(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0142893
(43) 공개일자 2024년10월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/00* (2022.01)
H04W 12/069 (2021.01)
(52) CPC특허분류
H04L 9/3271 (2013.01)
H04L 9/3236 (2013.01)
(21) 출원번호 10-2023-0037499
(22) 출원일자 2023년03월22일
심사청구일자 2023년03월22일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 1703호(송도동, 더샵센트럴파크2)
김윤아
서울특별시 서초구 방배로 21, 108동 1105호(방배동, 방배그랑자이)
허가빈
경상남도 창원시 의창구 하남천서길21번길 8-14, 1동 1107호(도계동, 강남훼미리아파트)
(74) 대리인
김연권

전체 청구항 수 : 총 10 항

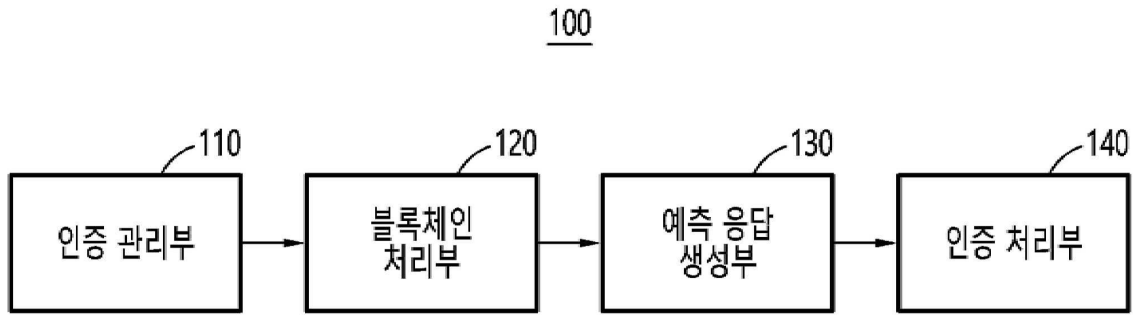
(54) 발명의 명칭 **ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치, 인증 시스템 및 인증 방법**

(57) 요 약

본 발명은 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치, 인증 시스템 및 인증 방법에 관한 것으로, 본 발명의 일실시예에 따른 노변 장치는 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 상기 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전

(뒷면에 계속)

대 표 도 - 도1



(challenge) 데이터를 전송하는 인증 관리부, 블록체인에 상기 차량과 관련하여 차량 식별자, 상기 다른 노변 장치에 대한 노변 장치 식별자 및 상기 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신하는 블록체인 처리부, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 예측 응답 생성부 및 상기 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 차량을 인증하는 인증 처리부를 포함할 수 있다.

(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/50 (2022.05)
H04W 12/069 (2021.01)
H04L 2209/84 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711191658
과제번호	2023R1A2C1005712
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	Urban computing 환경에서 UAM을 위한 지능형 통신 및 데이터 보안 기법
기 여 율	1/1
과제수행기관명	이화여자대학교
연구기간	2023.03.01 ~ 2024.02.29

명 세 서

청구범위

청구항 1

ITS(Intelligent Transport Systems) 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치에 있어서,

다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 상기 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하는 인증 관리부;

블록체인에 상기 차량과 관련하여 차량 식별자, 상기 다른 노변 장치에 대한 노변 장치 식별자 및 상기 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신하는 블록체인 처리부;

상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 예측 응답 생성부; 및

상기 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 차량을 인증하는 인증 처리부를 포함하는 것을 특징으로 하는

노변 장치.

청구항 2

제1항에 있어서,

상기 예측 응답 생성부는 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답(response) 데이터를 생성하는 것을 특징으로 하는

노변 장치.

청구항 3

제1항에 있어서,

상기 차량 식별자 및 상기 차량 인증서는 상기 차량이 상기 ITS 환경에 진입하면 차량 등록 후 상기 블록체인에 기록되고,

상기 노변 장치 식별자는 상기 차량이 상기 이전 구역으로 진입할 경우 상기 다른 노변 장치가 상기 차량을 인증한 이후 상기 블록체인에 기록되는 것을 특징으로 하는

노변 장치.

청구항 4

제1항에 있어서,

상기 블록체인 처리부는 상기 차량이 인증된 이후에 상기 현재 구역에서 인증 결과로 상기 현재 구역을 관리하는 노변 장치의 노변 장치 식별자를 상기 블록 체인에 기록하는 것을 특징으로 하는

노변 장치.

청구항 5

제1항에 있어서,

상기 인증 처리부는 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터가 매칭하는 경우에 상기 차량에 대한 인증 성공 결과를 상기 차량으로 전송하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터가

매칭되지 않는 경우에 상기 차량에 대한 인증 거부 결과를 상기 차량으로 전송하는 것을 특징으로 하는

노변 장치.

청구항 6

ITS(Intelligent Transport Systems) 환경에서 블록체인 기반 이동 차량을 인증하는 인증 방법에 있어서,

인증 관리부에서, 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 상기 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하는 단계;

블록체인 처리부에서, 블록체인에 상기 차량과 관련하여 차량 식별자, 상기 다른 노변 장치에 대한 노변 장치 식별자 및 상기 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신하는 단계;

예측 응답 생성부에서, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 단계; 및

인증 처리부에서, 상기 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 차량을 인증하는 단계를 포함하는 것을 특징으로 하는

인증 방법.

청구항 7

제6항에 있어서,

상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 단계는,

상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답(response) 데이터를 생성하는 것을 특징으로 하는

인증 방법.

청구항 8

ITS(Intelligent Transport Systems) 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템에 있어서,

복수의 노변 장치, 복수의 차량, 블록 체인 및 중앙 관리 서버를 포함하고,

상기 복수의 차량 중 어느 하나의 차량은 상기 복수의 노변 장치 중 제2 노변 장치가 관리하는 이전 구역으로부터 제1 노변 장치가 관리하는 현재 구역으로 이동하면서 상기 제1 노변 장치로 인증 요청 메시지를 전송하고,

상기 제1 노변 장치는 상기 어느 하나의 차량으로 상기 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하고, 상기 블록체인에 상기 어느 하나의 차량과 관련하여 차량 식별자, 상기 제2 노변 장치에 대한 노변 장치 식별자 및 상기 어느 하나의 차량에 대하여 상기 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신 하여 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하며,

상기 어느 하나의 차량은 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 도전 데이터에 대하여 해시 함수 값으로 응답 데이터를 생성하고,

상기 제1 노변 장치는 상기 어느 하나의 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 어느 하나의 차량을 인증하는 것을 특징으로 하는

인증 시스템.

청구항 9

제8항에 있어서,

상기 제1 노변 장치는 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답 데이터를 생성하고,

상기 어느 하나의 차량은 상기 해시 함수에 기반하여 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자, 상기 차량 인증서 및 시각 정보를 이용하여 상기 응답 데이터를 생성하는 것을 특징으로 하는

인증 시스템.

청구항 10

제8항에 있어서,

상기 차량 식별자 및 상기 차량 인증서는 상기 차량이 상기 ITS 환경에 진입하면 차량 등록 후 상기 블록체인에 기록되고,

상기 노변 장치 식별자는 상기 차량이 상기 이전 구역으로 진입할 경우 상기 제2 노변 장치가 상기 차량을 인증한 이후 상기 블록체인에 기록되는 것을 특징으로 하는

인증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치, 인증 시스템 및 인증 방법에 관한 것으로, 블록체인을 통해 ITS 환경을 구성하는 노드의 주요 인증 정보를 공유하여 개별 차량에 대한 민감한 데이터를 보호하고, 도전(challenge) 데이터와 응답(response) 데이터를 이용한 인증 방식에 해시 함수를 활용하여 신속하고 안전한 차량 인증을 수행하는 기술에 관한 것이다.

배 경 기 술

[0002] ITS(Intelligent Transportation Systems)는 교통 인프라 및 제어 시스템에 정보 통신 기술을 접목하여 교통정보의 종합적인 수집, 가공 및 전파를 통해 심각한 교통 문제에 효과적으로 대응하는 시스템이다.

[0003] ITS에서는 대량의 데이터가 실시간으로 수집 및 활용되는데, 이 과정에서 상당한 통신 비용과 계산 비용이 소모된다.

[0004] 따라서, 교통 체계의 혁신이라는 ITS의 목표를 효과적으로 달성하기 위해서는 구성 노드의 인증에 드는 비용을 절감하여 데이터 공유와 활용에 더 많은 자원을 할당하여야 한다.

[0005] 기존 이동통신 환경에서 사용되는 셀룰러 기술은 서비스 공간을 정육각형의 셀로 분할하여 각 셀의 중심에 기지국을 배치한다.

[0006] 각 셀 안에 존재하는 사용자는 해당 셀의 기지국과 통신하는데, 사용자가 하나의 셀 영역을 벗어나 인접 셀로 진입하면 통신하던 기지국이 변경되어야 한다.

[0007] 이 작업을 핸드오버라고 부르는데, 일반적인 이동통신 환경의 경우 사용자가 빠른 속도로 이동하는 상황에서 핸드오버가 지연되거나 실패하고, 핑퐁(Ping-pong) 효과가 발생하는 문제점이 있어 이동장치의 원활한 신호 수신을 방해한다.

[0008] ITS는 차량을 중심으로 교통정보를 수집하고 상호 교환하는 시스템인 만큼 고속으로 이동하는 차량에서도 이동장치가 원활한 신호 수신을 할 수 있도록 적절한 핸드오버가 보장되어야 한다.

[0009] 또한, 민감한 데이터를 실시간으로 주고받을 수 있어야 하므로 통신과 계산에 자원을 우선 배분하는 한편 차량을 인증하는 비용을 반드시 절감해야 한다.

[0010] 이러한 문제를 해결하기 위해 본 연구에서는 신속하고 안전한 노드 인증을 위해 블록체인 기술을 적용하고자 한다.

[0011] 데이터가 분산된 원장에 암호화 및 연결되어 저장된 데이터 사슬인 블록체인은 저장된 트랜잭션이 블록체인 시스템의 모든 참여자에게 투명하게 공개된다는 특징을 가진다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 한국공개특허 제10-2020-0089384호, "블록체인 기반의 교통안전정보에 응답하는 차량의 행동에 대한 보상 제공 시스템 및 방법"

(특허문헌 0002) 한국등록특허 제10-2144404호, "블록체인 기반 주행기록 데이터 저장 방법 및 이를 실행하는 시스템"

(특허문헌 0003) 한국등록특허 제10-1962425호, "무선 통신 시스템에서 차량 UE 및 RSU UE를 인증하기 위한 방법 및 장치"

발명의 내용

해결하려는 과제

[0013] 본 발명은 블록체인을 통해 ITS(Intelligent Transportation Systems) 환경을 구성하는 노드의 주요 인증 정보를 공유하여 개별 차량에 대한 민감한 데이터를 보호하고, 도전(challenge) 데이터와 응답(response) 데이터를 이용한 인증 방식에 해시 함수를 활용하여 신속하고 안전한 차량 인증을 수행하는 노변 장치, 인증 시스템 및 인증 방법을 제공하는 것을 목적으로 한다.

[0014] 본 발명은 ITS 환경에서 블록체인을 도입하여 인증에 사용되는 데이터를 공유함으로써 노변장치와 중앙 관리 서버 간에 소요되는 통신 자원을 절약하여 비용을 절감하면서 데이터의 무결성을 보장하고 접근 속도를 향상시키는 것을 목적으로 한다.

[0015] 본 발명은 해시 함수를 차량 인증에 활용하여 해시 함수가 가지는 단방향성이라는 특성에 기반하여 차량의 식별자나 인증서와 같은 민감한 데이터가 외부 공격으로부터 노출되는 것을 방지하고, 응답 데이터의 계산과 검증에 드는 시간과 비용을 줄여서 인증 과정을 간소화할 수 있다.

[0016] 본 발명은 도전 데이터와 응답 데이터에 기반한 인증 방식을 활용함에 따라 공격자가 중간에 응답 데이터를 스니핑(snipping)하더라도 이를 재사용 하는 것이 불가능하도록 하여 재전송 공격을 방지하여 안전한 인증이 이루어질 수 있도록 지원하는 것을 목적으로 한다.

과제의 해결 수단

[0017] 본 발명의 일실시예에 따른 노변 장치는 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 상기 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하는 인증 관리부, 블록체인에 상기 차량과 관련하여 차량 식별자, 상기 다른 노변 장치에 대한 노변 장치 식별자 및 상기 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신하는 블록체인 처리부, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 예측 응답 생성부 및 상기 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 차량을 인증하는 인증 처리부를 포함할 수 있다.

[0018] 상기 예측 응답 생성부는 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답(response) 데이터를 생성할 수 있다.

[0019] 상기 차량 식별자 및 상기 차량 인증서는 상기 차량이 상기 ITS 환경에 진입하면 차량 등록 후 상기 블록체인에 기록될 수 있다.

[0020] 상기 노변 장치 식별자는 상기 차량이 상기 이전 구역으로 진입할 경우 상기 다른 노변 장치가 상기 차량을 인

증한 이후 상기 블록체인에 기록될 수 있다.

[0021] 상기 블록체인 처리부는 상기 차량이 인증된 이후에 상기 현재 구역에서 인증 결과로 상기 현재 구역을 관리하는 노변 장치의 노변 장치 식별자를 상기 블록 체인에 기록할 수 있다.

[0022] 상기 인증 처리부는 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터가 매칭하는 경우에 상기 차량에 대한 인증 성공 결과를 상기 차량으로 전송하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터가 매칭되지 않는 경우에 상기 차량에 대한 인증 거부 결과를 상기 차량으로 전송할 수 있다.

[0023] 본 발명의 일실시예에 따르면 노변 장치의 인증 방법은 인증 관리부에서, 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 상기 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하는 단계, 블록체인 처리부에서, 블록체인에 상기 차량과 관련하여 차량 식별자, 상기 다른 노변 장치에 대한 노변 장치 식별자 및 상기 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신하는 단계, 예측 응답 생성부에서, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 단계 및 인증 처리부에서, 상기 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 차량을 인증하는 단계를 포함할 수 있다.

[0024] 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하는 단계는, 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답(response) 데이터를 생성할 수 있다.

[0025] 본 발명의 일실시예에 따르면 인증 시스템은 복수의 노변 장치, 복수의 차량, 블록 체인 및 중앙 관리 서버를 포함하고, 상기 복수의 차량 중 어느 하나의 차량은 상기 복수의 노변 장치 중 제2 노변 장치가 관리하는 이전 구역으로부터 제1 노변 장치가 관리하는 현재 구역으로 이동하면서 상기 제1 노변 장치로 인증 요청 메시지를 전송하고, 상기 제1 노변 장치는 상기 어느 하나의 차량으로 상기 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하고, 상기 블록체인에 상기 어느 하나의 차량과 관련하여 차량 식별자, 상기 제2 노변 장치에 대한 노변 장치 식별자 및 상기 어느 하나의 차량에 대하여 상기 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신 하여 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성하며, 상기 어느 하나의 차량은 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 도전 데이터에 대하여 해시 함수 값으로 응답 데이터를 생성하고, 상기 제1 노변 장치는 상기 어느 하나의 차량으로부터 상기 도전 데이터에 대한 응답 데이터를 수신하고, 상기 수신된 응답 데이터와 상기 생성된 예측 응답 데이터를 비교하여 상기 현재 구역에서 상기 어느 하나의 차량을 인증할 수 있다.

[0026] 상기 제1 노변 장치는 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 대하여 상기 중앙 관리 서버가 지정한 해시 함수에 기반하여 상기 해시 함수 값을 산출하고, 상기 산출된 해시 함수 값으로 상기 예측 응답 데이터를 생성하고, 상기 어느 하나의 차량은 상기 해시 함수에 기반하여 상기 도전 데이터, 상기 차량 식별자, 상기 노변 장치 식별자, 상기 차량 인증서 및 시각 정보를 이용하여 상기 응답 데이터를 생성할 수 있다.

[0027] 상기 차량 식별자 및 상기 차량 인증서는 상기 차량이 상기 ITS 환경에 진입하면 차량 등록 후 상기 블록체인에 기록되고, 상기 노변 장치 식별자는 상기 차량이 상기 이전 구역으로 진입할 경우 상기 제2 노변 장치가 상기 차량을 인증한 이후 상기 블록체인에 기록될 수 있다.

발명의 효과

[0028] 본 발명은 블록체인을 통해 ITS(Intelligent Transportation Systems) 환경을 구성하는 노드의 주요 인증 정보를 공유하여 개별 차량에 대한 민감한 데이터를 보호하고, 도전(challenge) 데이터와 응답(response) 데이터를 이용한 인증 방식에 해시 함수를 활용하여 신속하고 안전한 차량 인증을 수행하는 노변 장치, 인증 시스템 및 인증 방법을 제공할 수 있다.

[0029] 본 발명은 ITS 환경에서 블록체인을 도입하여 인증에 사용되는 데이터를 공유함으로써 노변장치와 중앙 관리 서버 간에 소요되는 통신 자원을 절약하여 비용을 절감하면서 데이터의 무결성을 보장하고 접근 속도를 향상시킬 수 있다.

[0030] 본 발명은 해시 함수를 차량 인증에 활용하여 해시 함수가 가지는 단방향성이라는 특성에 기반하여 차량의 식별자나 인증서와 같은 민감한 데이터가 외부 공격으로부터 노출되는 것을 방지하고, 응답 데이터의 계산과 검증에 드는 시간과 비용을 줄여서 인증 과정을 간소화할 수 있다.

[0031] 본 발명은 도전 데이터와 응답 데이터에 기반한 인증 방식을 활용함에 따라 공격자가 중간에 응답 데이터를 스니핑(snipping)하더라도 이를 재사용 하는 것이 불가능하도록 하여 재전송 공격을 방지하여 안전한 인증이 이루어질 수 있도록 지원할 수 있다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치를 설명하는 도면이다.

도 2는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치의 인증 방법을 설명하는 도면이다.

도 3은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템을 설명하는 도면이다.

도 4는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템의 인증 방법을 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 본 문서의 다양한 실시 예들이 첨부된 도면을 참조하여 기재된다.

[0034] 실시 예 및 이에 사용된 용어들은 본 문서에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 해당 실시 예의 다양한 변경, 균등물, 및/또는 대체물을 포함하는 것으로 이해되어야 한다.

[0035] 하기에서 다양한 실시 예들을 설명에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

[0036] 그리고 후술되는 용어들은 다양한 실시 예들에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0037] 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다.

[0038] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다.

[0039] 본 문서에서, "A 또는 B" 또는 "A 및/또는 B 중 적어도 하나" 등의 표현은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다.

[0040] "제1," "제2," "첫째," 또는 "둘째," 등의 표현들은 해당 구성요소들을, 순서 또는 중요도에 상관없이 수식할 수 있고, 한 구성요소를 다른 구성요소와 구분하기 위해 사용될 뿐 해당 구성요소들을 한정하지 않는다.

[0041] 어떤(예: 제1) 구성요소가 다른(예: 제2) 구성요소에 "(기능적으로 또는 통신적으로) 연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로 연결되거나, 다른 구성요소(예: 제3 구성요소)를 통하여 연결될 수 있다.

[0042] 본 명세서에서, "~하도록 구성된(또는 설정된)(configured to)"은 상황에 따라, 예를 들면, 하드웨어적 또는 소프트웨어적으로 "~에 적합한," "~하는 능력을 가지는," "~하도록 변경된," "~하도록 만들어진," "~를 할 수 있는," 또는 "~하도록 설계된"과 상호 호환적으로(interchangeably) 사용될 수 있다.

[0043] 어떤 상황에서는, "~하도록 구성된 장치"라는 표현은, 그 장치가 다른 장치 또는 부품들과 함께 "~할 수 있는" 것을 의미할 수 있다.

[0044] 예를 들면, 문구 "A, B, 및 C를 수행하도록 구성된(또는 설정된) 프로세서"는 해당 동작을 수행하기 위한 전용 프로세서(예: 임베디드 프로세서), 또는 메모리 장치에 저장된 하나 이상의 소프트웨어 프로그램들을 실행함으로써, 해당 동작들을 수행할 수 있는 범용 프로세서(예: CPU 또는 application processor)를 의미할 수 있다.

[0045] 또한, '또는' 이라는 용어는 배타적 논리합 'exclusive or' 이기보다는 포함적인 논리합 'inclusive or' 를 의미한다.

[0046] 즉, 달리 언급되지 않는 한 또는 문맥으로부터 명확하지 않는 한, 'x가 a 또는 b를 이용한다' 라는 표현은 포함적인 자연 순열들(natural inclusive permutations) 중 어느 하나를 의미한다.

[0047] 이하 사용되는 '..부', '..기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0049] 도 1은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치를 설명하는 도면이다.

[0050] 도 1은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치의 구성 요소를 예시한다.

[0051] 도 1을 참고하면, 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치(100)는 인증 관리부(110), 블록체인 처리부(120), 예측 응답 생성부(130) 및 인증 처리부(140)를 포함한다.

[0052] 본 발명의 일실시예에 따르면 인증 관리부는 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신한다.

[0053] 또한, 인증 관리부(110)는 차량으로 상기 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송한다.

[0054] 예를 들어, 차량은 ITS 환경을 구성하는 중앙 관리 서버와 복수의 노변 장치에서 노변 장치들 각각이 관리하는 구역 간을 이동하는 노드일 수 있다.

[0055] ITS 환경은 전체를 통합 관리하는 중앙 관리 서버가 복수의 노변 장치와 함께 블록 체인을 구축한다.

[0056] 차량은 ITS 환경에 최초로 진입할 때 중앙 관리 서버에 신원을 제출하고 등록 후 인증서를 발급받는 과정을 거친다.

[0057] ITS 환경에서 모든 서비스 공간은 구역 단위로 분할되며 각 구역은 단일 노변 장치에 의해 관리된다.

[0058] 노변 장치(100)는 차량과의 통신을 통해 인증을 담당하며 인증이 끝나면 해당 정보가 담긴 트랜잭션을 발행한다.

[0059] 트랜잭션은 블록 체인상에 기록되어 ITS 환경 내의 모든 참여자에게 공유된다.

[0060] 이에 따라, 노변 장치(100)는 특정 차량이 어떤 구역을 거쳐서 진입하였는지 파악할 수 있다.

[0061] 노변 장치(100)가 차량의 인증을 완료하면 해당 노변 장치(100)의 식별자가 블록체인에 기록된다.

[0062] 이후 해당 차량이 새로운 구역으로 이동하여 재인증을 받을 때, 직전 구역에서 인증을 수행한 주체인 노변 장치의 식별자는 응답 계산을 위한 일력 값 중 어느 하나로서 활용될 수 있다.

[0063] 본 발명의 일실시예에 따르면 블록체인 처리부(120)는 블록체인에 차량과 관련하여 차량 식별자, 다른 노변 장치에 대한 노변 장치 식별자 및 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신한다.

[0064] 예를 들어, 차량 식별자 및 차량 인증서는 중앙 관리 서버에 의해 차량이 ITS 환경에 진입하면 차량 등록 후 블록체인에 기록된다.

[0065] 노변 장치 식별자는 차량이 이전 구역으로 진입할 경우 다른 노변 장치가 차량을 인증한 이후 블록체인에 기록된다.

[0066] 즉, 이전 구역을 관리하는 다른 노변 장치는 차량이 이전 구역에 진입 시 인증하고, 인증이 완료되면 차량과 관련하여 블록 체인에 노변 장치 식별자를 등록한다.

[0067] 일례로, 블록체인 처리부(120)는 차량이 인증된 이후에 현재 구역에서 인증 결과로 현재 구역을 관리하는 노변 장치(100)의 노변 장치 식별자를 블록 체인에 기록할 수 있다.

[0068] 본 발명의 일실시예에 따르면 예측 응답 생성부(130)는 차량 식별자, 노변 장치 식별자 및 차량 인증서에 기반

하여 해시 함수 값으로 예측 응답(response) 데이터를 생성할 수 있다.

[0069] 일례로, 예측 응답 생성부(130)는 도전 데이터, 차량 식별자, 노변 장치 식별자 및 차량 인증서에 대하여 중앙 관리 서버가 지정한 해시 함수에 기반하여 해시 함수 값을 산출하고, 산출된 해시 함수 값으로 예측 응답(response) 데이터를 생성할 수 있다.

[0070] 본 발명의 일실시예에 따르면 인증 처리부(140)는 차량으로부터 도전 데이터에 대한 응답 데이터를 수신하고, 수신된 응답 데이터와 생성된 예측 응답 데이터를 비교하여 현재 구역에서 차량을 인증할 수 있다.

[0071] 일례로, 인증 처리부(140)는 차량으로부터 수신된 응답 데이터와 기 생성한 예측 응답 데이터가 동일한 것으로 매칭하는 경우에 차량에 대한 인증 성공 결과를 차량으로 전송한다.

[0072] 본 발명의 일실시예에 따르면, 인증 처리부(140)는 응답 데이터와 예측 응답 데이터가 매칭되지 않는 경우에 차량에 대한 인증 거부 결과를 차량으로 전송한다.

[0073] 노변 장치(100)는 해시 함수가 가지는 단방향성을 통해 민감한 데이터의 노출을 막고 계산과 검증 과정을 경량화한다.

[0074] 또한, 노변 장치(100)가 전송한 도전 데이터에 대해 인증 대상이 올바른 응답 데이터를 제시함으로써 인증을 승인받게 되는 방식으로 도전 데이터와 응답 데이터를 활용한 매커니즘을 통해 인증 과정에서 통신 속도와 비용을 개선하고 보안성을 강화한다.

[0075] 도전(challenge)과 응답(response) 방식을 사용하면 사용자 토큰과 클록(clock) 및 카운터(counter)와 같은 동기 유지할 필요가 없음에 빠른 인증을 진행할 수 있다는 장점이 있다.

[0076] 또한, 인증에 상용되는 도전 및 응답은 일회성으로 사용되는 값으로 발급 시점에서만 유효하기 때문에 공격자가 이러한 인증 정보를 탈취하더라도 이를 재사용하는 것이 불가능하여 재전송 공격이 불가함에 정보 유실에 따른 2차 피해를 방지할 수 있다.

[0077] 따라서, 본 발명은 블록체인을 통해 ITS(Intelligent Transportation Systems) 환경을 구성하는 노드의 주요 인증 정보를 공유하여 개별 차량에 대한 민감한 데이터를 보호하고, 도전(challenge) 데이터와 응답(response) 데이터를 이용한 인증 방식에 해시 함수를 활용하여 신속하고 안전한 차량 인증을 수행하는 노변 장치, 인증 시스템 및 인증 방법을 제공할 수 있다.

[0079] 도 2는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치의 인증 방법을 설명하는 도면이다.

[0080] 도 2는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 노변 장치의 인증 방법을 예시한다.

[0081] 도 2를 참고하면, 단계(S201)에서 본 발명의 일실시예에 따른 인증 방법은 인증 요청 메시지를 수신하여 도전 데이터를 전송한다.

[0082] 즉, 본 발명의 일실시예에 따른 인증 방법은 다른 노변 장치가 관리하는 이전 구역으로부터 현재 구역으로 이동하는 차량으로부터 인증 요청 메시지를 수신하고, 차량으로 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송한다.

[0083] 단계(S202)에서 본 발명의 일실시예에 따른 인증 방법은 블록 체인에 예측 응답을 위한 인증 정보를 요청한다.

[0084] 즉, 본 발명의 일실시예에 따른 인증 방법은 블록체인에 차량을 인증하기 위한 인증 정보로서, 차량과 관련하여 차량 식별자, 다른 노변 장치에 대한 노변 장치 식별자 및 차량에 대하여 중앙 관리서버가 부여한 차량 인증서를 요청하여 수신한다.

[0085] 단계(S203)에서 본 발명의 일실시예에 따른 인증 방법은 해시 함수 값으로 예측 응답 데이터를 생성한다..

[0086] 즉, 본 발명의 일실시예에 따르면 인증 방법은 차량 식별자, 상기 노변 장치 식별자 및 상기 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성한다.

[0087] 단계(S204)에서 본 발명의 일실시예에 따른 인증 방법은 도전 데이터에 대한 응답 데이터를 수신하고, 응답 데이터와 예측 응답 데이터를 비교하여 현재 구역에서 차량을 인증한다.

[0088] 즉, 본 발명의 일실시예에 따르면 인증 방법은 차량으로부터 도전 데이터에 대한 응답 데이터를 수신하고, 응답 데이터와 예측 응답 데이터를 비교하여 현재 구역에서 차량을 인증한다.

[0089] 따라서, 본 발명은 ITS 환경에서 블록체인을 도입하여 인증에 사용되는 데이터를 공유함으로써 노변장치와 중앙 관리 서버 간에 소요되는 통신 자원을 절약하여 비용을 절감하면서 데이터의 무결성을 보장하고 접근 속도를 향상시킬 수 있다.

[0091] 도 3은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템을 설명하는 도면이다.

[0092] 도 3은 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템의 구성 요소를 예시한다.

[0093] 도 3을 참고하면, 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템(300)은 중앙 관리 서버(310), 복수의 노변 장치(road side unit, RSU), 복수의 차량, 블록 체인(340)을 포함한다.

[0094] 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템(300)은 복수의 노변 장치 중 제1 노변 장치(320)와 제2 노변 장치(321) 사이에서 이동하는 복수의 차량 중 어느 하나의 차량(330)에 대한 인증 과정을 수행한다.

[0095] 인증 시스템(300)은 ITS 환경에 기반하고, 블록체인 시스템을 도입하여 민감한 데이터에 대한 무결성과 기밀성 그리고 가용성을 보장한다.

[0096] 인증 시스템(300)은 노드의 인증 과정에서 사용되는 정보가 블록체인(340) 상에 안전하게 저장된다.

[0097] 트랜잭션은 차량의 식별자, 해당 차량을 인증한 노변 장치의 식별자, 차량의 인증서 및 인증이 성사되는 시각 정보로 구성될 수 있다.

[0098] 중앙 관리 서버(310)는 ITS 전체를 통합 관리하는 것으로 온전히 신뢰할 수 있고, ITS가 처음 구축될 때 시스템을 초기화하며 중앙 관리 서버(310)와 복수의 노변 장치가 참여하는 블록체인(340)을 구축한다.

[0099] 중앙 관리 서버(310)는 새로운 차량을 시스템에 등록하고, 인증서를 발급하여 블록체인(340)을 기록한다.

[0100] 모든 차량은 ITS에 최초로 진입할 시 중앙 관리 서버(310)에 신원을 제출하고 등록 후 인증서를 발급받는 과정을 수행한다.

[0101] ITS의 모든 서비스 공간은 구역 단위로 분할되며 각 구역은 단일 노변 장치에 의해 관리된다.

[0102] 노변 장치는 차량과의 통신을 통해 인증을 담당하여 인증이 끝나면 해당 정보가 담긴 트랜잭션을 발행한다.

[0103] 이때, 블록체인 상에 저장된 인증 정보는 ITS 환경 내의 모든 참여자에게 공유되므로 노변 장치는 특정 차량이 어떤 구역을 거쳐서 진입하였는지 파악할 수 있다.

[0104] 노변 장치가 차량의 인증을 완료하면 해당 노변 장치의 식별자가 블록체인에 기록된다.

[0105] 이후 해당 차량이 새로운 구역으로 이동하여 재인증을 받을 때, 직전 구역에서 인증을 수행한 주체인 노변 장치의 식별자는 응답 계산을 위해 입력값 중 일부로 사용한다.

[0106] 복수의 차량 중 어느 하나의 차량(330)은 복수의 노변 장치 중 제2 노변 장치(321)가 관리하는 이전 구역으로부터 제1 노변 장치(320)가 관리하는 현재 구역으로 이동하면서 제1 노변 장치(320)로 인증 요청 메시지를 전송한다. 예를 들어, 이전 구역은 제2 구역으로 지칭될 수 있고, 현재 구역은 제1 구역으로 지칭될 수 있다.

[0107] 제1 노변 장치(320)는 어느 하나의 차량으로 수신된 인증 요청 메시지에 대응하는 도전(challenge) 데이터를 전송하고, 블록체인에 어느 하나의 차량과 관련하여 차량 식별자, 제2 노변 장치(321)에 대한 노변 장치 식별자 및 어느 하나의 차량(330)에 대하여 중앙 관리 서버(310)가 부여한 차량 인증서를 요청하여 수신 하여 차량 식별자, 노변 장치 식별자 및 차량 인증서에 기반하여 해시 함수 값으로 예측 응답(response) 데이터를 생성한다.

[0108] 어느 하나의 차량(330)은 중앙 관리 서버(310)가 지정한 해시 함수에 기반하여 도전 데이터에 대하여 해시 함수 값으로 응답 데이터를 생성한다.

[0109] 제1 노변 장치(320)는 어느 하나의 차량으로부터 도전 데이터에 대한 응답 데이터를 수신하고, 수신된 응답 데이터와 생성된 예측 응답 데이터를 비교하여 현재 구역에서 어느 하나의 차량(330)을 인증한다.

[0110] 제1 노변 장치(320)는 도전 데이터, 차량 식별자, 노변 장치 식별자 및 차량 인증서에 대하여 중앙 관리 서버(310)가 지정한 해시 함수에 기반하여 해시 함수 값을 산출하고, 산출된 해시 함수 값으로 예측 응답 데이터를 생성한다.

[0111] 어느 하나의 차량(330)은 해시 함수에 기반하여 도전 데이터, 차량 식별자, 노변 장치 식별자, 차량 인증서 및 시각 정보를 이용하여 응답 데이터를 생성한다.

[0112] 인증 시스템(300)은 제2 노변 장치(321)의 관리 구역인 제2 구역에서 제1 노변 장치(320)의 관리 구역인 제1 구역으로 이동한 차량이 제1 노변 장치에 의해 새롭게 인증받는 과정은 도 4를 이용하여 보충 설명한다.

[0113] 인증 시스템(300)에서는 ITS의 중앙 관리 주체이자 신뢰 기관인 중앙 관리 서버와 차량의 인증을 담당하는 노변 장치가 블록체인을 통해 노드의 주요 인증 정보를 공유한다.

[0114] 노변 장치는 인증 과정에서 차량에게 도전(Challenge) 데이터를 전송하고, 차량은 이를 적절히 활용하여 해시 함수 계산 값인 응답(Response) 데이터를 도출한 뒤 노변 장치에게 제출한다.

[0115] 이후, RSU는 스스로 계산한 해시값과 차량으로부터 수신한 응답(Response) 데이터를 비교하여 인증 여부를 결정한다.

[0116] 따라서, 본 발명은 해시 함수를 차량 인증에 활용하여 해시 함수가 가지는 단방향성이라는 특성에 기반하여 차량의 식별자나 인증서와 같은 민감한 데이터가 외부 공격으로부터 노출되는 것을 방지하고, 응답 데이터의 계산과 검증에 드는 시간과 비용을 줄여서 인증 과정을 간소화할 수 있다.

[0118] 도 4는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템의 인증 방법을 설명하는 도면이다.

[0119] 도 4는 본 발명의 일실시예에 따른 ITS 환경에서 블록체인 기반 이동 차량을 인증하는 인증 시스템의 인증 방법으로서 인증 과정을 예시한다.

[0120] 도 4를 참고하면, 본 발명의 일실시예에 따른 인증 시스템의 인증 방법은 차량(400), 노변 장치(410), 블록 체인(420) 및 중앙 관리 서버(430)로 구성된 인증 시스템의 동작 방법일 수 있다.

[0121] 단계(S401)에서 차량(400)은 신원 제출하고, 단계(S402)에서 중앙 관리 서버(430)는 차량 등록하고, 단계(S403)에서 중앙 관리 서버(430)는 차량 인증서를 저장하며, 단계(S404)에서 중앙 관리 서버(430)는 차량 등록 결과를 전송한다.

[0122] 단계(S405)에서 차량(400)은 인증 요청 메시지를 전송하고, 단계(S406)에서 노변 장치(410)는 인증 요청 메시지 검증하고, 단계(S407)에서 노변 장치(410)는 도전 데이터를 전송 하며, 단계(S408)에서 노변 장치(410)는 블록체인(420)으로 예측 응답을 위한 인증 정보를 요청한다.

[0123] 단계(S409)에서 차량(400)은 응답 데이터를 생성하고, 단계(S410)에서 노변 장치(410)는 블록 체인(420)으로부터 인증 정보를 수신한다.

[0124] 단계(S411)에서 노변 장치(410)는 예측 응답 데이터를 생성하고, 단계(S412)에서 차량(400)은 노변 장치(410)로 응답 데이터를 전송한다.

[0125] 단계(S413)에서 노변 장치(410)는 응답 데이터와 예측 응답 데이터를 비교한다.

[0126] 단계(S414)에서 노변 장치(410)는 인증 결과를 차량(400)으로 전달하고, 단계(S415)에서 노변 장치 식별자를 저장한다.

[0127] 차량(400)은 노변 장치(410)에 인증 요청 메시지를 전송하고, 노변 장치(410)는 이를 수신하여 검증하며, 차량(400)에게 도전 데이터를 보낸다.

[0128] 차량(400)은 도전 데이터에 대한 응답 데이터를 계산하여 노변 장치(410)에 전송한다.

[0129] 응답 데이터는 하기 수학식 1에 기반한다.

[0131] [수학식 1]

[0132] $$R = H(Challenge||ID_V||ID_RSU2||time||CERT_V)$$

[0134] 수학식 1에서, R은 응답 데이터를 나타낼 수 있고, H는 중앙 관리 서버(430)가 지정한 해시함수를 나타낼 수 있으며, Id_V는 차량의 식별자(ID)를 나타낼 수 있고, ID_RSU2는 차량의 출발지에서 차량을 인증해준 제2 노변 장치의 식별자를 나타낼 수 있고, time은 현재 시각을 나타낼 수 있으며, CERT_V는 중앙 관리 서버(430)가 차량에 부여한 인증서일 수 있다.

[0135] 예를 들어, 기존 인증 이력이 없는 차량인 경우에는 직전에 자신을 인증해준 노변 장치(410)의 식별자를 중앙 관리 서버(430)의 식별자로 대체하여 계산이 수행될 수 있다.

[0136] 노변 장치(410)가 블록 체인(420)에 예측 응답을 위한 인증 정보로서 Id_V, ID_RSU2, CERT_V를 쿼리하고, 쿼리 결과를 바탕으로 예측 응답 데이터(R') 값의 계산을 수행한다.

[0137] 노변 장치(410)가 스스로 계산한 결과와 차량(400)으로부터 수신한 응답 값을 비교하여 차량(400)의 인증 여부를 결정한다.

[0138] 노변 장치(410)가 차량(400)에 인증 성공 또는 거부 결과를 전송하고, 인증이 정상적으로 이루어졌을 경우 블록 체인에 해당 정보를 담은 트랜잭션을 올린다.

[0139] 본 발명의 일실시예에 따른 인증 시스템의 인증 방법은 신속하고 안전한 인증 절차를 거친 각 노드가 ITS에서 수집한 정보를 상호 교환하고 재가공하여 교통의 질을 높일 수 있다.

[0140] 인증 방법은 블록체인을 통해 개별 차량에 대한 민감한 데이터를 보호할 수 있으며, Challenge-Response 인증 방식의 장점인 빠른 인증 속도와 보안성 증대, 통신 비용 절감을 보장한다.

[0141] 또한, Response 계산 시 해시 함수를 사용함으로써 계산 비용을 낮추고 개별 데이터의 무결성과 기밀성을 보장하여 신속하고 안전한 인증이 가능하도록 하였다.

[0142] 따라서, 본 발명은 도전 데이터와 응답 데이터에 기반한 인증 방식을 활용함에 따라 공격자가 중간에 응답 데이터를 스니핑(snipping)하더라도 이를 재사용 하는 것이 불가능하도록 하여 재전송 공격을 방지하여 안전한 인증이 이루어질 수 있도록 지원할 수 있다.

[0144] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0145] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상

장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0146] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0147] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

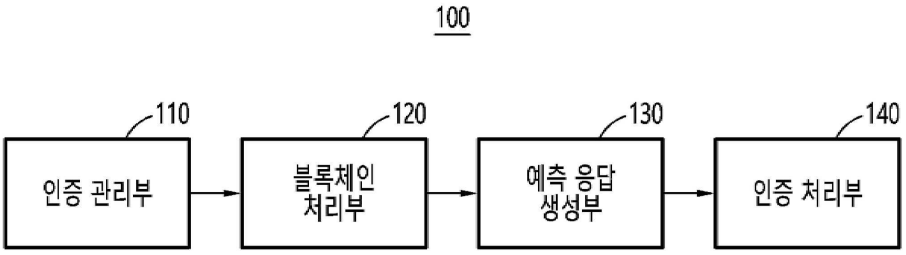
[0148] 100: 노변 장치

110: 인증 관리부 120: 블록체인 처리부

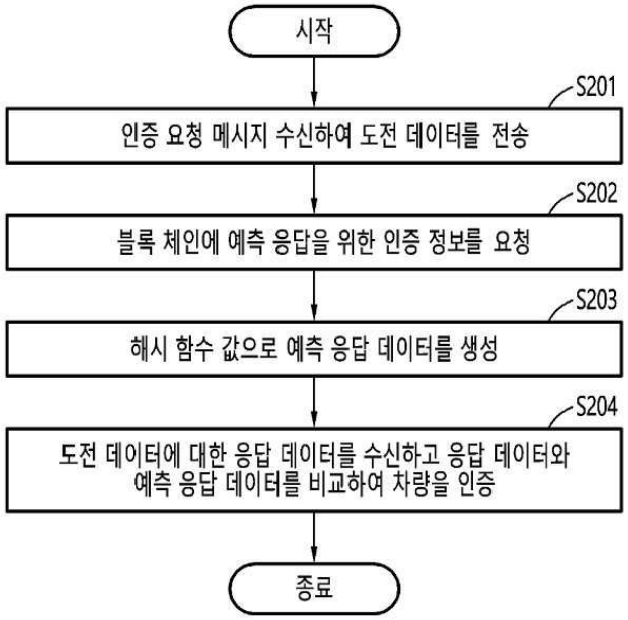
130: 예측 응답 생성부 140: 인증 처리부

도면

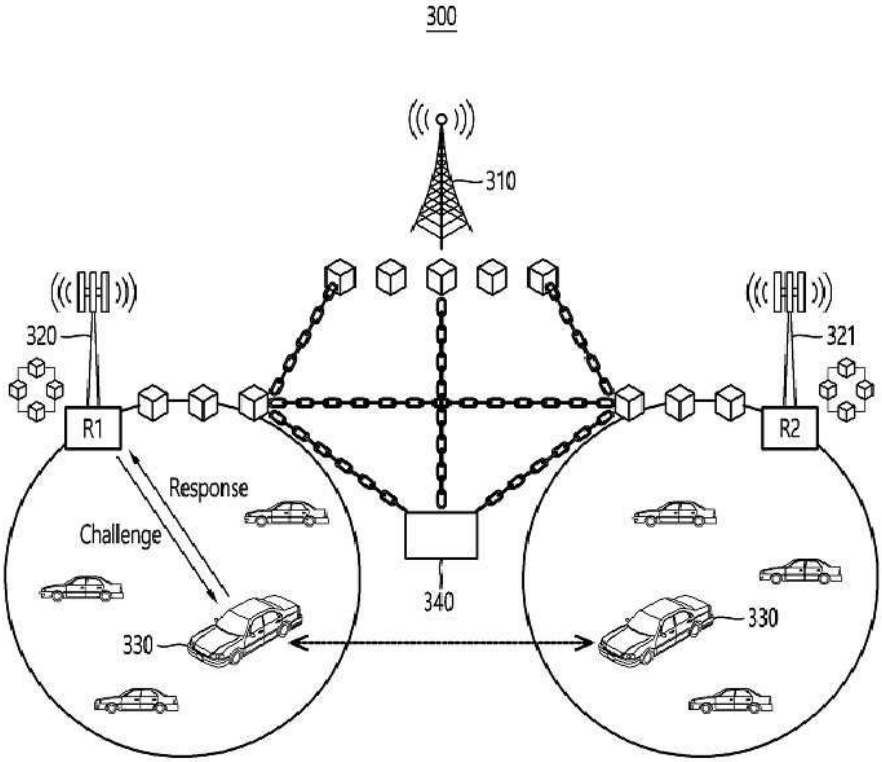
도면1



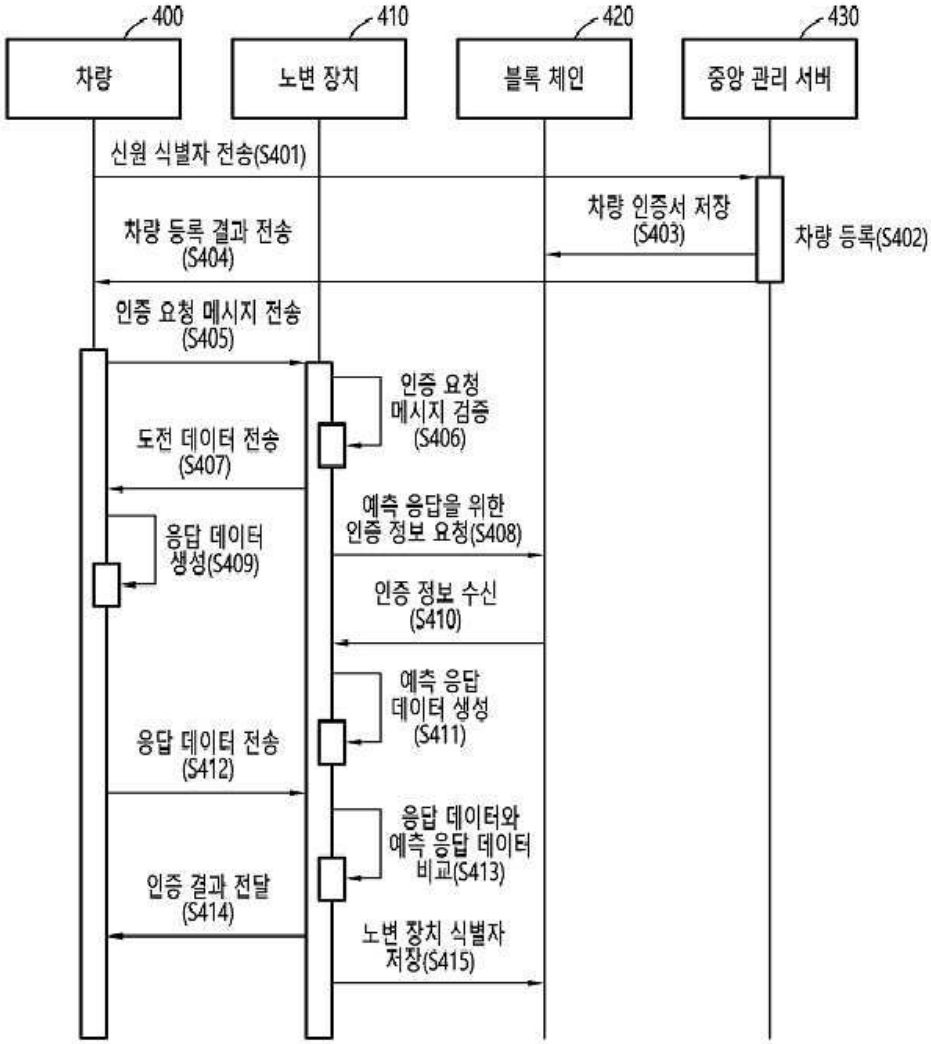
도면2



도면3



도면4


400
410
420
430
차량
노변 장치
블록 체인
중앙 관리 서버
신원 식별자 전송(S401)
차량 인증서 저장
(S403)
차량 등록(S402)
차량 등록 결과 전송
(S404)
인증 요청 메시지 전송
(S405)
인증 요청
메시지 검증
(S406)
도전 데이터 전송
(S407)
예측 응답을 위한
인증 정보 요청(S408)
응답 데이터
생성(S409)
인증 정보 수신
(S410)
예측 응답
데이터 생성
(S411)
응답 데이터 전송
(S412)
응답 데이터와
예측 응답 데이터
비교(S413)
인증 결과 전달
(S414)
노변 장치 식별자
저장(S415)