



V2X 환경에서 블록체인을 이용하여 차량을 인증하기 위한 방법

기술 개요

Overview

① 적용분야

스마트카 및 스마트 모빌리티를 위한 V2X 통신 기술 분야

② 기술요약

V2X (Vehicle to Everything) 환경에서 차량 인증을 통해 악의적인 차량으로 보호하기 위한 인증 및 통신 기술에 관한 것으로, 차량의 식별 정보로부터 생성된 차량의 DID(Decentralized Identification)를 블록체인에 저장하고, 저장된 DID를 이용하여 차량 인증을 수행하고, 차량 사이에 전송되는 메시지 모니터링을 통해 악의적인 차량을 탐지함

③ 특허 권리 범위

- DID 발급 서버는 차량의 식별 정보로부터 차량의 DID를 생성하여 블록체인에 저장하고, 노변 기지국(RSU: Road Side Unit)은 차량의 DID를 이용하여 차량을 인증하고, 인증된 차량으로 그룹 서명키와 그룹 서명 검증키를 송신함. 차량은 그룹 서명키와 DID 개인키를 이용하여 서명된 메시지를 생성하고, V2X 모니터링 서버는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지함
- DID 발급 서버는 생성한 DID를 차량으로 송신하고, 노변 기지국은 차량으로부터 수신된 DID와 블록체인에 저장된 DID를 이용하여 차량을 인증함
- 차량은 그룹 서명 검증키와 DID 공개키를 이용하여 다른 차량으로부터 수신된 메시지를 검증하고 검증에 실패한 경우 노변 기지국으로 알람을 송신함

기술의 목적

IEEE 1609.2에서 제공하는 V2X 보안 표준은 PKI(Public Key Infrastructure) 기반 인증서를 통한 서명 및 암호화 방식으로 통신이 진행되므로 인증서를 관리하는 측면에서 오버헤드(overhead)가 발생하고, 주기적으로 인증서를 교체해 주어야 하는 문제점이 있음. 이에 인증서 관리의 오버헤드와 인증서 교체를 방지하면서 악의적 차량을 탐지할 수 있는 V2X 보안 기술이 요구되고 있음

해결 방안

차량의 식별 정보로부터 차량의 DID를 생성하여 블록체인에 저장하고, 노변 기지국(RSU: Road Side Unit)은 차량의 DID를 이용하여 차량을 인증하고, 인증된 차량으로 그룹 서명키와 그룹 서명 검증키를 송신함. 차량은 그룹 서명키와 DID 개인키를 이용하여 서명된 메시지를 생성하고, V2X 모니터링 서버는 차량간 메시지를 이용하여 악의적인 차량이 존재하는지 여부를 탐지함

기술의 특징점

V2X의 보안을 위해 DID를 사용함으로써 인증서 관리의 오버헤드와 인증서 교체 문제를 방지할 수 있으며, V2X 메시지 모니터링을 통해 악의적인 차량을 탐지하고 탐지 결과에 따라 V2X 통신에 사용되는 키를 교체함으로써 악의적인 차량으로 인한 보안 위협을 차단할 수 있음



기술적용 시 기업의 이점

V2X의 보안을 위해 종래 기술에서 요구되는 인증서 관리의 오버헤드와 인증서 교체 문제를 방지하면서
악의적인 차량에 의한 보안 위협을 차단이 가능하므로, 기술적 측면에서 시장 경쟁력 확보 가능함

SWOT분석 Analysis



PKI 기반 인증서를 통한 서명 및 암호화 방식을 이용하는 종래 V2X 보안 기술과 달리 인증서 관리의 오버헤드와 인증서 교체 문제를 방지할 수 있으며, 차량 사이에 교환되는 V2X 메시지를 모니터링 함으로써 악의적인 차량을 탐지할 수 있음



차량 인증을 위한 DID 저장 및 관리를 위해 블록 체인 기술의 활용을 요구하고 있으며, 이로 인해 느린 거래 처리 속도와 확장성 문제와 같은 블록체인이 가지고 있는 한계점이 상용화를 위한 제약 사항으로 작용할 가능성이 있음

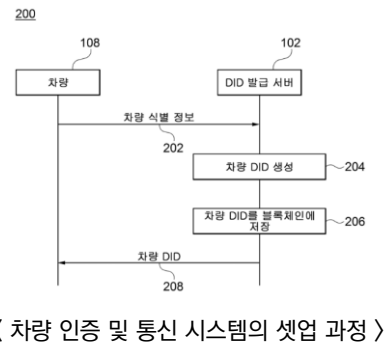
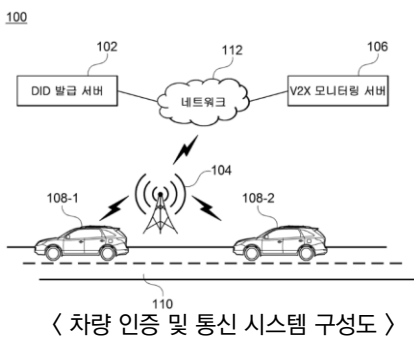


자율주행기술과 스마트 모빌리티에 대한 관심과 시장 규모가 증가하고 있으며, 세계 각국에서 V2X 보안 기술에 대한 개발 및 실증이 활발하게 이루어지고 있어 기술 수요가 꾸준히 증가할 것으로 예상됨



V2X 통신 표준 제정을 위한 경쟁이 심화되고 있으며, 표준 제정 결과에 따라 표준 합치 여부가 문제될 가능성이 있음

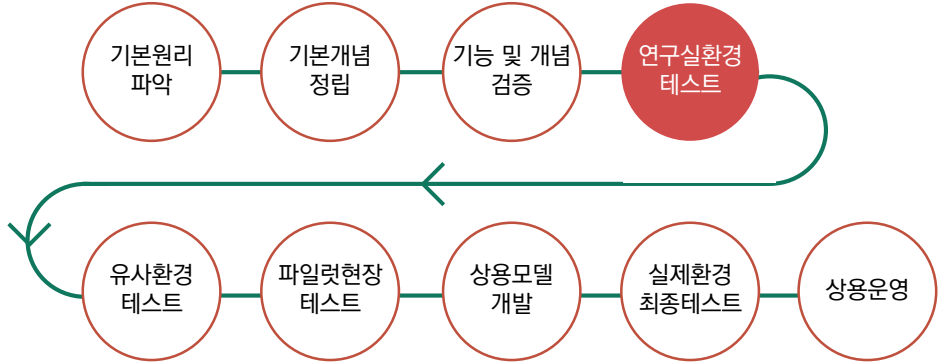
대표도면 Drawing



기술의 완성도

Technology
Readiness level

● : 현재 단계입니다.



특허현황

Patent status

발명의 명칭	출원번호	등록번호	출원국가
차량 인증 및 통신 시스템 및 방법	10-2020-0126022 (2020.09.28.)	10-2256730 (2020.05.20.)	한국

기술키워드

Keyword

한글키워드	영문키워드
블록체인, 차량, 인증, 보안, 스마트 모빌리티, 커넥티드 카	block chain, vehicle, verification, security, V2X, DID, smart mobility, connected car

발명자

Inventor Info.

교수명	신지선
소속	세종대학교 정보보호학과
연구분야	스마트 보안, 근거리 통신 및 사물지능인터넷 인증 프로토콜, 스마트카 보안 및 인증 등
E-mail	jsshin@sejong.ac.kr
웹사이트	http://home.sejong.ac.kr/~jsshin/

