(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년05월26일
(11) 등록번호 10-2256730
(24) 등록일자 2021년05월20일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
H04W 12/06 (2021.01) *H04W 12/12* (2021.01)
H04W 4/40 (2018.01)
(52) CPC특허분류
H04L 63/0815 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2020-0126022
(22) 출원일자 2020년09월28일
심사청구일자 2020년09월28일
(56) 선행기술조사문헌
KR101400275 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호(신천동, 파크리오)
조민재
서울특별시 동작구 사당로 180-6, 201호 (사당동)
(74) 대리인
두호특허법인

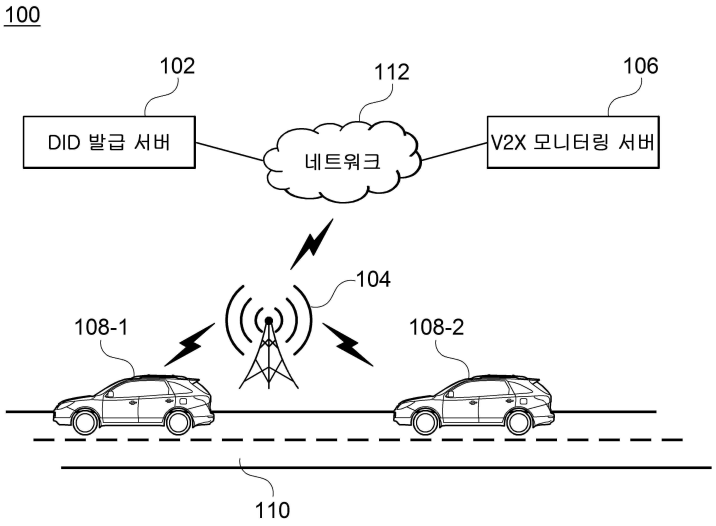
전체 청구항 수 : 총 15 항 심사관 : 문형섭

(54) 발명의 명칭 **차량 인증 및 통신 시스템 및 방법**

(57) 요 약

차량 인증 및 통신 시스템 및 방법이 개시된다. 일 실시예에 따른 차량 인증 및 통신 시스템은 차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장하는 DID 발급 서버; 상기 차량의 DID를 이용하여 상기 차량을 인증하고, 인증된 상기 차량으로 서명키 및 암호키 중 하나 이상을 송신하는 노변 기지국(RSU; Road Side Unit); 및 상기 노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지하는 V2X 모니터링 서버를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0823 (2013.01)
H04L 63/1408 (2013.01)
H04L 67/1097 (2013.01)
H04L 9/0833 (2013.01)
H04L 9/3255 (2013.01)
H04W 12/069 (2021.01)
H04W 12/122 (2021.01)
H04W 4/40 (2020.05)
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116145
과제번호	2018-0-01423-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터육성지원사업
연구과제명	지능형 비행로봇 융합 기술 연구
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장하는 DID 발급 서버;

상기 차량의 DID를 이용하여 상기 차량을 인증하고, 인증된 상기 차량으로 서명키 및 암호키 중 하나 이상을 송신하는 노변 기지국(RSU; Road Side Unit);

메시지를 그룹 서명키로 서명하여 제1 서명값을 생성하고, 상기 메시지를 자신의 DID 개인키로 서명하여 제2 서명값을 생성하는 차량; 및

상기 노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지하는 V2X 모니터링 서버를 포함하되,

상기 서명키는, 그룹 서명키 및 그룹 서명 검증키를 포함하는 차량 인증 및 통신 시스템.

청구항 2

청구항 1에 있어서,

상기 DID 발급 서버는, 생성한 상기 DID를 상기 차량으로 송신하고, 상기 차량은 수신된 상기 DID를 저장하는, 차량 인증 및 통신 시스템.

청구항 3

청구항 1에 있어서,

상기 노변 기지국은, 상기 차량으로부터 상기 DID를 수신하고, 상기 차량으로부터 수신되는 상기 DID 및 상기 블록체인에 기 저장된 DID를 비교하여 상기 차량을 인증하는, 차량 인증 및 통신 시스템.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 차량은,

상기 메시지, DID, 상기 제1 서명값, 및 상기 제2 서명값을 수신 차량으로 송신하는, 차량 인증 및 통신 시스템.

청구항 6

청구항 5에 있어서,

상기 차량은, 상기 메시지를 상기 암호키로 암호화하여 암호문을 생성하고, 상기 메시지를 상기 암호문으로 대체하여 상기 수신 차량으로 송신하는, 차량 인증 및 통신 시스템.

청구항 7

청구항 6에 있어서,

상기 수신 차량은, 상기 암호키를 이용하여 상기 암호문을 복호화하여 상기 메시지를 생성하는, 차량 인증 및 통신 시스템.

청구항 8

청구항 5에 있어서,

상기 수신 차량은, 상기 그룹 서명 검증키로 상기 제1 서명값을 검증하고,

검증에 성공한 경우, 상기 차량의 DID 공개키로 상기 제2 서명값을 검증하는, 차량 인증 및 통신 시스템.

청구항 9

청구항 8에 있어서,

상기 수신 차량은, 상기 제1 서명값 또는 상기 제2 서명값의 검증에 실패한 경우, 수신된 상기 메시지를 폐기하고, 상기 노변 기지국으로 알림을 송신하는, 차량 인증 및 통신 시스템.

청구항 10

청구항 8에 있어서,

상기 수신 차량은, 상기 제2 서명값의 검증에 성공한 경우 상기 노변 기지국에 상기 차량의 DID를 송신하는, 차량 인증 및 통신 시스템.

청구항 11

청구항 10에 있어서,

상기 노변 기지국은, 상기 블록체인을 이용하여 상기 수신 차량으로부터 수신한 상기 차량의 DID를 검증하고, 검증 결과를 상기 수신 차량으로 송신하는, 차량 인증 및 통신 시스템.

청구항 12

청구항 11에 있어서,

상기 노변 기지국은, 상기 차량 DID의 검증에 실패한 경우 상기 서명키 및 암호키를 재생성하는, 차량 인증 및 통신 시스템.

청구항 13

청구항 1에 있어서,

상기 V2X 모니터링 서버는,

상기 악의적인 차량의 존재가 탐지되는 경우, 해당 차량의 정보를 상기 노변 기지국 및 상기 DID 발급 서버로 송신하는, 차량 인증 및 통신 시스템.

청구항 14

청구항 13에 있어서,

상기 DID 발급 서버는, 상기 V2X 모니터링 서버로부터 수신되는 상기 악의적인 차량에 대응되는 DID를 상기 블록체인에서 폐기하는, 차량 인증 및 통신 시스템.

청구항 15

청구항 13에 있어서,

상기 노변 기지국은, 상기 V2X 모니터링 서버로부터 악의적인 차량의 정보가 수신되는 경우, 상기 서명키 및 암호키를 재생성하는, 차량 인증 및 통신 시스템.

청구항 16

차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장하는 단계;

상기 차량의 DID를 이용하여 상기 차량을 인증하고, 인증된 상기 차량으로 서명키 및 암호키 중 하나 이상을 송신하는 단계;

메시지를 그룹 서명키로 서명하여 제1 서명값을 생성하고, 상기 메시지를 자신의 DID 개인키로 서명하여 제2 서명값을 생성하는 차량; 및

노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지하는 단계를 포함하되,

상기 서명키는, 그룹 서명키 및 그룹 서명 검증키를 포함하는 차량 인증 및 통신 방법.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 V2X(Vehicle to Everything) 환경에서 차량을 인증하고 악의적인 차량으로부터 보호하기 위한 인증 및 통신 기술과 관련된다.

배 경 기 술

[0003] V2X(Vehicle to Everything) 통신이란, 차량이 유선 또는 무선망을 통해 다른 차량 및 도로 등 인프라가 구축된 사물과 정보를 교환하는 것을 의미하며, V2V(Vehicle to Vehicle), V2I(Vehicle to Infrastructure), V2N(Vehicle to Nomadic Device), V2P(Vehicle to Pedestrian) 등을 총칭한다.

[0004] V2X와 관련된 보안 표준은 IEEE 1609.2에서 정의된다. IEEE 1609.2에서 제공하는 V2X 보안은 PKI(Public Key Infrastructure) 기반 인증서를 통한 서명 및 암호화 방식으로 통신이 진행된다. 그러나 기존 표준에 따른 방식은 인증서를 관리하는 측면에서 오버헤드(overhead)가 발생하고, 또한 차량의 경우 주기적으로 인증서를 교체해 주어야 하는 문제점이 존재한다.

발명의 내용

해결하려는 과제

[0006] 개시되는 실시예들은 V2X(Vehicle to Everything) 환경에서 차량을 인증하고 악의적인 차량으로부터 보호하기 위한 기술적인 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0008] 예시적인 실시예에 따르면, 차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장하는 DID 발급 서버; 상기 차량의 DID를 이용하여 상기 차량을 인증하고, 인증된 상기 차량으로 서명키 및 암호키 중 하나 이상을 송신하는 노변 기지국(RSU; Road Side Unit); 및 상기 노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지하는 V2X 모니터링 서버를 포함하는 차량 인증 및 통신 시스템이 제공된다.

[0009] 상기 DID 발급 서버는, 생성한 상기 DID를 상기 차량으로 송신하고, 상기 차량은 수신된 상기 DID를 저장할 수 있다.

[0010] 상기 노변 기지국은, 상기 차량으로부터 상기 DID를 수신하고, 상기 차량으로부터 수신되는 상기 DID 및 상기 블록체인에 기 저장된 DID를 비교하여 상기 차량을 인증할 수 있다.

[0011] 상기 서명키는, 그룹 서명키 및 그룹 서명 검증키를 포함할 수 있다.

[0012] 상기 차량은, 메시지를 상기 그룹 서명키로 서명하여 제1 서명값을 생성하고, 상기 메시지를 자신의 DID 개인키로 서명하여 제2 서명값을 생성하며, 상기 메시지, DID, 상기 제1 서명값, 및 상기 제2 서명값을 수신 차량으로 송신할 수 있다.

[0013] 상기 차량은, 상기 메시지를 상기 그룹키로 암호화하여 암호문을 생성하고, 상기 메시지를 상기 암호문으로 대체하여 상기 수신 차량으로 송신할 수 있다.

[0014] 상기 수신 차량은, 상기 그룹키를 이용하여 상기 암호문을 복호화하여 상기 메시지를 생성할 수 있다.

[0015] 상기 수신 차량은, 상기 그룹 서명 검증키로 상기 제1 서명값을 검증하고, 검증에 성공한 경우, 상기 차량의 DID 공개키로 상기 제2 서명값을 검증할 수 있다.

[0016] 상기 수신 차량은, 상기 제1 서명값 또는 상기 제2 서명값의 검증에 실패한 경우, 수신된 상기 메시지를 폐기하고, 상기 노변 기지국으로 알림을 송신할 수 있다.

[0017] 상기 수신 차량은, 상기 제2 서명값의 검증에 성공한 경우 상기 노변 기지국에 상기 차량의 DID를 송신할 수 있다.

[0018] 상기 노변 기지국은, 상기 블록체인을 이용하여 상기 수신 차량으로부터 수신한 상기 차량의 DID를 검증하고, 검증 결과를 상기 수신 차량으로 송신할 수 있다.

[0019] 상기 노변 기지국은, 상기 차량 DID의 검증에 실패한 경우 상기 서명키 및 암호키를 재생성할 수 있다.

[0020] 상기 V2X 모니터링 서버는, 상기 악의적인 차량의 존재가 탐지되는 경우, 해당 차량의 정보를 상기 노변 기지국 및 상기 DID 발급 서버로 송신할 수 있다.

[0021] 상기 DID 발급 서버는, 상기 V2X 모니터링 서버로부터 수신되는 상기 악의적인 차량에 대응되는 DID를 상기 블록체인에서 폐기할 수 있다.

[0022] 상기 노변 기지국은, 상기 V2X 모니터링 서버로부터 악의적인 차량의 정보가 수신되는 경우, 상기 서명키 및 암호키를 재생성할 수 있다.

[0023] 다른 예시적인 실시예에 따르면, 차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장하는 단계; 상기 차량의 DID를 이용하여 상기 차량을 인증하고, 인증된 상기 차량으로 서명키 및 암호키 중 하나 이상을 송신하는 단계; 및 상기 노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지하는 단계를 포함하는 차량 인증 및 통신 방법이 제공된다.

발명의 효과

[0025] 개시되는 실시예에 따르면, V2X의 보안을 위하여 DID(Decentralized Identification)을 사용함으로써 인증서 관리의 오버헤드를 방지하고 차량이 주기적으로 인증서를 교체하여야 하는 문제를 방지할 수 있다.

[0026] 또한 V2X 메시지를 모니터링하여 악의적인 차량을 탐지하고 이에 따라 V2X 통신에 사용되는 키를 교체함으로써 악의적인 차량으로 인한 보안 위협을 차단할 수 있다.

도면의 간단한 설명

[0028] 도 1은 일 실시예에 따른 차량 인증 및 통신 시스템(100)을 설명하기 위한 블록도

도 2는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 셋업(setup) 과정(200)을 설명하기 위한 흐름도

도 3은 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 차량 인증(vehicle authentication) 과정(300)을 설명하기 위한 흐름도

도 4는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 서명된 메시지 송수신 과정(400)을 설명하기 위한 흐름도

도 5는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 암호화된 메시지 송수신 과정(500)을 설명하기 위한 흐름도

도 6은 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 악의적인 차량 모니터링 및 탐지 과정(600)을 설명하기 위한 흐름도

도 7은 일 실시예에 따른 차량 인증 및 통신 방법(700)을 설명하기 위한 흐름도

도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0030] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0032] 도 1은 일 실시예에 따른 차량 인증 및 통신 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 차량 인증 및 통신 시스템(100)은 DID 발급 서버(102), 노변 기지국(104), 및 V2X 모니터링 서버(106)를 포함한다.

[0033] DID 발급 서버(102)는 차량(108)으로부터 식별 정보를 수신하고, 이로부터 차량(108)의 DID(Decentralized Identification)를 생성한다. DID 발급 서버(102)는 생성된 상기 DID를 블록체인 네트워크(미도시)를 통해 블록체인에 저장한다. 또한 DID 발급 서버(102)는 생성한 상기 DID를 차량(108)으로 송신하고, 차량(108)은 수신된 상기 DID를 저장한다. 개시되는 실시예들에서, 블록체인을 기반으로 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 가질 수 있게 하는 방식의 신원 확인 체계에서 사용되는 아이디를 의미한다.

[0034] 노변 기지국(Road Side Unit, 104)은 도로(110)상의 차량(108)과 무선 네트워크를 통해 연결되어 차량(108)과 메시지를 주고받거나, 또는 차량(108)간의 메시지 송수신을 중계하기 위한 기지국이다. 개시되는 실시예들에서, 메시지를 송신하는 차량은 송신 차량(108-1)으로, 송신 차량(108-1으로부터 메시지를 수신하는 차량은 수신 차량(108-1)으로, 송신 차량(108-1) 및 수신 차량(108-2)을 포함하는 포괄적인 의미로 사용할 경우는 차량(108)으로 표기하기로 한다.

[0035] 노변 기지국(104)은 차량(108)으로부터 수신되는 DID를 블록체인 네트워크를 통해 인증한다. 일 실시예에서 노변 기지국(104)은 차량(108)으로부터 상기 DID를 수신하고, 수신된 DID 및 상기 블록체인에 기 저장된 DID를 비

교하여 차량(108)을 인증할 수 있다.

[0036] 차량(108)의 인증이 완료되면, 노변 기지국(104)은 인증된 차량(108)으로 서명키 및 암호키 중 하나 이상을 송신한다. 일 실시예에서, 상기 서명키는 차량(108) 간의 서명된 메시지 송수신을 위하여 사용되는 키로서 그룹 서명키(gsk) 및 그룹 서명 검증키(gvk)를 포함할 수 있다. 또한 상기 암호키(gk)는 차량(108) 간의 암호화된 메시지 송수신을 위하여 사용되는 일종의 그룹키이다. 개시되는 실시예들에서, 상기 암호키는 AES(Advanced Encryption Standard) 등의 대칭키 암호화에 사용되는 키일 수 있다.

[0037] V2X 모니터링 서버(106)는 노변 기지국(104)에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지한다. 일 실시예에서, V2X 모니터링 서버(106)는 악의적인 차량의 존재가 탐지되는 경우, 해당 차량의 정보를 노변 기지국(104) 및 DID 발급 서버(102)로 송신할 수 있다. 그러면 DID 발급 서버(104)는 V2X 모니터링 서버(106)로부터 수신되는 악의적인 차량에 대응되는 DID를 상기 블록체인에서 폐기할 수 있다. 또한 노변 기지국(104)은 V2X 모니터링 서버(106)로부터 악의적인 차량의 정보가 수신되는 경우, 상기 서명키 및 암호키를 재생성하여 악의적인 차량을 제외한 나머지 차량(108)에 재배포할 수 있다.

[0038] 개시되는 실시예들에서, DID 발급 서버(102), 노변 기지국(104) 및 V2X 모니터링 서버(106)는 네트워크(112)를 통하여 메시지를 송수신할 수 있다. 개시되는 실시예들에서, 몇몇 실시예들에서, 네트워크(112)는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wide area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0040] 도 2는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 셋업(setup) 과정(200)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0041] 단계 202에서, DID 발급 서버(102)는 차량(108)으로부터 차량 식별 정보를 수신한다. 개시되는 실시예에서, 차량 식별 정보는 특정 차량을 타 차량과 구분하기 위한 모든 종류의 정보를 제한없이 포함할 수 있다.

[0042] 단계 204에서, DID 발급 서버(102)는 수신된 상기 차량 식별 정보를 기반으로 차량 DID를 생성한다.

[0043] 단계 206에서, DID 발급 서버(102)는 생성된 차량 DID를 블록체인에 저장한다.

[0044] 단계 208에서, DID 발급 서버(102)는 생성된 차량 DID를 차량(108)으로 전송한다.

[0046] 도 3은 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 차량 인증(vehicle authentication) 과정(300)을 설명하기 위한 흐름도이다.

[0047] 단계 302에서, 노변 기지국(104)은 차량(108)으로부터 차량 DID를 수신한다.

[0048] 단계 304에서, 노변 기지국(104)은 수신된 상기 차량 DID를 블록체인을 통해 인증한다. 일 실시예에서 노변 기지국(104)은 차량(108)으로부터 수신된 DID 및 상기 블록체인에 기 저장된 DID를 비교하여 차량(108)을 인증할 수 있다.

[0049] 단계 306에서, 노변 기지국(104)은 인증된 차량(108)에게 서명키 및 암호키 중 하나 이상을 송신한다. 일 실시예에서, 상기 서명키는 차량(108) 간의 서명된 메시지 송수신을 위하여 사용되는 키로서 그룹 서명키(gsk) 및 그룹 서명 검증키(gvk)를 포함할 수 있다. 또한 상기 암호키(gk)는 차량(108) 간의 암호화된 메시지 송수신을 위하여 사용되는 일종의 그룹키이다.

[0051] 도 4는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 서명된 메시지 송수신 과정(400)을 설명하기 위한 흐름도이다.

[0052] 단계 402에서, 송신 차량(108-1)은 전송할 메시지(m)를 생성한다.

[0053] 단계 404에서, 송신 차량(108-1)은 생성한 메시지(m)를 서명한다. 구체적으로 송신 차량(108-1)은 메시지(m)를 그룹 서명키(gsk)로 서명하여 제1 서명값(σ_R)을 생성한다. 일 실시예에서, 송신 차량(108-1)은 타원곡선 디지털서명 알고리즘(ECDSA; Elliptic Curve Digital Signature Algorithm)을 이용하여 상기 제1 서명값을 생성할 수 있다. 또한 송신 차량(108-1)은 생성한 메시지(m)를 자신의 DID에 대응되는 개인키로 서명하여 제2 서명값(σ_S)을 생성한다.

[0054] 단계 406에서, 송신 차량(108-1)은 메시지(m), 제1 서명값(σ_R), 제2 서명값(σ_S), 및 송신 차량(108-1)의 DID를 수신 차량(108-2)으로 송신한다.

[0055] 단계 408에서, 수신 차량(108-2)은 수신된 제1 서명값(σ_R), 및 제2 서명값(σ_S)을 검증한다. 구체적으로 수신 차량(108-2)은 수신된 메시지(m), 제1 서명값(σ_R) 및 그룹 서명 검증키(gvk)를 이용하여 제1 서명값(σ_R)을 검증한다. 만약 상기 1차 검증에 실패한 경우 수신 차량(108-2)은 수신된 메시지(m)를 폐기하고 노변 기지국(104)으로 알림 메시지를 전송할 수 있다.

[0056] 만약 상기 1차 검증에 성공한 경우, 다음으로 수신 차량(108-2)은 수신된 메시지(m), 제2 서명값(σ_S) 및 송신 차량(108-1)의 DID에 대응되는 공개키를 이용하여 제2 서명값(σ_S)을 검증한다. 만약 상기 2차 검증에 실패한 경우 수신 차량(108-2)은 수신된 메시지(m)를 폐기하고 노변 기지국(104)으로 알림 메시지를 전송할 수 있다. 일 실시예에서, 상기 2차 검증은 상기 메시지(m)가 차량의 안전과 관련된 메시지인 경우에만 수행될 수 있다.

[0057] 검증이 완료된 경우, 단계 410에서 수신 차량(108-2)은 송신 차량(108-1)의 DID를 노변 기지국(104)으로 송신하여 송신 차량(108-1)의 DID에 대한 검증을 요청할 수 있다.

[0058] 단계 412에서, 수신 차량(108-2)은 수신된 송신 차량(108-1)의 DID를 블록체인을 통해 검증하고, 검증 결과를 수신 차량(108-2)으로 회신한다. 만약 송신 차량(108-1)의 검증에 실패한 경우, 상기 서명키 및 암호키를 재생성하여 송신 차량(108-1)을 제외한 차량(108)에 재배포할 수 있다.

[0060] 도 5는 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 암호화된 메시지 송수신 과정(500)을 설명하기 위한 흐름도이다.

[0061] 단계 502에서, 송신 차량(108-1)은 전송할 메시지(m)를 생성한다.

[0062] 단계 504에서, 송신 차량(108-1)은 생성한 메시지(m)를 암호화 및 서명한다. 먼저 송신 차량(108-1)은 메시지(m)를 그룹키(gk)로 암호화하여 암호문(C)을 생성한다. 다음으로 송신 차량(108-1)은 메시지(m)를 그룹 서명키(gsk)로 서명하여 제1 서명값(σ_R)을 생성한다. 일 실시예에서, 송신 차량(108-1)은 타원곡선 디지털서명 알고리즘(ECDSA; Elliptic Curve Digital Signature Algorithm)을 이용하여 상기 제1 서명값을 생성할 수 있다. 또한 송신 차량(108-1)은 생성한 메시지(m)를 자신의 DID에 대응되는 개인키로 서명하여 제2 서명값(σ_S)을 생성한다.

[0063] 단계 506에서, 송신 차량(108-1)은 암호문(C), 제1 서명값(σ_R), 제2 서명값(σ_S), 및 송신 차량(108-1)의 DID를 수신 차량(108-2)으로 송신한다.

[0064] 단계 508에서, 수신 차량(108-2)은 수신된 암호문을 복호화하고 서명값을 검증한다. 먼저 수신 차량(108-2)은 암호문(C)을 그룹키(gk)로 복호화하여 메시지(m)를 복원한다. 다음으로 수신 차량(108-2)은 복호화된 메시지(m), 제1 서명값(σ_R) 및 그룹 서명 검증키(gvk)를 이용하여 제1 서명값(σ_R)을 1차 검증한다. 만약 상기 1차 검증에 실패한 경우 수신 차량(108-2)은 복호화된 메시지(m)를 폐기하고 노변 기지국(104)으로 알림 메시지를 전송할 수 있다.

[0065] 만약 상기 1차 검증에 성공한 경우, 다음으로 수신 차량(108-2)은 수신된 메시지(m), 제2 서명값(σ_S) 및 송신 차량(108-1)의 DID에 대응되는 공개키를 이용하여 제2 서명값(σ_S)을 2차 검증한다. 만약 상기 2차 검증에 실패한 경우 수신 차량(108-2)은 복호화된 메시지(m)를 폐기하고 노변 기지국(104)으로 알림 메시지를 전송할 수 있다. 일 실시예에서, 상기 2차 검증은 상기 메시지(m)가 차량의 안전과 관련된 메시지인 경우에만 수행될 수 있다.

[0066] 검증이 완료된 경우, 단계 510에서 수신 차량(108-2)은 송신 차량(108-1)의 DID를 노변 기지국(104)으로 송신하여 송신 차량(108-1)의 DID에 대한 검증을 요청할 수 있다.

[0067] 단계 512에서, 수신 차량(108-2)은 수신된 송신 차량(108-1)의 DID를 블록체인을 통해 검증하고, 검증 결과를 수신 차량(108-2)으로 회신한다. 만약 송신 차량(108-1)의 검증에 실패한 경우, 상기 서명키 및 암호키를 재생성하여 송신 차량(108-1)을 제외한 차량(108)에 재배포할 수 있다.

[0069] 도 6은 일 실시예에 따른 차량 인증 및 통신 시스템(100)의 악의적인 차량 모니터링 및 탐지 과정(600)을 설명

하기 위한 흐름도이다.

[0070] 단계 602에서, V2X 모니터링 서버(106)는 노변 기지국(104)에서 수집되는 차량간 메시지(V2V 메시지)를 수신한다. 일 실시예에서, 노변 기지국(104)은 V2V 메시지를 수신하여 정기적 또는 비정기적으로 V2X 모니터링 서버(106)에 전송할 수 있다. 차량간 메시지는 SAE J2735 표준에서 정의된다. 주된 메시지는 다음과 같다.

[0071] - BSM(BasicSafetyMessage): 차량 상태와 관련된 safety data를 교환하는데 사용되는 메시지

[0072] - TIM(TravlerInformationMessage): 다양한 타입의 정보를 전송하기 위한 메시지 (예, 도로 표지판 정보 등)

[0073] - PVD(ProbeVehicleData): 차량의 주행정보 등 차량 상태를 수집하기 위한 메시지, 주로 기지국에 전송함

[0074] - RSA(RoadSideAlert): 차량에게 도로 상의 위험을 알리기 위한 메시지

[0075] - EVA(EmergencyVehicleAlert): 응급차량이 주변 차량에게 응급상황 경고를 알리는 메시지 (응급차량은 경찰차, 구급차, 소방차 등이 될 수 있음)

[0076] - SPAT(SignalPhaseandTiming Message): 기지국이 차량에 신호 현시 상태를 알리기 위한 메시지

[0077] - MAP(MapData): 기지국이 차량에게 전송하는 지도 데이터 메시지

[0078] 단계 604에서, V2X 모니터링 서버(106)는 수신 받은 메시지를 분석하여 악의적인 차량이 존재하는지 탐지한다. 개시되는 실시예들에서, 악의적인 차량이란 메시지를 조작하거나 변조하여 전송함으로써 정상적인 차량들의 도로 주행을 방해하는 차량을 의미한다. 예를 들어 도로 위험구간의 정보나, 차량 충돌 등의 정보를 담은 안전 관련 메시지를 변조하거나 조작하여 전송하거나 이를 임의로 생성하여 전송하는 차량을 악의적인 차량으로 정의할 수 있다. V2X 모니터링 서버(106)는 수신된 메시지간의 비교 분석, 또는 메시지에 포함된 정보와 실제 도로 상황과의 비교 분석 등을 통하여 변조되거나 조작된 메시지를 송신하는 악의적인 차량의 존재 여부를 탐지할 수 있다.

[0079] 만약 상기 604 단계의 탐지 결과 악의적인 차량이 탐지된 경우, 단계 606 및 608에서 V2X 모니터링 서버(106)는 해당 차량의 정보를 노변 기지국(104) 및 DID 발급 서버(102)로 송신한다.

[0080] 단계 610에서, 노변 기지국(104)은 V2X 모니터링 서버(106)로부터 악의적인 차량의 정보가 수신되는 경우, 상기 서명키 및 암호키를 재생성하여 악의적인 차량을 제외한 나머지 차량(108)에 재배포한다. 이와 같이 노변 기지국(104)에서 서명키 및 암호키를 재배포할 경우, 악의적인 차량은 새로 바뀐 서명키 및 암호키를 알 수 없게 되므로 악의적인 메시지가 추가로 전파되는 것을 방지할 수 있다.

[0081] 단계 612에서, DID 발급 서버(104)는 V2X 모니터링 서버(106)로부터 수신되는 악의적인 차량에 대응되는 DID를 상기 블록체인에서 폐기한다. 이 경우 악의적인 차량은 더 이상 노변 기지국(104)을 통하여 인증이 불가하게 되므로 역시 악의적인 메시지가 추가로 전파되는 것을 방지할 수 있다.

[0083] 도 7은 일 실시예에 따른 차량 인증 및 통신 방법(700)을 설명하기 위한 흐름도이다. 도시된 방법은 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치, 예컨대 전술한 차량 인증 및 통신 장치(100)에서 수행될 수 있다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0084] 단계 702에서, DID 발급 서버(102)는 차량의 식별 정보로부터 상기 차량의 DID(Decentralized Identification)를 생성하고, 생성된 상기 DID를 블록체인에 저장한다.

[0085] 단계 704에서, 노변 기지국(104)은 차량의 DID를 이용하여 차량을 인증하고, 인증된 차량으로 서명키 및 암호키 중 하나 이상을 송신한다.

[0086] 단계 706에서, V2X 모니터링 서버(106)는 노변 기지국(104)에서 수집되는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지한다.

[0088] 도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0089] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 실시예들에 따른 차량 인증 및 통신 시스템(100)에 포함된 장치들일 수 있다. 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0090] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0091] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0092] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(104)와 연결될 수도 있다.

[0094] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0095] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

[0096] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0097] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허

청구범위 뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0099] 100: 차량 인증 및 통신 시스템

102: DID 발급 서버

104: 노변 기지국

106: V2X 모니터링 서버

108-1: 송신 차량

108-2: 수신 차량

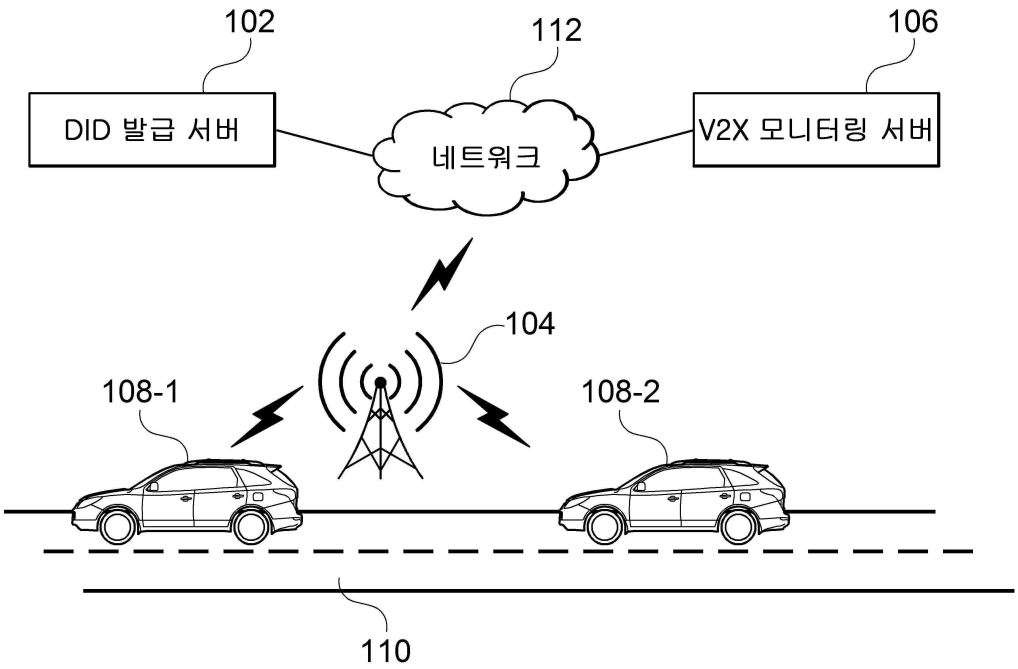
110: 도로

112: 네트워크

도면

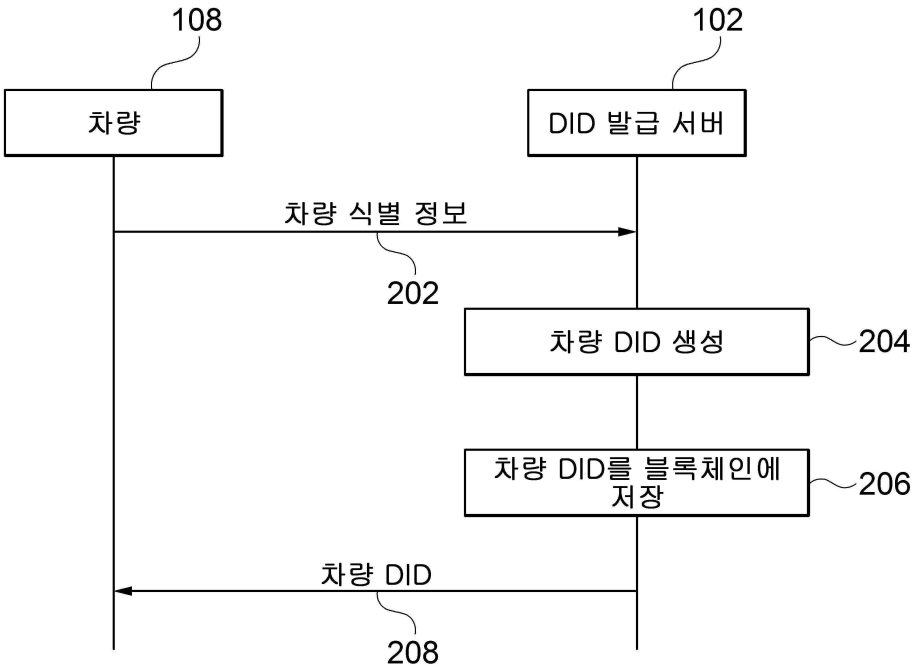
도면1

100



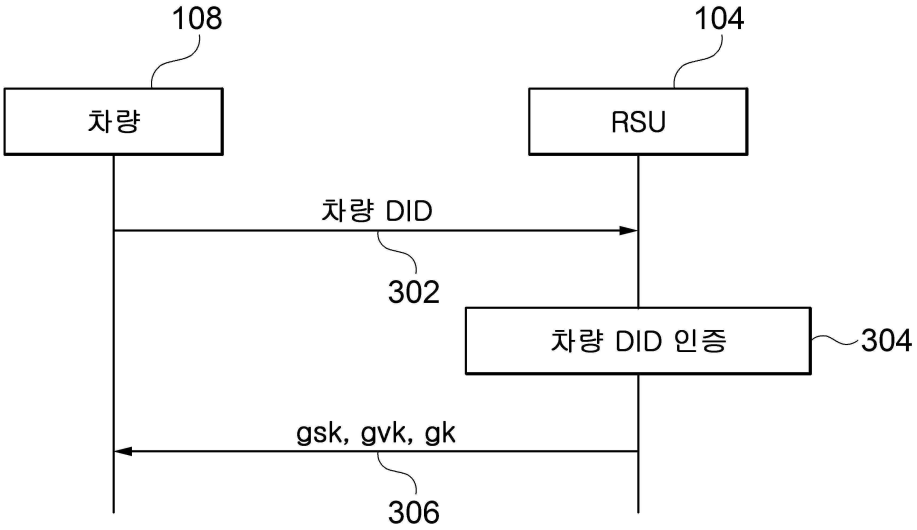
도면2

200



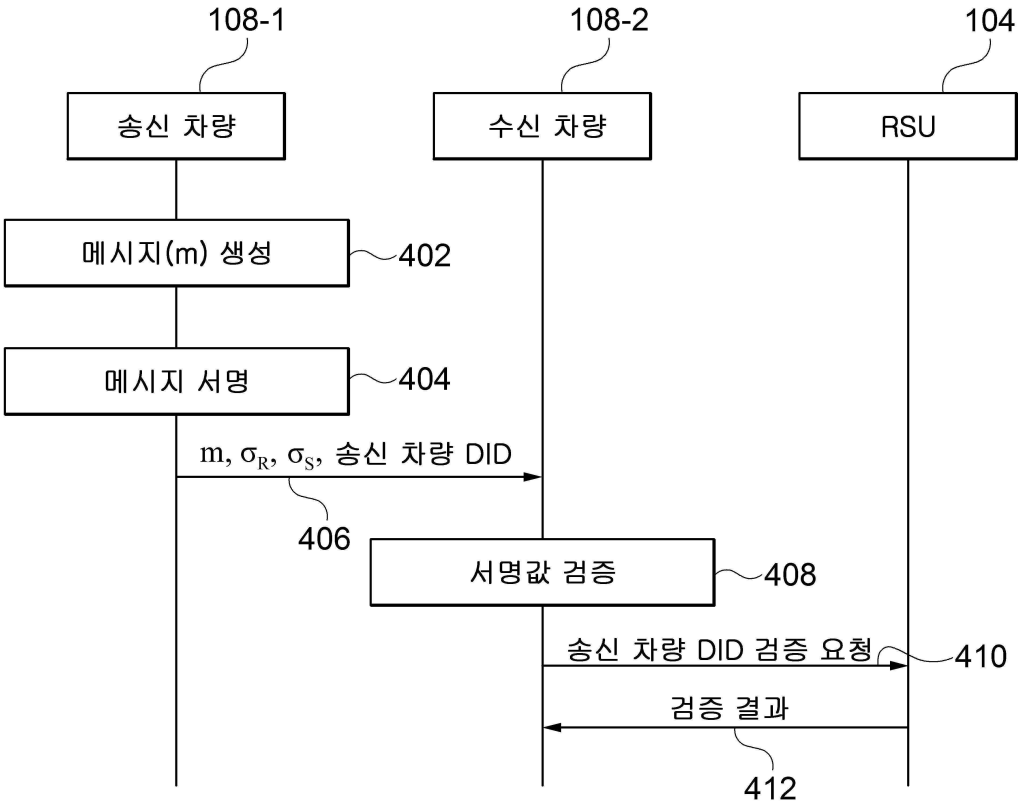
도면3

300



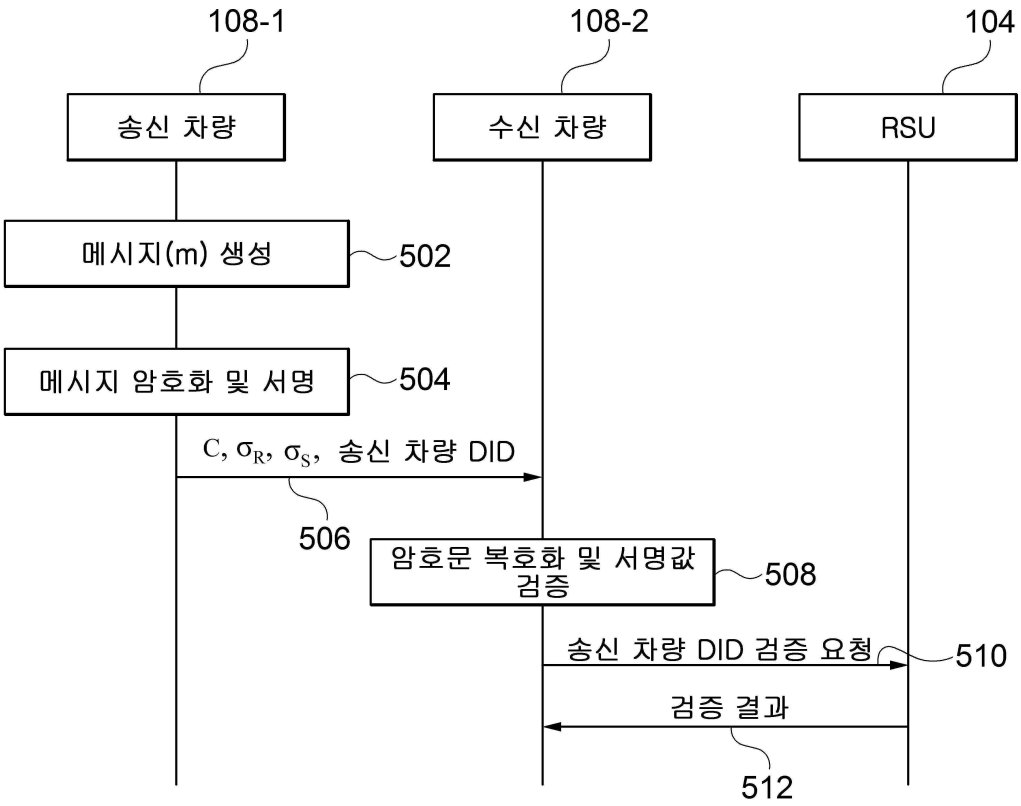
도면4

400


108-1
108-2
104
송신 차량
수신 차량
RSU
메시지(m) 생성
402
메시지 서명
404
m, σR, σS, 송신 차량 DID
406
서명값 검증
408
송신 차량 DID 검증 요청
410
검증 결과
412

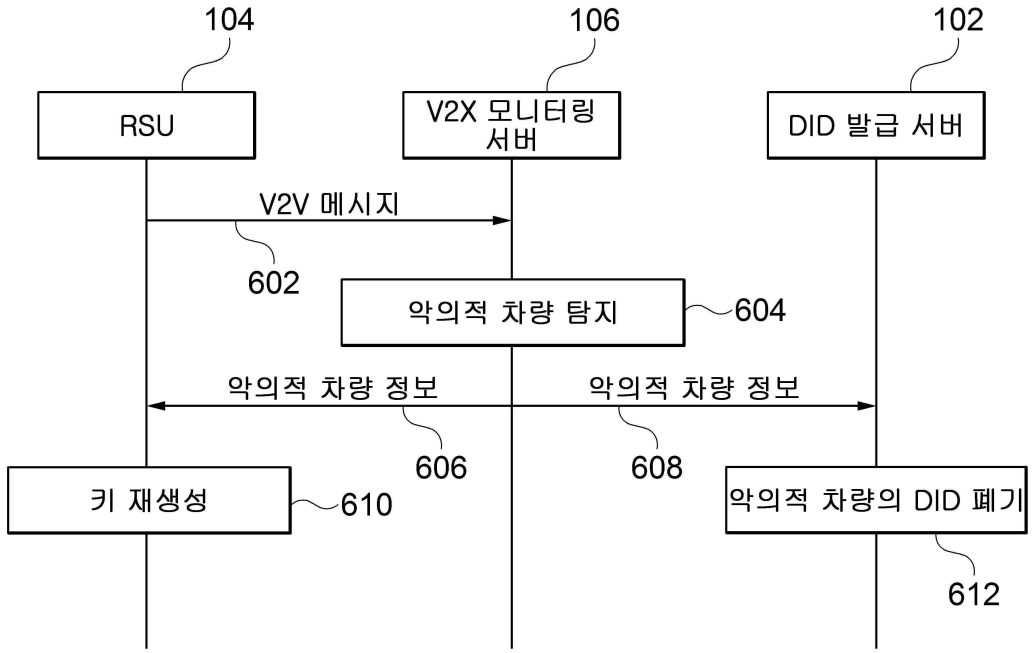
도면5

500

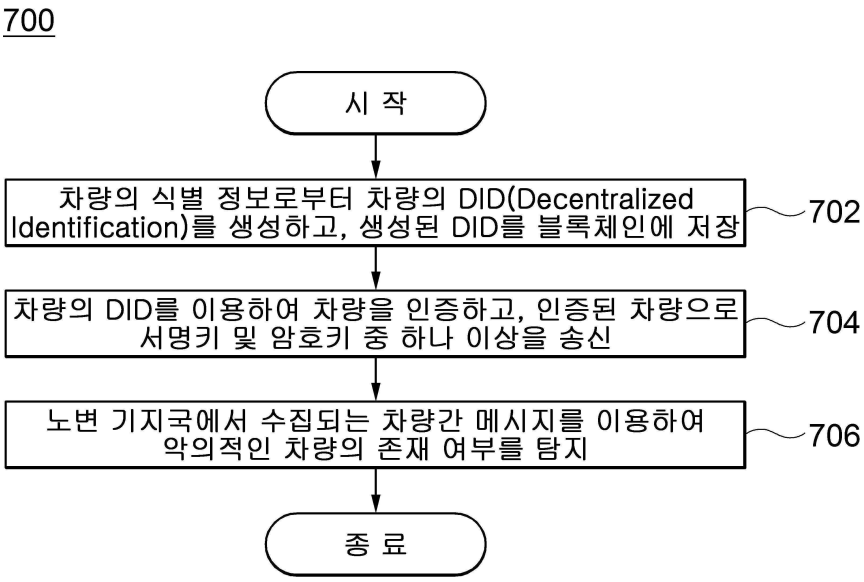


도면6

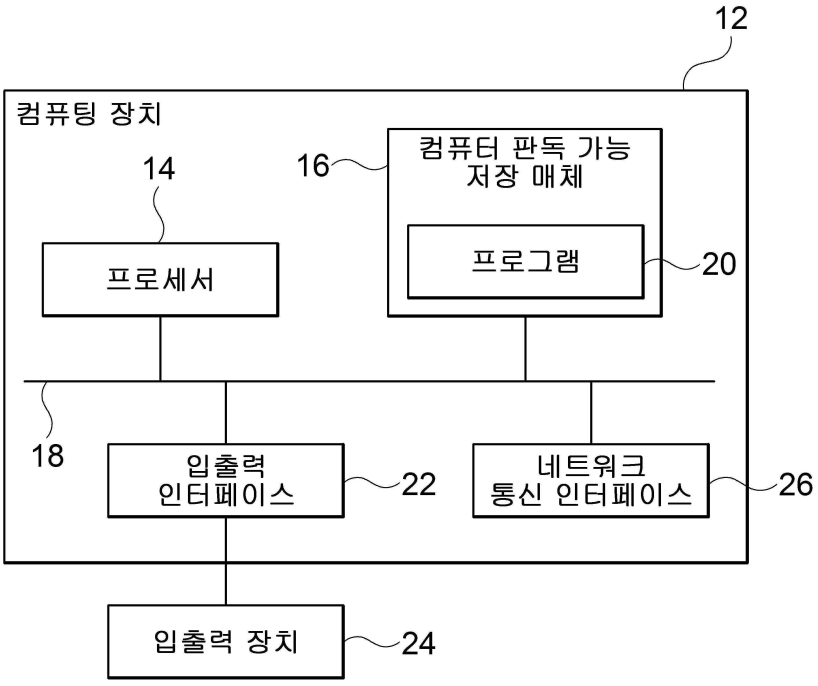
600



도면7


700
시 작
차량의 식별 정보로부터 차량의 DID(Decentralized Identification)를 생성하고, 생성된 DID를 블록체인에 저장
702
차량의 DID를 이용하여 차량을 인증하고, 인증된 차량으로 서명키 및 암호키 중 하나 이상을 송신
704
노변 기지국에서 수집되는 차량간 메시지를 이용하여 악의적인 차량의 존재 여부를 탐지
706
종 료

도면8


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능 저장 매체
프로그램
20
18
입출력 인터페이스
22
네트워크 통신 인터페이스
26
입출력 장치
24