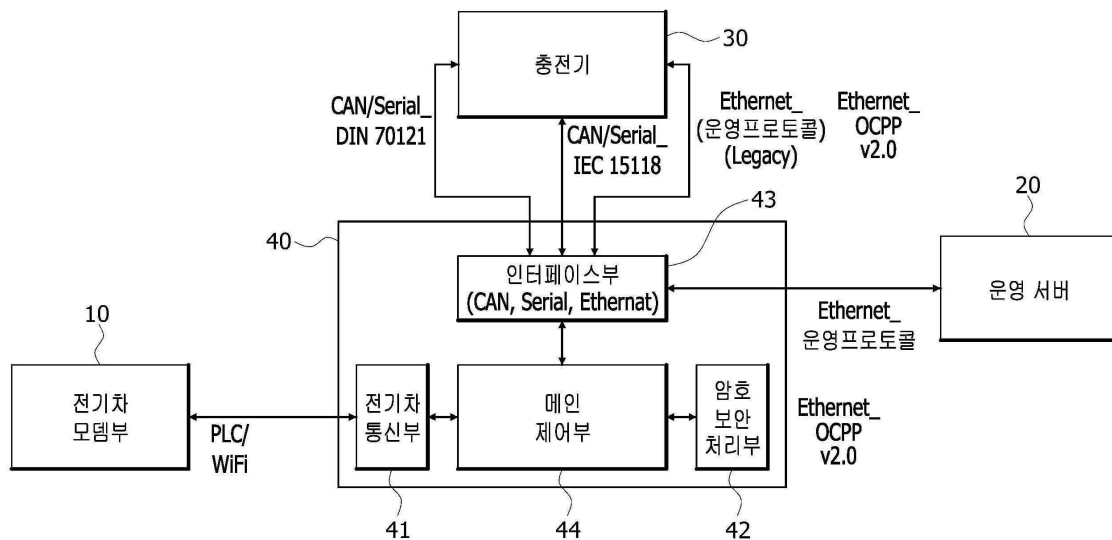
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **전기차 충전기용 양방향 보안통신장치**

**(57) 요약**

전기차 충전기용 양방향 보안통신장치가 개시된다. 본 발명의 전기차 충전기용 양방향 보안통신장치는 전기차 충전을 위해 전기차와 통신을 수행하는 전기차 통신부; 충전기와 운영서버 및 충전기와 전기차 간의 통신 인터페이스를 제공하는 인터페이스부; 운영서버 및 전기차와의 통신을 위해 송수신되는 데이터를 암호보안처리하는 암호보안 처리부; 및 전기차 및 운영서버와의 통신을 위한 프로토콜을 처리하여 인터페이스부를 통해 데이터를 송수신하고, 운영서버 및 전기차로 송수신되는 데이터에 대해 암호보안 처리부를 통해 암호보안처리를 수행하는 메인 제어부를 포함하는 것을 특징으로 한다.

**대표도**



(52) CPC특허분류

*H04L 47/6275* (2022.05)

*H04L 63/0428* (2013.01)

*H04L 63/18* (2013.01)

*H04L 69/08* (2022.05)

(72) 발명자

**오도은**

세종특별시 갈매로 480 207-1102

**임성우**

대전광역시 유성구 문지로 105

**한승호**

대전광역시 유성구 문지로 105

## 명세서

### 청구범위

#### 청구항 1

전기차 충전을 위해 전기차와 통신을 수행하는 전기차 통신부;

충전기와 운영서버 및 충전기와 전기차 간의 통신 인터페이스를 제공하는 인터페이스부;

상기 운영서버 및 상기 전기차와의 통신을 위해 송수신되는 데이터를 암호화처리하는 암호화 처리부; 및

상기 전기차 및 상기 운영서버와의 통신을 위한 프로토콜을 처리하여 상기 인터페이스부를 통해 데이터를 송수신하고, 상기 운영서버 및 상기 전기차로 송수신되는 데이터에 대해 상기 암호화 처리부를 통해 암호화처리를 수행하는 메인 제어부를 포함하고,

상기 메인 제어부는 상기 인터페이스부를 통한 상기 충전기와 상기 전기차 간의 통신, 및 상기 충전기와 상기 운영서버 간의 통신 매체에 따른 프로토콜을 처리하는 통신매체 프로토콜 처리부; 상기 전기차와의 통신 매체에 따라 전기차 충전 프로토콜의 종류를 판단하는 전기차 충전 프로토콜 판단부; 상기 전기차 충전 프로토콜 판단부의 판단 결과에 따라 전기차 충전 프로토콜을 처리하는 전기차 충전 프로토콜 처리부; 상기 전기차 및 상기 운영서버와의 통신에 따라 데이터를 암호화하기 위한 메시지 큐 관리를 수행하는 메시지 큐 관리부; 상기 충전기의 고유인증서 및 개인키를 관리하고 전자서명 처리를 수행하는 보안기능 처리부; 상기 운영서버와의 통신을 위한 운영서버 프로토콜을 판단하는 운영서버 프로토콜 판단부; 상기 운영서버 프로토콜 판단부의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 보안처리 프로토콜 메시지를 처리하는 제1 운영서버 프로토콜 처리부; 및 상기 운영서버 프로토콜 판단부의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 일반처리 프로토콜 메시지를 처리하는 제2 운영서버 프로토콜 처리부를 포함하고,

상기 메시지 큐 관리부는 상기 충전기와 상기 전기차 간의 통신, 및 상기 충전기와 상기 운영서버 간의 통신 중 기 설정된 우선순위에 따라 메시지 큐를 관리하고,

상기 운영서버 프로토콜 판단부는 운영서버와 충전기 간에 송수신되는 메시지가 TLS 메시지이면 상기 TLS 메시지를 복호화시킨 후, 운영서버 프로토콜이 OCPP 프로토콜인지 여부를 판단하고, 판단 결과 OCPP 프로토콜이면 상기 암호화 처리부를 통해 보안에 해당되는 보안처리 프로토콜 메시지를 처리하고, OCPP 프로토콜이 아니면 보안버전이 있는지 여부에 따라 상기 암호화 처리부를 통해 보안처리를 수행하거나 또는 메시지를 상기 충전기에 전송하는 것을 특징으로 하는 전기차 충전기용 양방향 보안통신장치.

### 발명의 설명

#### 기술분야

[0001] 본 발명은 전기차 충전기용 양방향 보안통신장치에 관한 것으로서, 보다 상세하게는 충전기와 전기차 및 운영서버 간의 통신 보안 기능을 향상시킨 전기차 충전기용 양방향 보안통신장치에 관한 것이다.

#### 배경기술

[0003] 기존 충전시스템은 차량과 충전기 사이의 통신, 및 충전기와 운영서버 사이의 통신으로 구분되어 각각 다른 통신매체 및 통신프로토콜을 활용하여 정보를 교환하고 있다.

[0004] 특히, DC 충전방식은 3가지 충전커넥터 방식이 혼용되는데, CHAdeMO로 불리는 커넥터는 CAN (SGSF-064-1) 통신방식을 활용하고, Combo Type1의 커넥터는 PLC(DIN 70121) 통신방식을 활용하며, 나머지 Type2 커넥터 방식과 AC 충전방식은 차량과 통신을 하지 않는다.

[0005] 그러나, 충전 커넥터가 Combo Type 1(AC/DC 통합)으로 통일하게 됨에 따라, 향후 출시되는 전기차는 ISO/IEC 15118 표준이 전기차와 충전기간 통신으로 적용될 예정이다. 또한, 충전기와 운영서버 간의 프로토콜은 충전사업자 또는 운영자들마다 상이한데, 현재 충전기와 운영서버간 통신에 보안기술(메시지 암호화, 장치 인증 등)이

적용되어있지 않은 실정이다.

[0006] 이와 같이, 향후 개선되는 전기차의 기능이 확대되고 국제표준이 제정됨에 따라, AC/DC 충전시 통신기능이 더욱 확대되거나 운영서버와의 통신에 보안기능을 적용하는 상황에서, 기존에 운영중인 충전기를 업그레이드하는 것이 어려운 실정이다. 왜냐하면, 충전기 내부의 PLC 모듈 및 서버와의 통신을 담당하는 MCU는 자원을 최적화하여 제작하였기 때문이다. 그 결과, 새로운 형태의 프로토콜 구현, 암호모듈 연동 등 부가적인 기능이 수행되기 어려운 실정이다.

[0007] 게다가, 기존의 충전인프라 보급을 위해 상당수의 충전기가 이미 보급되었고 보급될 계획이 있어, 기존 구축된 충전인프라를 업데이트할 경우에는 비용을 최소화하면서 다양한 기능을 확장하여 구현할 수 있는 방법을 고려해야만 한다. 또한 향후에는 V2G 등 다양한 기능을 요구하는 서비스 정보교환이 요구되기 때문에 다양한 서비스 사업과의 연계를 위해서는 추가기능 업그레이드에 유연하게 대처할 수 있는 통신모듈 또는 충전시스템이 필요한 실정이다.

[0008] 본 발명의 배경기술은 대한민국 공개특허공보 10-2017-0045876호(2017.04.28)의 '전기차 전력 전송 시스템의 보안 방법 및 장치'에 개시되어 있다.

### 발명의 내용

#### 해결하려는 과제

[0010] 본 발명은 전술한 문제점을 개선하기 위해 창안된 것으로서, 본 발명의 일 측면에 따른 목적은 충전기와 전기차 및 운영서버 간의 통신 보안 기능을 향상시킨 전기차 충전기용 양방향 보안통신장치를 제공하는 것이다.

#### 과제의 해결 수단

[0012] 본 발명의 일 측면에 따른 전기차 충전기용 양방향 보안통신장치는 전기차 충전을 위해 전기차와 통신을 수행하는 전기차 통신부; 충전기와 운영서버 및 충전기와 전기차 간의 통신 인터페이스를 제공하는 인터페이스부; 상기 운영서버 및 상기 전기차와의 통신을 위해 송수신되는 데이터를 암호보안처리하는 암호보안 처리부; 및 상기 전기차 및 상기 운영서버와의 통신을 위한 프로토콜을 처리하여 상기 인터페이스부를 통해 데이터를 송수신하고, 상기 운영서버 및 상기 전기차로 송수신되는 데이터에 대해 상기 암호보안 처리부를 통해 암호보안 처리를 수행하는 메인 제어부를 포함하고, 상기 메인 제어부는 상기 인터페이스부를 통한 상기 충전기와 상기 전기차 간의 통신, 및 상기 충전기와 상기 운영서버 간의 통신 매체에 따른 프로토콜을 처리하는 통신매체 프로토콜 처리부; 상기 전기차와의 통신 매체에 따라 전기차 충전 프로토콜의 종류를 판단하는 전기차 충전 프로토콜 판단부; 상기 전기차 충전 프로토콜 판단부의 판단 결과에 따라 전기차 충전 프로토콜을 처리하는 전기차 충전 프로토콜 처리부; 상기 전기차 및 상기 운영서버와의 통신에 따라 데이터를 암호화하기 위한 메시지 큐 관리를 수행하는 메시지 큐 관리부; 상기 충전기의 고유 인증서 및 개인키를 관리하고 전자서명 처리를 수행하는 보안기능 처리부; 상기 운영서버와의 통신을 위한 운영서버 프로토콜을 판단하는 운영서버 프로토콜 판단부; 상기 운영서버 프로토콜 판단부의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 보안처리 프로토콜 메시지를 처리하는 제1 운영서버 프로토콜 처리부; 및 상기 운영서버 프로토콜 판단부의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 일반처리 프로토콜 메시지를 처리하는 제2 운영서버 프로토콜 처리부를 포함하고, 상기 메시지 큐 관리부는 상기 충전기와 상기 전기차 간의 통신, 및 상기 충전기와 상기 운영서버 간의 통신 중 기 설정된 우선순위에 따라 메시지 큐를 관리하고, 상기 운영서버 프로토콜 판단부는 운영서버와 충전기 간에 송수신되는 메시지가 TLS 메시지이면 상기 TLS 메시지를 복호화시킨 후, 운영서버 프로토콜이 OCPP 프로토콜인지 여부를 판단하고, 판단 결과 OCPP 프로토콜이면 상기 암호보안 처리부를 통해 보안에 해당하는 보안처리 프로토콜 메시지를 처리하고, OCPP 프로토콜이 아니면 보안버전이 있는지 여부에 따라 상기 암호보안 처리부를 통해 보안 처리를 수행하거나 또는 메시지를 상기 충전기에 전송하는 것을 특징으로 한다.

#### 발명의 효과

[0014] 본 발명의 일 측면에 따른 전기차 충전기용 양방향 보안통신장치는 향후 개정되는 전기차와 충전기 간의 프로토

콜, 전기차와 충전기 간의 통신 방식, 및 충전기와 운영서버 간의 프로토콜을 확장성 있게 수용할 수 있다.

[0015] 본 발명의 다른 측면에 따른 전기차 충전기용 양방향 보안통신장치는 기존 충전기 내부 통신링크 사이에 연결되어 전기차와 충전기, 및 충전기와 운영서버 간의 통신을 개선할 뿐만 아니라 보안기능(TLS)을 제공하여 보다 안전한 통신채널을 확보할 수 있도록 한다.

[0016] 본 발명의 또 다른 측면에 따른 전기차 충전기용 양방향 보안통신장치는 기존에 상당수 보급된 충전 인프라의 기능 업그레이드를 저비용으로 수행할 수 있어 보급사업에 효율적으로 이용될 수 있다.

### 도면의 간단한 설명

[0018] 도 1 은 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치의 통신 네트워크 연계 구성을 나타낸 도면이다.

도 2 는 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치의 블럭 구성도이다.

도 3 은 본 발명의 일 실시예에 따른 메인 제어부의 블럭 구성도이다.

도 4 는 본 발명의 일 실시예에 따른 전기차 충전 프로토콜을 판단하는 과정을 도시한 순서도이다.

도 5 는 본 발명의 일 실시예에 따른 메시지 큐 관리 과정을 도시한 순서도이다.

도 6 은 본 발명의 일 실시예에 따른 운영서버 프로토콜을 판단하는 과정을 도시한 순서도이다.

### 발명을 실시하기 위한 구체적인 내용

[0019] 이하에서는 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치를 첨부된 도면들을 참조하여 상세하게 설명한다. 이러한 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다. 또한 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 이용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0020] 도 1 은 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치의 통신 네트워크 연계 구성을 나타낸 도면이고, 도 2 는 본 발명의 일 실시예에 따른 보안통신모듈의 블럭 구성도이며, 도 3 은 본 발명의 일 실시예에 따른 메인 제어부의 블럭 구성도이며, 도 4 는 본 발명의 일 실시예에 따른 전기차 충전 프로토콜을 판단하는 과정을 도시한 순서도이며, 도 5 는 본 발명의 일 실시예에 따른 메시지 큐 관리 과정을 도시한 순서도이며, 도 6 은 본 발명의 일 실시예에 따른 운영서버 프로토콜을 판단하는 과정을 도시한 순서도이다.

[0021] 도 1 을 참조하면, 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치(40)는 전기차(10), 운영서버(20) 및 충전기(30) 사이에 설치되며, 전기차 충전을 위해 충전기(30)와 전기차 간의 통신 및 충전기(30)와 운영서버(20) 간의 통신을 수행한다.

[0022] 전기차 충전기용 양방향 보안통신장치는 충전기(30)와 전기차(10) 간에는 PLC(Power Line Communication) 또는 WiFi를 이용하여 통신을 수행하고, 충전기(30)와 운영서버(20) 간에는 이더넷(Ethernet)을 이용하여 통신을 수행하며, 이러한 통신을 위한 프로토콜을 처리한다.

[0023] 특히, 전기차 충전기용 양방향 보안통신장치는 충전기(30)와 전기차(10), 및 충전기(30)와 운영서버(20) 간에 송수신되는 데이터에 대해 AES(Advanced Encryption Standard) 또는 ARIA(Academy, Research Institute, Agency) 중 적어도 하나를 이용하여 암호화를 수행하거나, 충전기(30)의 고유 인증서 및 개인키를 관리하거나, 또는 전자 서명함으로써, 송수신되는 데이터에 대한 보안처리가 이루어지도록 한다.

[0024] 이러한 전기차 충전기용 양방향 보안통신장치는 충전시스템 내부에 설치될 수 있으나, 반드시 충전시스템 내부에 설치되어야 하는 것은 아니며 충전 시스템과 독립적으로 설치될 수도 있다.

[0025] 도 2 를 참조하면, 전기차 충전기용 양방향 보안통신장치는 전기차 통신부(41), 암호보안 처리부(42), 인터페이스부(43) 및 메인 제어부(44)를 포함한다.

[0026] 전기차 통신부(41)는 전기차 충전을 위해 전기차, 예를 들어 전기차(10)와 통신을 수행한다. 즉, 전기차 통신부(41)는 전기차(10)와의 통신을 수행하기 위해 전기차(10)와 연결된 통신 매체를 판단하고, 판단된 통신 매체에

따라 통신을 수행한다.

- [0027] 여기서, 전기차와의 통신 매체로는 PLC(Power Line Communication) 및 WiFi가 포함될 수 있다. 예를 들어, 전기차 통신부(41)는 WiFi 신호가 수신되면 통신 매체를 WiFi로 판단하고, PLC 신호가 수신되면 통신매체를 PLC로 판단한다.
- [0028] 이와 같이, 전기차 통신부(41)에 의해 통신매체가 판단되면, 메인 제어부(44)는 해당 통신매체 각각에 대응되는 프로토콜을 처리한다. 이에 대해서는 후술한다.
- [0029] 한편, 전기차 통신부(41)는 WiFi 신호와 PLC 신호가 모두 수신되지 않은 경우에는 컨트롤 파일럿(Control Pilot:CP) 제어신호를 이용하는 시그널 통신을 수행한다. 이에 대해서는 후술한다.
- [0030] 암호보안 처리부(42)는 운영서버(20) 및 전기차(10)와의 통신을 위해 송수신되는 데이터를 암호보안처리한다. 이 경우, 암호보안 처리부(42)는 전기차(10) 및 운영서버(20)와 송수신되는 데이터를 암호화시키거나, 고유 인증서와 개인키를 관리하거나 또는 전자서명한다.
- [0031] 특히, 암호보안 처리부(42)는 메인 제어부(44)의 메시지 큐에 따라 충전기(30)와 전기차(10) 간의 통신, 및 충전기(30)와 운영서버(20) 간의 통신 각각에 대응되는 암호화 방식으로 데이터를 암호화한다. 이는 충전기(30)와 전기차(10) 간의 통신, 및 충전기(30)와 운영서버(20) 간의 암호화 알고리즘이 서로 다르게 규정되어 있기 때문이다. 예를 들어, 전기차와 충전기(30) 간의 국제표준 IEC15118에서는 암호화수를 AES 방식을 규정하고 있으나, 충전기(30)와 운영서버(20) 간에는 KCMVP 기반의 ARIA 알고리즘이 규정되어 있다.
- [0032] 이에, 암호보안 처리부(42)는 메인 제어부(44)의 메시지 큐에 따라, 충전기(30)와 전기차(10) 간의 통신에서는 AES 알고리즘을 이용하여 암호화하고, 충전기(30)와 운영서버(20) 간의 통신에서는 ARIA 알고리즘을 이용하여 암호화한다.
- [0033] 인터페이스부(43)는 충전기(30)와 운영서버(20) 및 충전기(30)와 전기차 간의 통신 인터페이스를 제공한다. 인터페이스부(43)는 캔(CAN) 통신, 시리얼(Serial) 통신 및 이더넷(Ethernet) 통신 중 적어도 하나의 통신매체를 이용하여 통신 인터페이스를 제공한다.
- [0034] 이 경우, 인터페이스부(43)는 충전기(30)와 전기차(10) 간에는 캔(CAN) 통신 및 시리얼(Serial) 통신 중 적어도 하나를 통해 통신을 수행하고, 충전기(30)와 운영서버(20) 간에는 이더넷(Ethernet) 통신을 통해 통신을 수행한다.
- [0035] 메인 제어부(44)는 전기차 및 운영서버(20)와의 통신을 위한 프로토콜을 처리하고, 운영서버(20) 및 전기차(10)로 송수신되는 데이터에 대해 암호 보안 처리한다.
- [0036] 도 3 을 참조하면, 메인 제어부(44)는 통신매체 프로토콜 처리부(441), 전기차 충전 프로토콜 판단부(442), 전기차 충전 프로토콜 처리부(443), 메시지 큐 관리부(444), 보안기능 처리부(445), 운영서버 프로토콜 판단부(446), 제1 운영서버 프로토콜 처리부(447), 제2 운영서버 프로토콜 처리부(448), 고객 인증서 CRL 관리부, 및 부가서비스 연계부(4411)를 포함한다.
- [0037] 통신매체 프로토콜 처리부(441)는 인터페이스부(43)를 통한 충전기(30)와 전기차(10) 간의 통신, 및 충전기(30)와 운영서버(20) 간의 통신 매체에 따른 프로토콜을 처리한다. 이와 같은 각 통신매체에 따른 프로토콜 처리에 따라, 인터페이스부(43)는 캔 통신, 시리얼 통신 및 이더넷 통신 중 적어도 하나의 통신매체를 이용하여 통신을 수행한다.
- [0038] 전기차 충전 프로토콜 판단부(442)는 전기차(10)와의 통신을 위한 전기차 충전 프로토콜의 종류를 판단한다. 이 경우, 전기차 충전 프로토콜 판단부(442)는 전기차와 WiFi 통신을 수행하면 해당 전기차 충전 프로토콜을 WiFi 통신에 대응되는 프로토콜로 판단하고, 전기차와 PLC 통신을 수행하면 해당 전기차 충전 프로토콜을 PLC 통신에 대응되는 프로토콜로 판단한다.
- [0039] 여기서, WiFi 통신에 대응되는 전기차 충전 프로토콜은 IEC 15118 프로토콜이 포함될 수 있으며, PLC 통신에 대응되는 프로토콜은 DIN 프로토콜(DIN 70121 프로토콜)이 포함될 수 있다. 그러나, 본 발명의 기술적 범위는 상기한 실시예에 한정되는 것은 아니며, 전기차 충전 프로토콜은 이후 추가 또는 변경될 수 있는 통신매체에 따라 다양한 전기차 충전 프로토콜이 모두 적용될 수 있다.
- [0040] 전기차 충전 프로토콜 처리부(443)는 전기차 충전 프로토콜 판단부(442)의 판단 결과에 따라 해당 전기차 충전 프로토콜을 처리한다. 즉, 전기차 충전 프로토콜 판단부(442)에 의해 전기차 충전 프로토콜이 DIN 프로토콜로

판단되면 전기차 충전 프로토콜 처리부(443)는 DIN 프로토콜을 처리하고, 전기차 충전 프로토콜 판단부(442)에 의해 전기차 충전 프로토콜이 IEC 15118 프로토콜로 판단되면 전기차 충전 프로토콜 처리부(443)는 IEC 15118 프로토콜을 처리한다. 이러한 전기차 충전 프로토콜의 판단 및 처리 과정을 도 4 를 참조하여 좀 더 상세하게 설명한다.

- [0041] 도 4 를 참조하면, 먼저 전기차 통신부(41)는 전기차 충전을 위해 전기차(10)와의 통신을 수행하기 위해 전기차(10)와 연결된 통신 매체를 판단하는데, 이 경우 우선적으로 WiFi 신호가 수신되는지를 판단한다(S102).
- [0042] 단계(S102)에서의 판단 결과 WiFi 신호가 수신되면, 전기차 충전 프로토콜 판단부(442)가 해당 데이터에 대한 보안처리가 필요한지를 판단한다(S104).
- [0043] 단계(S104)에서의 판단 결과 보안처리가 필요하면, 메시지 큐 관리부(444)가 AES 알고리즘을 이용하여 암호화하기 위한 메시지 큐를 생성하고, 이러한 메시지 큐에 따라 암호보안 처리부(42)가 AES 알고리즘을 이용하여 암호화를 수행한다. 아울러, 전기차 충전 프로토콜 처리부(443)가 해당 통신매체에 따른 전기차 충전 프로토콜, 즉 IEC 15118 프로토콜을 처리한다(S108).
- [0044] 반면에, 단계(S104)에서의 판단 결과 보안처리가 필요하지 않으면, 전기차 충전 프로토콜 처리부(443)가 해당 통신매체에 따른 전기차 충전 프로토콜, 즉 IEC 15118 프로토콜을 처리한다(S106).
- [0045] 한편, 단계(S102)의 판단 결과 WiFi 신호가 수신되지 않으면, 전기차 통신부(41)는 전기차에 전기적으로 접속되어 PLC 신호가 수신되는 지를 판단한다(S110,S112).
- [0046] 단계(S112)의 판단 결과 PLC 신호가 수신되면, 전기차 충전 프로토콜 처리부(443)가 해당 통신매체에 따른 전기차 충전 프로토콜, 즉 DIN 프로토콜인지를 판단(S114)하고, 판단 결과 DIN 프로토콜이면 해당 DIN 프로토콜을 처리한다(S116). 반면에, 단계(S114)의 판단 결과 DIN 프로토콜이 아니면 단계(104)로 진입한다.
- [0047] 이와 같이 전기차 충전 프로토콜이 처리되면, 통신매체 프로토콜 처리부(441)가 전기차와의 통신에 따른 CAN 통신 또는 시리얼 통신 프로토콜로 변환하고(S118), 이에 따라 인터페이스부(43)를 통해 전기차와 충전기(30) 간에 데이터 송수신이 이루어지며, 이러한 데이터 송수신에 따른 충전이 진행되도록 한다(S120,S128).
- [0048] 한편, 단계(S112)의 판단 결과 PLC 신호가 수신되지 않으면, 전기차 충전 프로토콜 판단부(442)는 IEC 61851-1 표준에 따른 신호처리를 수행한다(S122). 즉, 전기차 충전 프로토콜 판단부(442)는 컨트롤 파일럿(Control Pilot:CP) 제어신호에 따른 통신없이 충전을 수행하는데, 이때 DC 충전요청이 입력되는지를 확인(S124)하고, DC 충전 요청이 입력되면 충전불가 메시지를 생성하여 전기차로 전달한다(S126).
- [0049] 반면에, DC 충전요청이 입력되지 않으면, 인터페이스부(43)가 컨트롤 파일럿(Control Pilot:CP) 제어신호를 충전기(30)에 송신하여 충전이 진행되도록 한다(S120,S128).
- [0050] 보안기능 처리부(445)는 충전기의 고유 인증서 및 개인키를 관리하고 전자서명 처리를 수행한다.
- [0051] 메시지 큐 관리부(444)는 전기차 및 운영서버(20)와의 통신에 따라 데이터를 암호화하기 위한 메시지 큐 관리를 수행한다. 이 경우, 메시지 큐 관리부(444)는 WiFi 신호가 수신되면, 데이터에 대한 보안처리가 필요한지에 따라 메시지 큐를 관리하여 암호보안 처리부(42)를 통해 암호화한다.
- [0052] 특히, 메시지 큐 관리부(444)는 충전기(30)와 전기차(10) 간의 통신, 및 충전기(30)와 운영서버(20) 간의 통신 중 기 설정된 우선순위에 따라 메시지 큐를 관리한다. 이 경우, 메시지 큐 관리부(444)는 충전기(30)와 전기차(10) 간의 통신, 및 충전기(30)와 운영서버(20) 간의 통신 중 충전기(30)와 전기차 간의 통신을 우선적으로 처리하도록 메시지 큐를 관리한다. 이는 충전기(30)와 전기차 간의 통신에는 타임아웃이 설정되어 있기 때문이다.
- [0053] 도 5 를 참조하면, 메시지 큐 관리부(444)는 전기차(10)와 운영서버(20)로부터 메시지가 동시에 수신되었는지 판단하고(S202), 메시지가 동시에 수신되었으면, 충전기(30)와 전기차(10) 간의 통신을 위한 메시지 큐를 생성하여 암호보안 처리부(42)가 AES 암호화 처리를 우선 수행한다(S204).
- [0054] 이어, 메시지 큐 관리부(444)는 충전기(30)와 운영서버(20) 간의 통신을 위한 메시지 큐를 생성하여 암호보안 처리부(42)가 ARIA 암호화 처리를 수행한다(S206).
- [0055] 한편, 단계(S202)의 판단 결과 전기차(10)와 운영서버(20)로부터 메시지가 동시에 수신되지 않았으면, 메시지 큐 관리부(444)는 전기차(10)로부터 메시지가 우선 수신되어 충전기(30)와 전기차 간의 차량 통신이 먼저 이루어졌는지를 판단한다(S208).

- [0056] 단계(S208)에서의 판단 결과, 충전기(30)와 전기차 간의 차량 통신이 먼저 이루어지면, 메시지 큐 관리부(444)가 충전기(30)와 전기차(10) 간의 통신을 위한 메시지 큐를 생성하고, 암호보안 처리부(42)가 AES 암호화 처리를 수행한다(S210).
- [0057] 반면에, 단계(208)에서의 판단 결과, 충전기(30)와 전기차(10) 간의 차량 통신이 먼저 이루어지지 않으면, 메시지 큐 관리부(444)가 충전기(30)와 운영서버(20) 간의 통신을 위한 메시지 큐를 생성하고, 암호보안 처리부(42)가 ARIA 암호화 처리를 수행한다(S212).
- [0058] 운영서버 프로토콜 판단부(446)는 운영서버(20)와의 통신을 위한 운영서버 프로토콜을 판단한다. 일 예로, 운영서버 프로토콜 판단부(446)는 해당 운영서버 프로토콜이 기존 방식 프로토콜, 예컨대 KEPCO 프로토콜인지, 아니면 OCPP(Open Charge Point Protocol) 프로토콜인지를 판단한다.
- [0059] 제1 운영서버 프로토콜 처리부(447)는 운영서버 프로토콜 판단부(446)의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 보안처리 프로토콜 메시지, 예를 들어 인증서 관리, 개인키 관리 및 전자서명 등 보안에 해당되는 프로토콜 메시지를 처리한다.
- [0060] 제2 운영서버 프로토콜 처리부(448)는 운영서버 프로토콜 판단부(446)의 판단 결과에 따른 운영서버 프로토콜에서 기 정의된 일반처리 프로토콜 메시지, 예를 들어 상기한 보안처리 프로토콜 메시지를 제외한 충전 운영이나 개량과 관련된 프로토콜 메시지를 처리한다. 이 경우, 제2 운영서버 프로토콜 처리부(448)는 OCPP 프로토콜과 같이 기존의 충전기(30)에서 처리하기 어려운 프로토콜 메시지를 선택적으로 처리한다.
- [0061] 도 6 을 참조하면, 먼저 운영서버 프로토콜 판단부(446)는 운영서버(20)와 충전기(30) 간에 송수신되는 메시지가 TLS(Transport Layer Security) 메시지인지를 판단하고(S302), TLS 메시지이면, 메시지 큐 관리부(444)가 운영서버(20)와의 통신을 위한 메시지 큐를 생성한다. 이에 따라, 암호보안 처리부(42)가 해당 TLS 메시지를 복호화한다(S304).
- [0062] 이어, 운영서버 프로토콜 판단부(446)는 복호화된 메시지를 통해 OCPP 프로토콜인지를 판단하고(S306). OCPP 프로토콜이면 충전기(30)에서 처리가 가능한 프로토콜 메시지인지를 판단한다(S308).
- [0063] 이 경우, 충전기(30)에서 처리가 가능한 프로토콜 메시지가 아니면, 즉 기존의 충전기(30)에서 처리하기 어려운 프로토콜 메시지이면, 제1 운영서버 프로토콜 처리부(447)가 인증서 관리, 개인키 관리 및 전자서명 등 보안에 해당되는 보안처리 프로토콜 메시지를 처리한다(S310).
- [0064] 한편, 단계(S306)의 판단 결과 OCPP 프로토콜이 아니면, 보안버전이 있는지를 판단하고(S312), 판단 결과 보안버전이 있으면, 암호보안 처리부(42)가 개인 인증서 관리, 개인키 관련 메시지를 처리(S314)하여 충전기(30)에 전달한다.
- [0065] 반면에, 단계(S312)의 판단 결과 보안버전이 없으면, 운영서버 프로토콜 판단부(446)는 해당 프로토콜 메시지를 충전기(30)에 보안버전이 있는 메시지를 제외한 기타 메시지를 충전기(30)로 전송한다(S316).
- [0066] 한편, 단계(S302)에서의 판단 결과 TLS 메시지가 아니면, 운영서버 프로토콜 판단부(446)는 SOCKS5인지를 판단하고(S318), 판단 결과 SOCKS5이면 부가서비스 연계부(441)가 VAS(value added service)를 연계(S320)시켜 VAS로 명기된 부가서비스를 제공할 수 있도록 한다.
- [0067] 로컬인증 처리부(449)는 고객 계약인증서를 인증서 CRL 기반으로 충전기(30)에서 인증하여 충전을 허가하고, 정산을 위한 충전기록을 관리한다. 즉, 로컬인증 처리부(449)는 고객 계약인증서를 인증서 CRL 기반으로 충전기(30)에서 인증하여 충전을 허가하며, 향후 정산을 위한 충전기록을 관리하는 기능을 수행함으로써, 운영서버(20)와의 네트워크 장애시 충전이 가능토록 한다. 이러한 로컬인증 처리부(449)는 기타 서비스 측면에서 선택적으로 사용될 수 있다.
- [0068] 고객인증서 CRL 관리부(4410)는 고객 계약인증서의 폐기목록(CRL)을 주기적으로 수집 및 관리하고 로컬 인증에 활용할 수 있도록 한다.
- [0069] 부가서비스 연계부(4411)는 상기한 충전운영과 관련된 메시지 이외에 부가서비스, 즉 ISO/IEC 15118에서 VAS(value added service)로 명기된 부가서비스를 제공한다.
- [0070] 이와 같이, 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치는 향후 개정되는 전기차와 충전기 간의 프로토콜, 전기차와 충전기 간의 통신 방식, 및 충전기와 운영서버 간의 프로토콜을 확장성 있게 수용

할 수 있다.

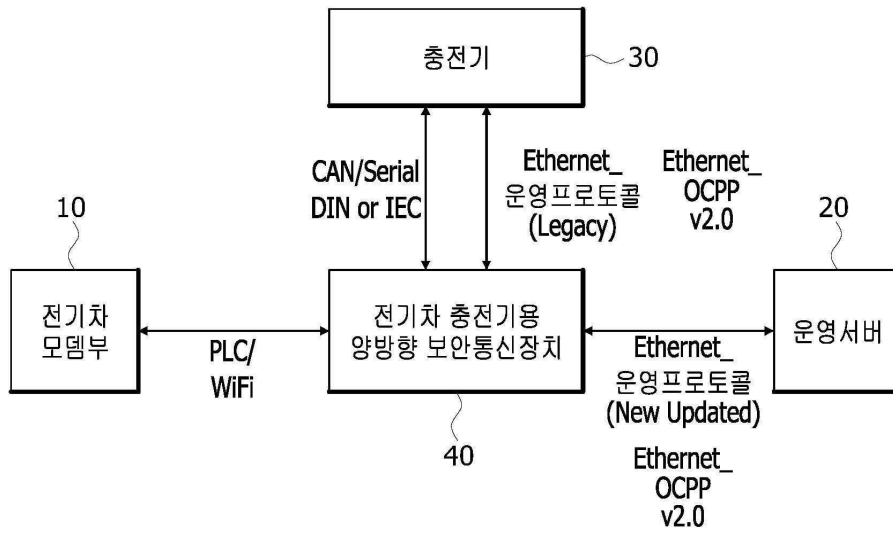
- [0071] 또한, 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치는 기존 충전기 내부 통신링크 사이에 연결되어 전기차와 충전기, 및 충전기와 운영서버 간의 통신을 개선할 뿐만 아니라 보안기능(TLS)을 제공하여 보다 안전한 통신채널을 확보할 수 있도록 한다.
- [0072] 게다가, 본 발명의 일 실시예에 따른 전기차 충전기용 양방향 보안통신장치는 기존에 상당수 보급된 충전 인프라의 기능 업그레이드를 저비용으로 수행할 수 있어 보급사업에 효율적으로 이용될 수 있다.
- [0073] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며 당해 기술이 속하는 기술분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 아래의 특허청구범위에 의하여 정해져야할 것이다.

**부호의 설명**

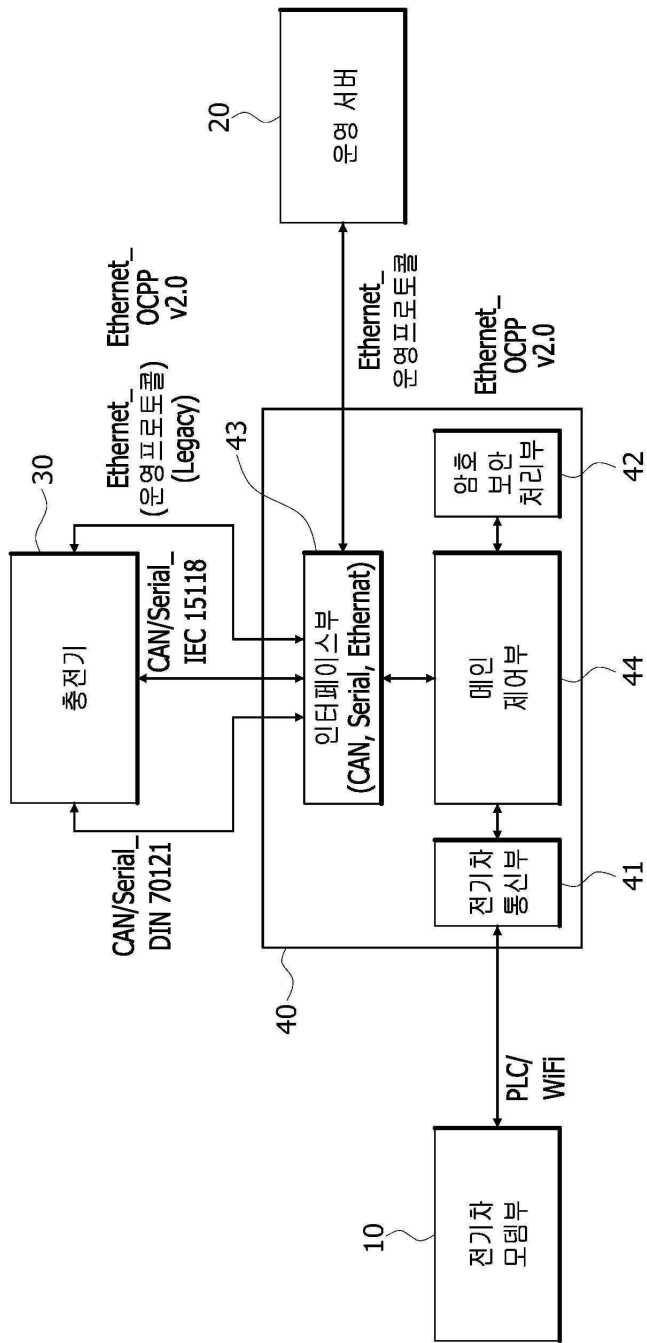
- [0075] 10: 전기차 모델부 20: 운영서버
- 30: 충전기
- 40: 전기차 충전기용 양방향 보안통신장치
- 41: 전기차 통신부 42: 암호보안 처리부
- 43: 인터페이스부 44: 메인 제어부
- 441: 통신매체 프로토콜 처리부
- 442: 전기차 충전 프로토콜 판단부
- 443: 전기차 충전 프로토콜 처리부
- 444: 메시지 큐 관리부
- 445: 보안기능 처리부
- 446: 운영서버 프로토콜 판단부
- 447: 제1 운영서버 프로토콜 처리부
- 448: 제2 운영서버 프로토콜 처리부
- 449: 로컬인증 처리부
- 4410: 고객인증서 CRL 관리부
- 4411: 부가서비스 연계부

도면

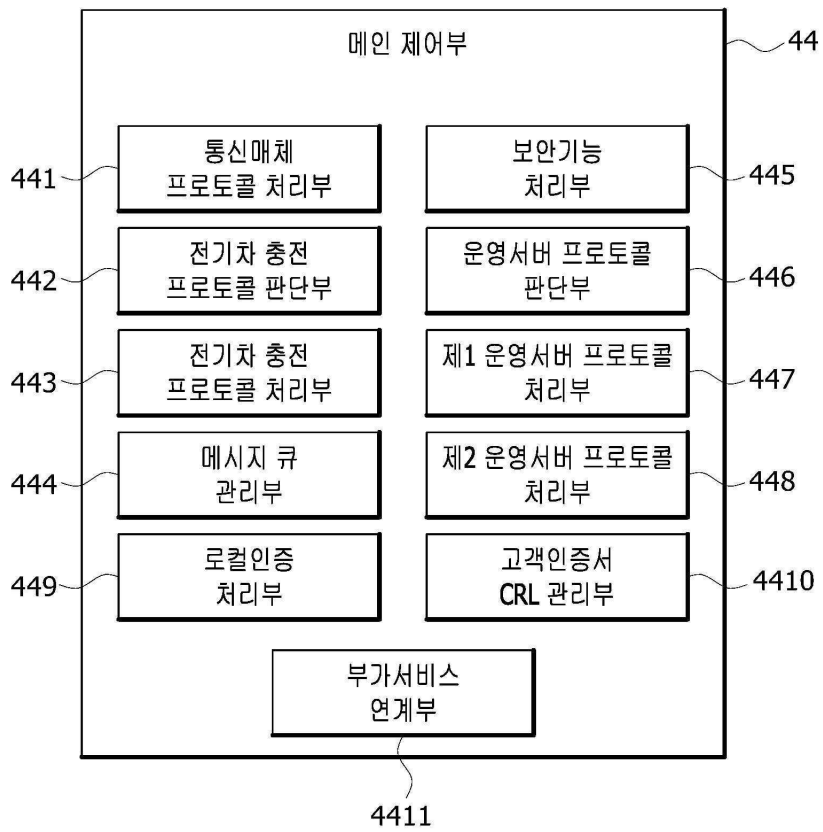
도면1



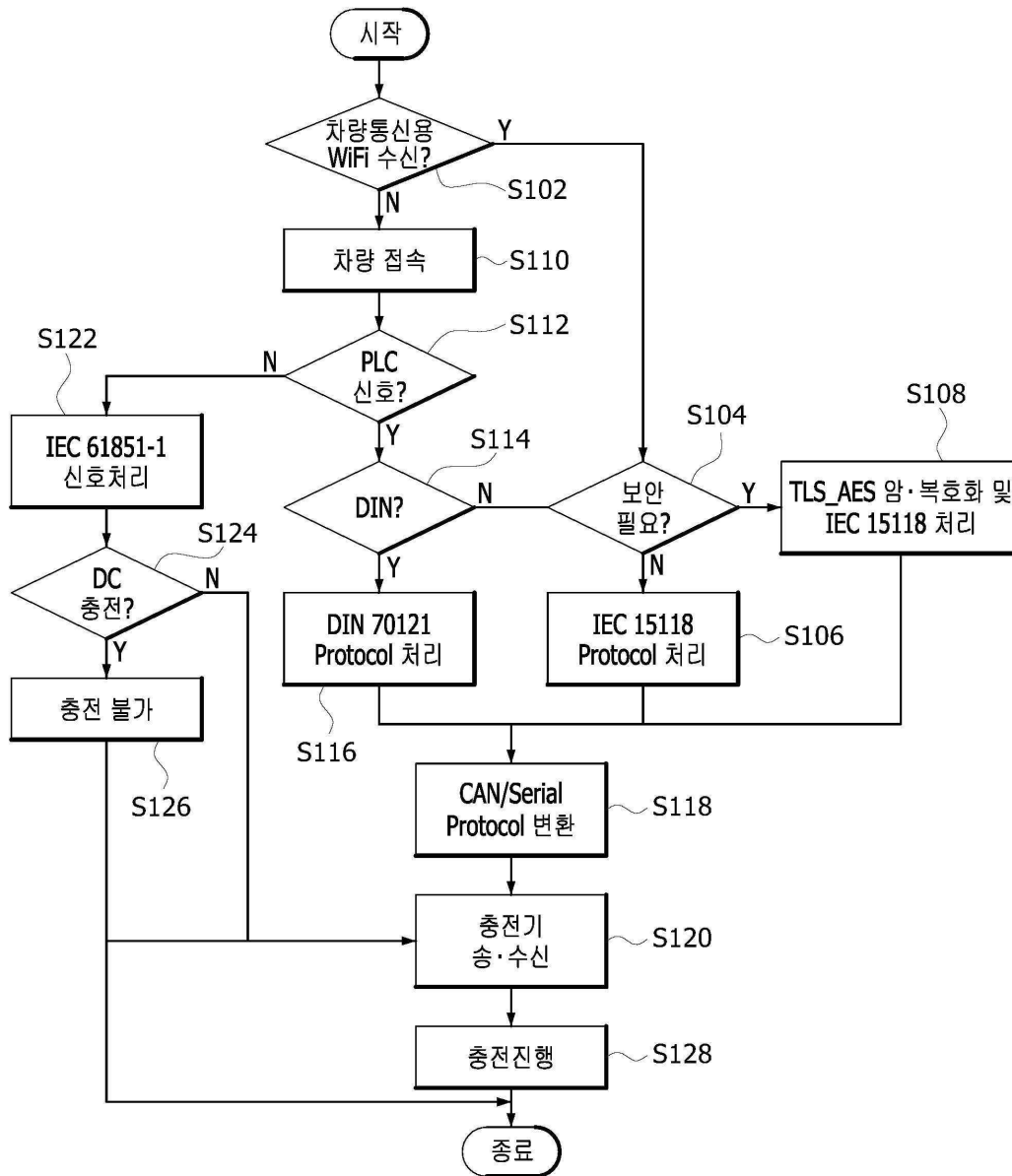
도면2



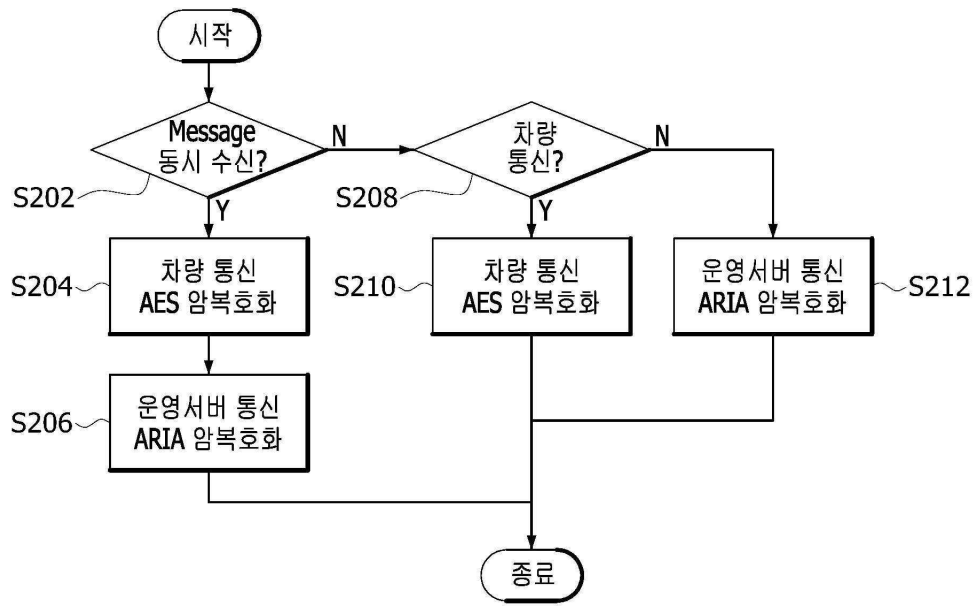
도면3



도면4



도면5



도면6

