(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0105083
(43) 공개일자 2024년07월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 4/44* (2018.01)
(52) CPC특허분류
H04L 9/3242 (2013.01)
H04L 9/3297 (2013.01)
(21) 출원번호 10-2022-0187933
(22) 출원일자 2022년12월28일
심사청구일자 2022년12월28일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웰카운티2단지)
(74) 대리인
특허법인충정

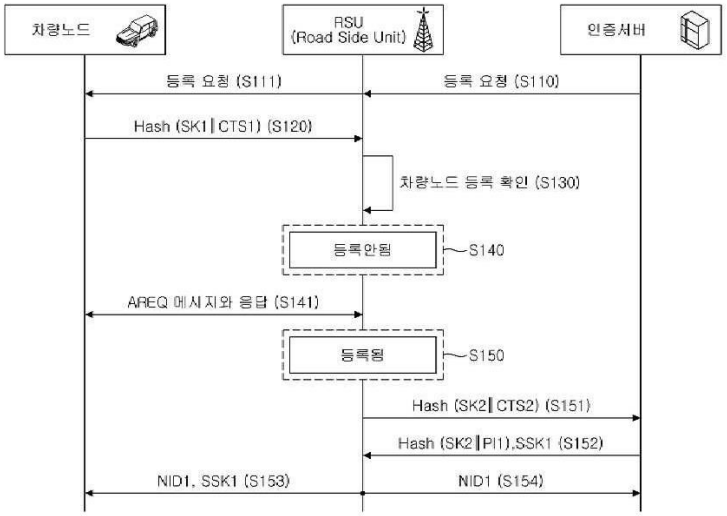
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **지능형 교통 시스템**

(57) 요 약

본 발명은 지능형 교통 시스템의 안전한 통신을 위한 인증 방법에 관한 것으로서, 본 발명의 지능형 교통 시스템에서의 인증 방법은, 지능형 교통 시스템(ITS)이 운용되는 네트워크에서 지상의 차량 또는 드론 등 무인 항공기와 같은 무선 이동 노드들에 대한 효과적인 인증이 이루어져 안전한 통신이 가능하다. 따라서, 무선 이동 노드들은 무차별 공격, 중간자 공격, 재생 공격, 가장 공격, 메시지 조작 공격 등을 시도하는 공격자로부터 안전하게 데이터를 주고받을 수 있으며 무선 이동 노드들의 높은 이동성을 보장할 수 있다.

대 표 도



(52) CPC특허분류
H04W 4/44 (2020.05)
H04L 2209/80 (2013.01)

명 세 서

청구범위

청구항 1

무선으로 연결되는 무선 이동 노드들을 포함하는 지능형 교통 시스템에서의 노드들 간의 통신을 위한 세션의 설정을 위한 인증 방법에 있어서,

(A) RSU의 커버리지에 진입하는 무선 이동 노드에서, 제1 비밀키와 제1 현재 타임 스탬프로 생성한 제1 해시 인증 데이터 및 상기 제1 현재 타임 스탬프를 상기 RSU로 전송하는 단계;

(B) 상기 제1 비밀키를 미리 유지하고 있는 상기 RSU에서, 등록이 확인된 상기 무선 이동 노드에 대하여, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프를 이용해 상기 제1 해시 인증 데이터를 인증한 후, 상기 제1 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키와 제2 현재 타임 스탬프로 생성한 제2 해시 인증 데이터 및 상기 제2 현재 타임 스탬프를 네트워크 상의 인증 서버로 전송하는 단계;

(C) 상기 인증 서버에서, 등록이 확인된 상기 RSU에 대하여, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 상기 제2 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 상기 제2 비밀키와 슈도 식별자로 생성한 제3 해시 인증 데이터 및 상기 슈도 식별자를 세션키와 함께 상기 RSU로 회신하는 단계; 및

(D) 상기 RSU에서, 상기 제2 비밀키와 상기 슈도 식별자를 이용해 상기 제3 해시 인증 데이터를 인증한 후, 상기 슈도 식별자와 상기 RSU의 식별자를 합성한 뉴 식별자를 생성하여, 상기 무선 이동 노드 및 상기 인증 서버로 통보함으로써, 상기 무선 이동 노드, 상기 RSU, 및 상기 인증 서버 간에 통신을 위한 세션이 설정되는 단계

를 포함하는 인증 방법.

청구항 2

제1항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드로서 차량 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행하기 위한 인증 방법.

청구항 3

제1항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드로서 무인 항공기 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행하기 위한 인증 방법.

청구항 4

제1항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드는 차량 노드들 및 무인 항공기 노드들을 포함하고,

상기 RSU는 상기 통신을 위해 상기 차량 노드들 사이, 상기 무인 항공기 노드들 사이, 및 상기 차량 노드와 상기 무인 항공기 노드 사이의 신호 중계를 수행하는 인증 방법.

청구항 5

제1항에 있어서,

(A) 단계 전에,

상기 인증 서버에서, 복수의 상기 RSU 및 복수의 상기 무선 이동 노드에 대한 식별자들을 데이터베이스에 유지하고,

복수의 상기 RSU로 상기 무선 이동 노드에 대한 식별자들을 전송해 등록하도록 제어하고, 복수의 상기 RSU 각각

이 커버리지 내의 하나 이상의 상기 무선 이동 노드로 자신의 식별자를 전송해 등록하도록 제어함으로써, 상기 세션 설정을 위한 (A), (B), (C), (D) 각 단계의 수행을 위해, 상기 인증 서버, 상기 RSU 및 상기 무선 이동 노드 간의 메시지 송수신에서, 송신 노드는 상대방 노드로 자신의 식별자를 포함하는 메시지를 전송해 해당 반응이 이루어지도록 하는 인증 방법.

청구항 6

제1항에 있어서,

(B) 단계에서, 상기 제1 해시 인증 데이터의 인증에서, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프에 대하여, (A) 단계에서 상기 무선 이동 노드가 상기 제1 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 무선 이동 노드로부터 수신한 상기 제1 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 인증 방법.

청구항 7

제1항에 있어서,

(C) 단계에서, 상기 제2 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프에 대하여, (B) 단계에서 상기 RSU가 상기 제2 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 RSU로부터 수신한 상기 제2 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 인증 방법.

청구항 8

제1항에 있어서,

(D) 단계에서, 상기 제3 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 슈도 식별자에 대하여, (C) 단계에서 상기 인증 서버가 상기 제3 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 인증 서버로부터 수신한 상기 제3 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 인증 방법.

청구항 9

무선으로 연결되는 무선 이동 노드들을 포함하는 지능형 교통 시스템에서의 노드들 간의 통신을 위한 세션의 설정을 위한 인증 기능을 구현하기 위한 컴퓨터에 의해 판독 가능한 기록매체에 있어서,

(A) RSU의 커버리지에 진입하는 무선 이동 노드에서, 제1 비밀키와 제1 현재 타임 스탬프로 생성한 제1 해시 인증 데이터 및 상기 제1 현재 타임 스탬프를 상기 RSU로 전송하는 기능;

(B) 상기 제1 비밀키를 미리 유지하고 있는 상기 RSU에서, 등록이 확인된 상기 무선 이동 노드에 대하여, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프를 이용해 상기 제1 해시 인증 데이터를 인증한 후, 상기 제1 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키와 제2 현재 타임 스탬프로 생성한 제2 해시 인증 데이터 및 상기 제2 현재 타임 스탬프를 네트워크 상의 인증 서버로 전송하는 기능;

(C) 상기 제2 비밀키를 미리 유지하고 있는 상기 인증 서버에서, 등록이 확인된 상기 RSU에 대하여, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 상기 제2 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 상기 제2 비밀키와 슈도 식별자로 생성한 제3 해시 인증 데이터 및 상기 슈도 식별자를 세션키와 함께 상기 RSU로 회신하는 기능; 및

(D) 상기 RSU에서, 상기 제2 비밀키와 상기 슈도 식별자를 이용해 상기 제3 해시 인증 데이터를 인증한 후, 상기 슈도 식별자와 상기 RSU의 식별자를 합성한 뉴 식별자를 생성하여, 상기 무선 이동 노드 및 상기 인증 서버로 통보함으로써, 상기 무선 이동 노드, 상기 RSU, 및 상기 인증 서버 간에 통신을 위한 세션이 설정되는 기능

을 수행하는 기록 매체.

청구항 10

제9항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드로서 차량 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행하기 위한 기록 매체.

청구항 11

제9항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드로서 무인 항공기 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행하기 위한 기록 매체.

청구항 12

제9항에 있어서,

상기 세션이 설정된 복수의 상기 무선 이동 노드는 차량 노드들 및 무인 항공기 노드들을 포함하고,

상기 RSU는 상기 통신을 위해 상기 차량 노드들 사이, 상기 무인 항공기 노드들 사이, 및 상기 차량 노드와 상기 무인 항공기 노드 사이의 신호 중계를 수행하는 기록 매체.

청구항 13

제9항에 있어서,

(A) 기능 전에,

상기 인증 서버에서, 복수의 상기 RSU 및 복수의 상기 무선 이동 노드에 대한 식별자들을 데이터베이스에 유지하고,

복수의 상기 RSU로 상기 무선 이동 노드에 대한 식별자들을 전송해 등록하도록 제어하고, 복수의 상기 RSU 각각이 커버리지 내의 하나 이상의 상기 무선 이동 노드로 자신의 식별자를 전송해 등록하도록 제어함으로써, 상기 세션 설정을 위한 (A), (B), (C), (D) 각 기능의 수행을 위해, 상기 인증 서버, 상기 RSU 및 상기 무선 이동 노드 간의 메시지 송수신에서, 송신 노드는 상대방 노드로 자신의 식별자를 포함하는 메시지를 전송해 해당 반응이 이루어지도록 하는 기록 매체.

청구항 14

제9항에 있어서,

(B) 기능에서, 상기 제1 해시 인증 데이터의 인증에서, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프에 대하여, (A) 기능에서 상기 무선 이동 노드가 상기 제1 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 무선 이동 노드로부터 수신한 상기 제1 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 기록 매체.

청구항 15

제9항에 있어서,

(C) 기능에서, 상기 제2 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프에 대하여, (B) 기능에서 상기 RSU가 상기 제2 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 RSU로부터 수신한 상기 제2 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 기록 매체.

청구항 16

제9항에 있어서,

(D) 기능에서, 상기 제3 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 슈도 식별자에 대하여, (C) 기능에서 상기 인증 서버가 상기 제3 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 인증 서버로부터 수신한 상기 제3 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것인 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 지능형 교통 시스템(ITS)에 관한 것으로서, 특히, 차량 또는 무인 항공기와 같은 무선 이동 노드의 안전한 통신을 위한 인증 방법을 적용한 지능형 교통 시스템에 관한 것이다.

배 경 기 술

[0002] 지능형 교통 시스템(ITS)은 고도화되고 빠른 통신 서비스로 인해 인기를 얻고 있다. 지난 수십 년 동안 자동차 산업은 보다 실현 가능하고 효율적인 차량 품질을 개발하기 위해 다른 부문과 지속적으로 협력해 왔다. 차량 인터넷(IoV)은 차량 노드가 서로 연결되어 네트워크를 형성하는 지능형 교통 시스템(ITS)의 하위 클래스 중 하나이다. 스마트 시티 시스템의 급속한 발전은 차량 인터넷(IoV)의 발전을 촉진해 왔다. 오늘날 많은 차량 애플리케이션이 모바일 로봇 및 자율 주행에 적용되고 있다. 그러나 이러한 유형의 서비스에는 많은 복잡한 데이터 처리 및 연산이 필요하다. 차량 노드는 클라우드 컴퓨팅 센터에서 해당 컴퓨팅 리소스를 확보하여 환경 인식 및 주행 협력 등 첨단 응용 서비스를 구현하고 차량 탑재 클라우드 컴퓨팅 VCC (Vehicular Cloud Computing)를 구성할 수 있다. 그러나 많은 컴퓨팅 작업과 빈번한 데이터 전송으로 인해 클라우드 장치가 과부하되어 제 시간에 계산을 완료할 수 없게 될 수 있다.

[0003] 스마트 시티 구축을 위한 이와 같은 지능형 교통 시스템(ITS)이 운용되는 네트워크는 특히 도시의 혼잡한 지역에서 약간의 혼잡, 라우팅 및 보안 문제로 어려움을 겪고 있으며 지연 및 계산 복잡성 문제로 이어지고 있다. 차량 노드에서 데이터를 수집하고 지연 및 교통 혼잡 없이 의사 결정을 위해 RSU(roadside unit) 또는 백본 아키텍처로 데이터를 전달하여 처리하도록 네트워크 구성하는 방식이 도입되기도 하였다.

[0004] 다만, 이러한 지능형 교통 시스템(ITS)이 운용되는 네트워크는 다양한 보안 공격에 취약한 개방형 통신 환경을 제공하고 있다. 수신 차량이 전방의 도로가 막힌 것으로 오인하도록, 공격자는 메시지를 위조하고 무차별 공격, 중간자 공격, 재생 공격, 가장 공격, 메시지 조작 공격 등의 우회를 시도할 수 있다. 따라서, 차량은 수신된 메시지를 확인하고 인증하는 기능을 필수적으로 운용할 필요가 있으며, 일반적으로 차량 노드의 높은 이동성을 보장하기 위해 매우 짧은 시간에 빠르게 인증을 수행해야 한다.

발명의 내용

해결하려는 과제

[0005] 따라서, 본 발명은 상술한 문제점을 해결하기 위하여 안출된 것으로, 본 발명의 목적은, 지능형 교통 시스템(ITS)이 운용되는 네트워크에서 지상의 차량 또는 드론 등 무인 항공기와 같은 무선 이동 노드들의 안전하고 빠른 통신이 가능하도록 하기 위한 인증 방법을 적용하는 지능형 교통 시스템을 제공하는 데 있다.

과제의 해결 수단

[0006] 먼저, 본 발명의 특징을 요약하면, 상기의 목적을 달성하기 위한 본 발명의 일면에 따른 무선으로 연결되는 무선 이동 노드들을 포함하는 지능형 교통 시스템에서의 노드들 간의 통신을 위한 세션의 설정을 위한 인증 방법은, (A) RSU의 커버리지에 진입하는 무선 이동 노드에서, 제1 비밀키와 제1 현재 타임 스탬프로 생성한 제1 해시 인증 데이터 및 상기 제1 현재 타임 스탬프를 상기 RSU로 전송하는 단계; (B) 상기 제1 비밀키를 미리 유지하고 있는 상기 RSU에서, 등록이 확인된 상기 무선 이동 노드에 대하여, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프를 이용해 상기 제1 해시 인증 데이터를 인증한 후, 상기 제1 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키와 제2 현재 타임 스탬프로 생성한 제2 해시 인증 데이터 및 상기 제2 현재 타임 스탬프를 네트워크 상의 인증 서버로 전송하는 단계; (C) 상기 인증 서버에서, 등록이 확인된 상기 RSU에 대하여, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 상기 제2 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 상기 제2 비밀키와 슈도 식별자로 생성한 제3 해시 인증 데이터 및 상기 슈도 식별자를 세션키와 함께 상기 RSU로 회신하는 단계; 및 (D) 상기 RSU에서, 상기 제2 비밀키와 상기 슈도 식별자를 이용해 상기 제3 해시 인증 데이터를 인증한 후, 상기 슈도 식별자와 상기 RSU의 식별자를 합성한 뉴 식별자를 생성하여, 상기 무선 이동 노드 및 상기 인증 서버로 통보함으로써, 상기 무선 이

동 노드, 상기 RSU, 및 상기 인증 서버 간에 통신을 위한 세션이 설정되는 단계를 포함할 수 있다.

[0007] 상기 세션이 설정된 복수의 상기 무선 이동 노드로서 차량 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행할 수 있다.

[0008] 상기 세션이 설정된 복수의 상기 무선 이동 노드로서 무인 항공기 노드들 간에 상기 RSU의 중계를 통해 상기 통신을 수행할 수 있다.

[0009] 상기 세션이 설정된 복수의 상기 무선 이동 노드는 차량 노드들 및 무인 항공기 노드들을 포함하고, 상기 RSU는 상기 통신을 위해 상기 차량 노드들 사이, 상기 무인 항공기 노드들 사이, 및 상기 차량 노드와 상기 무인 항공기 노드 사이의 신호 중계를 수행할 수 있다.

[0010] (A) 단계 전에, 상기 인증 서버에서, 복수의 상기 RSU 및 복수의 상기 무선 이동 노드에 대한 식별자들을 데이터베이스에 유지하고, 복수의 상기 RSU로 상기 무선 이동 노드에 대한 식별자들을 전송해 등록하도록 제어하고, 복수의 상기 RSU 각각이 커버리지 내의 하나 이상의 상기 무선 이동 노드로 자신의 식별자를 전송해 등록하도록 제어함으로써, 상기 세션 설정을 위한 (A), (B), (C), (D) 각 단계의 수행을 위해, 상기 인증 서버, 상기 RSU 및 상기 무선 이동 노드 간의 메시지 송수신에서, 송신 노드는 상대방 노드로 자신의 식별자를 포함하는 메시지를 전송해 해당 반응이 이루어지도록 할 수 있다.

[0011] (B) 단계에서, 상기 제1 해시 인증 데이터의 인증에서, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프에 대하여, (A) 단계에서 상기 무선 이동 노드가 상기 제1 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 무선 이동 노드로부터 수신한 상기 제1 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것으로 판단될 수 있다.

[0012] (C) 단계에서, 상기 제2 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프에 대하여, (B) 단계에서 상기 RSU가 상기 제2 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 RSU로부터 수신한 상기 제2 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것으로 판단될 수 있다.

[0013] (D) 단계에서, 상기 제3 해시 인증 데이터의 인증에서, 상기 제2 비밀키와 상기 슈도 식별자에 대하여, (C) 단계에서 상기 인증 서버가 상기 제3 해시 인증 데이터를 생성하는 절차와 동일한 절차로 임시 해시 인증 데이터를 생성한 후, 상기 임시 해시 인증 데이터가 상기 인증 서버로부터 수신한 상기 제3 해시 인증 데이터와 동일할 때, 상기 인증이 완료된 것으로 판단될 수 있다.

[0014] 그리고, 본 발명의 다른 일면에 따른 무선으로 연결되는 무선 이동 노드들을 포함하는 지능형 교통 시스템에서의 노드들 간의 통신을 위한 세션의 설정을 위한 인증 기능을 구현하기 위한 컴퓨터에 의해 판독 가능한 기록매체는, (A) RSU의 커버리지에 진입하는 무선 이동 노드에서, 제1 비밀키와 제1 현재 타임 스탬프로 생성한 제1 해시 인증 데이터 및 상기 제1 현재 타임 스탬프를 상기 RSU로 전송하는 기능; (B) 상기 제1 비밀키를 미리 유지하고 있는 상기 RSU에서, 등록이 확인된 상기 무선 이동 노드에 대하여, 상기 제1 비밀키와 상기 제1 현재 타임 스탬프를 이용해 상기 제1 해시 인증 데이터를 인증한 후, 상기 제1 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키와 제2 현재 타임 스탬프로 생성한 제2 해시 인증 데이터 및 상기 제2 현재 타임 스탬프를 네트워크 상의 인증 서버로 전송하는 기능; (C) 상기 제2 비밀키를 미리 유지하고 있는 상기 인증 서버에서, 등록이 확인된 상기 RSU에 대하여, 상기 제2 비밀키와 상기 제2 현재 타임 스탬프를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 상기 제2 현재 타임 스탬프의 시각으로부터 소정의 시간 이내일 때, 상기 제2 비밀키와 슈도 식별자로 생성한 제3 해시 인증 데이터 및 상기 슈도 식별자를 세션키와 함께 상기 RSU로 회신하는 기능; 및 (D) 상기 RSU에서, 상기 제2 비밀키와 상기 슈도 식별자를 이용해 상기 제3 해시 인증 데이터를 인증한 후, 상기 슈도 식별자와 상기 RSU의 식별자를 합성한 뉴 식별자를 생성하여, 상기 무선 이동 노드 및 상기 인증 서버로 통보함으로써, 상기 무선 이동 노드, 상기 RSU, 및 상기 인증 서버 간에 통신을 위한 세션이 설정되는 기능을 수행할 수 있다.

발명의 효과

[0015] 본 발명에 따른 지능형 교통 시스템에서의 인증 방법은, 지능형 교통 시스템(ITS)이 운용되는 네트워크에서 지상의 차량 또는 드론 등 무인 항공기와 같은 무선 이동 노드들에 대한 효과적인 인증이 이루어져 안전한 통신이 가능하다. 따라서, 무선 이동 노드들은 무차별 공격, 중간자 공격, 재생 공격, 가장 공격, 메시지 조작 공격 등을 시도하는 공격자로부터 안전하게 데이터를 주고 받을 수 있으며 무선 이동 노드들의 높은 이동성을 보

장할 수 있다.

도면의 간단한 설명

[0016] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는 첨부도면은, 본 발명에 대한 실시예를 제공하고 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1은 본 발명의 일 실시예에 따른 지능형 교통 시스템을 설명하기 위한 도면이다.

도 2는 도 1의 인증 서버에서 차량 노드들에 대한 세션 설정을 설명하기 위한 도면이다.

도 3은 도 1의 인증 서버에서 무인 항공기 노드들에 대한 세션 설정을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 해시 인증 방식을 설명하기 위한 도면이다.

도 5는 본 발명과 종래 기술들의 차량 노드들에서의 세션 설정 완료에 소요되는 시간 비용에 대한 예이다.

도 6은 본 발명과 종래 기술들의 차량 노드들에서의 세션 설정 완료에 소요되는 시간 비용에 대한 다른 예이다.

도 7은 본 발명의 일 실시예에 따른 지능형 교통 시스템에서 노드들 간의 통신을 위한 세션의 설정을 위한 인증 방법을 처리하는 장치의 구현 방법의 일례를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하에서는 첨부된 도면들을 참조하여 본 발명에 대해서 자세히 설명한다. 이때, 각각의 도면에서 동일한 구성요소는 가능한 동일한 부호로 나타낸다. 또한, 이미 공지된 기능 및/또는 구성에 대한 상세한 설명은 생략한다. 이하에 개시된 내용은, 다양한 실시 예에 따른 동작을 이해하는데 필요한 부분을 중점적으로 설명하며, 그 설명의 요지를 흐릴 수 있는 요소들에 대한 설명은 생략한다. 또한 도면의 일부 구성요소는 과장되거나 생략되거나 또는 개략적으로 도시될 수 있다. 각 구성요소의 크기는 실제 크기를 전적으로 반영하는 것이 아니며, 따라서 각각의 도면에 그려진 구성요소들의 상대적인 크기나 간격에 의해 여기에 기재되는 내용들이 제한되는 것은 아니다.

[0018] 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 용어들로서 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 실시 예들을 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.

[0019] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0020] 도 1은 본 발명의 일 실시예에 따른 지능형 교통 시스템(100)을 설명하기 위한 도면이다.

[0021] 도 1을 참조하면, 본 발명의 일 실시예에 따른 지능형 교통 시스템(100)은, 차량 노드들(110)과 무인 항공기 노드들(120)을 포함하는 무선 이동 노드들(110, 120), RSU(Roadside Unit, 노변기지국)(130) 및 RSU(130)와 유무선 인터넷을 통한 통신이 이루어지는 인증 서버(150)를 포함한다.

[0022] 무선 이동 노드들(110, 120)은 RSU(130)와 무선 통신, 예를 들어, WAVE(Wireless Access in Vehicular Environment) 등 무선 통신 방식으로 통신할 수 있다. 경우에 따라서는, 무선 이동 노드들(110, 120)은 RSU(130)와 WiFi, WiBro 등 무선 인터넷 통신, WCDMA, LTE, 5G 등 이동통신 등의 무선 통신 방식으로 통신할 수 있다.

[0023] 무선 이동 노드들(110, 120)은 RSU(130)의 중계를 통해 위와 같은 무선 통신 방식으로 연결될 수 있다. 즉, RSU(130)는 상기 통신을 위해 차량 노드들(110) 사이, 무인 항공기 노드들(120) 사이, 및 하나 이상의 차량 노

드(110)와 하나 이상의 무인 항공기 노드(120) 사이의 신호 중계를 수행할 수 있다. RSU(130)는 상기 지능형 교통 시스템(100)의 서비스가 운용되는 지상의 운전자 차량, 자율 주행 차량이 주행하는 모든 도로들의 주변에 소정의 간격으로 설치될 수 있다. RSU(130)는 인증 서버(150)와 인터넷으로 연결되어 차량 노드들(110)과 무인 항공기 노드들(120)의 통신을 중계하는 노변 기지국에 해당한다.

[0024] 차량 노드들(110)은 위와 같은 무선 통신이 가능한 지상의 운전자 차량, 자율 주행 차량 또는 차량에 구비된 모듈일 수 있으며, 위와 같은 무선 통신이 가능한 모뎀을 구비하고 RSU(130)의 중계를 받는 도 7과 같은 제어장치나 프로세서 및 사용자 인터페이스 등을 포함할 수 있다. 무인 항공기 노드들(120)은 위와 같은 무선 통신이 가능한 드론과 같은 무인 항공기 또는 무인 항공기에 구비된 모듈일 수 있으며, 위와 같은 무선 통신이 가능한 모뎀을 구비하고 RSU(130)의 중계를 받는 도 7과 같은 제어장치나 프로세서 및 사용자 인터페이스 등을 포함할 수 있다.

[0025] 본 발명의 지능형 교통 시스템(100)에서는, 이와 같은 무선 이동 노드들(110, 120)의 통신을 위한 세션의 설정을 위하여, 무선 이동 노드들(110, 120), RSU(130) 및 인증 서버(150)가 운용되는 네트워크에서 지상의 차량 또는 드론 등 무인 항공기와 같은 무선 이동 노드들에 대한 효과적인 인증이 이루어져 안전한 통신이 가능하도록 하였다. 따라서, 무선 이동 노드들(110, 120)은 무차별 공격, 중간자 공격, 재생 공격, 가장 공격, 메시지 조작 공격 등을 시도하는 공격자로부터 안전하게 데이터를 주고받을 수 있으며 무선 이동 노드들(110, 120)의 높은 이동성을 보장할 수 있도록 하였다.

[0026] 이하, 도 2에서는 인증 서버(150)에서 차량 노드들(110)에 대한 세션 설정 과정을 설명하고, 도 3에서는 인증 서버(150)에서 무인 항공기 노드들(120)에 대한 세션 설정 과정을 설명한다.

[0027] 도 2는 도 1의 인증 서버(150)에서 차량 노드들(110)에 대한 세션 설정을 설명하기 위한 도면이다.

[0028] 먼저, 도 2를 참조하면, 인증 서버(150)는, 복수의 RSU(130) 및 복수의 무선 이동 노드로서의 차량 노드들(110)에 대한 식별자들(예, ID)을 데이터베이스에 유지하고 있고, 인증 서버(150)는, 복수의 RSU(130)로 무선 이동 노드로서의 차량 노드들(110)에 대한 식별자들을 전송해 등록하도록 제어하고(S110), 이때, 복수의 RSU(130) 각각은 커버리지 내의 하나 이상의 차량 노드들(110)로 자신의 식별자를 전송해 등록하도록 제어한다(S111). RSU(130)는 인증 서버(150)로부터 수신한 식별자들을 갖는 차량 노드들(110)에 대항 상기 등록을 제어할 수 있으며, 인증 서버(150)에 유지 관리되고 있는 식별자들을 가진 차량 노드들(110)은 상기 등록을 완료할 수 있다. 이에 따라, 하기의 세션 설정을 위한 각 단계(S120 ~ S154)의 수행을 위해, 인증 서버(150), RSU(130) 및 무선 이동 노드로서의 차량 노드(110) 간의 메시지 송수신에서, 송신 노드(송신측 노드)는 상대방 노드(수신측 노드)로 자신의 식별자를 포함하는 메시지를 전송해 해당 반응, 즉, 메시지에 대응되는 절차의 수행이나 응답 등이 이루어지도록 할 수 있다. 세션 설정 후 노드들 간의 통신에서도 위와 같은 송신 노드(송신측 노드)와 상대방 노드(수신측 노드) 간에는 상기 식별자를 포함하는 메시지를 통해 데이터 전송 등의 통신이 이루어질 수 있다.

[0029] 이후, RSU(130)의 커버리지에 진입하는 무선 이동 노드로서의 차량 노드(110)에서, 제1 비밀키(SK1)와 제1 현재 타임 스탬프(CTS1)로 생성한 제1 해시 인증 데이터(Hash(SK1 || CTS1)) 및 제1 현재 타임 스탬프(CTS1)를 포함하는 메시지를 RSU(130)로 전송할 수 있다(S120). 상기 제1 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기 제1 현재 타임 스탬프(CTS1)는 차량 노드(110)에서 측정한 현재 시각, 즉, 상기 제1 해시 인증 데이터를 생성할 때의 시각이다.

[0030] RSU(130)는 차량 노드(110)로부터 수신한 메시지에 대해 상술한 식별자를 확인하여 차량 노드(110)의 등록 여부를 확인하고(S130), 등록이 안된 경우라면(S140) 다시한번 식별자를 요구하는 메시지(AREQ)를 차량 노드(110)로 전송한 후, 차량 노드(110)로부터 응답 메시지에 포함된 식별자를 수신하여(S141), RSU(130)는 수신된 식별자가 인증 서버(150)로부터 수신한 식별자 목록에 있는 경우라면, 해당 차량 노드(110)를 등록하고, 세션 설정 절차를 하기와 같이 이어갈 수 있다(S150).

[0031] 즉, RSU(130)는 제1 비밀키(SK1)를 미리 메모리에 저장하여 유지하고 있으며, RSU(130)는 등록이 확인된 무선 이동 노드로서의 차량 노드(110)에 대하여(S150), 제1 비밀키(SK1)와 수신한 메시지의 제1 현재 타임 스탬프(CTS1)를 이용해 제1 해시 인증 데이터(Hash(SK1 || CTS1))를 인증한 후, 제1 현재 타임 스탬프(CTS1)의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키(SK2)와 제2 현재 타임 스탬프(CTS2)로 생성한 제2 해시 인증 데이터(Hash(SK2 || CTS2)) 및 제2 현재 타임 스탬프(CTS2)를 네트워크 상의 인증 서버(150)로 전송한다(S151). 상기 제2 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기 제2 현재 타

임 스탬프(CTS2)는 RSU(130)에서 측정한 현재 시각, 즉, 상기 제2 해시 인증 데이터를 생성할 때의 시각이다.

[0032] 이에 따라, 인증 서버(150)는 제2 비밀키(SK2)를 미리 메모리에 저장하여 유지하고 있으며, 인증 서버(150)에서, 등록이 확인된 RSU(130)에 대하여, 제2 비밀키(SK2)와 수신된 메시지의 제2 현재 타임 스탬프(CTS2)를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 제2 현재 타임 스탬프(CTS2)의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키(SK2)와 슈도 식별자(PI1)로 생성한 제3 해시 인증 데이터(Hash(SK2 || PI1)) 및 슈도 식별자(PI1)를 세션키(SSK1)와 함께 RSU(130)로 회신할 수 있다(S152). 상기 제3 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기 슈도 식별자(PI1)는 인증 서버(150)가 세션 설정을 위해 생성하는 임시 식별자 정보이며, 세션키(SSK1)는 인증 서버(150)가 세션 설정을 위해 생성하는 세션키 정보이다.

[0033] 이후, RSU(130)는, 제2 비밀키(SK2)와 슈도 식별자(PI1)를 이용해 제3 해시 인증 데이터(Hash(SK2 || PI1))를 인증한 후, 슈도 식별자(PI1)와 RSU(130)의 식별자를 합성한 뉴 식별자(NID1)를 생성하여, 무선 이동 노드로서의 차량 노드(110) 및 인증 서버(150)로 통보함으로써, 차량 노드(110), RSU(130), 및 인증 서버(150) 간에 통신을 위한 세션이 설정된다(S153, S154). RSU(130)는 차량 노드(110)로 뉴 식별자(NID1)를 전송할 때 세션키(SSK1)를 더 전송할 수도 있다. 상기 뉴 식별자(NID1)는 슈도 식별자(PI1)와 RSU(130)의 식별자에 대한 소정의 연산(예, 곱셈, 덧셈, 배타적 논리합(XOR) 등)을 통해 합성되는 값일 수 있다.

[0034] 이와 같은 절차를 통해 세션 설정이 이루어진 후 상호 간에 상기 세션키를 주고받으면서, 차량 노드들(110)은 RSU(130)의 중계를 통해 위와 같은 무선 통신 방식으로 연결될 수 있다. 즉, RSU(130)는 상기 통신을 위해 차량 노드들(110) 사이의 신호 중계를 수행할 수 있다.

[0035] 도 3은 도 1의 인증 서버(150)에서 무인 항공기 노드들(120)에 대한 세션 설정을 설명하기 위한 도면이다.

[0036] 도 3을 참조하면, 인증 서버(150)는, 복수의 RSU(130) 및 복수의 무선 이동 노드로서의 무인 항공기 노드들(120)에 대한 식별자들(예, ID)을 데이터베이스에 유지하고 있고, 인증 서버(150)는, 복수의 RSU(130)로 무선 이동 노드로서의 무인 항공기 노드들(120)에 대한 식별자들을 전송해 등록하도록 제어하고(S210), 이때, 복수의 RSU(130) 각각은 커버리지 내의 하나 이상의 무인 항공기 노드들(120)로 자신의 식별자를 전송해 등록하도록 제어한다(S211). RSU(130)는 인증 서버(150)로부터 수신한 식별자들을 갖는 무인 항공기 노드들(120)에 대항 상기 등록을 제어할 수 있으며, 인증 서버(150)에 유지 관리되고 있는 식별자들을 가진 무인 항공기 노드들(120)은 상기 등록을 완료할 수 있다. 이에 따라, 하기의 세션 설정을 위한 각 단계(S220 ~ S254)의 수행을 위해, 인증 서버(150), RSU(130) 및 무선 이동 노드로서의 무인 항공기 노드(120) 간의 메시지 송수신에서, 송신 노드(송신측 노드)는 상대방 노드(수신측 노드)로 자신의 식별자를 포함하는 메시지를 전송해 해당 반응, 즉, 메시지에 대응되는 절차의 수행이나 응답 등이 이루어지도록 할 수 있다. 세션 설정 후 노드들 간의 통신에서도 위와 같은 송신 노드(송신측 노드)와 상대방 노드(수신측 노드) 간에는 상기 식별자를 포함하는 메시지를 통해 데이터 전송 등의 통신이 이루어질 수 있다.

[0037] 이후, RSU(130)의 커버리지에 진입하는 무선 이동 노드로서의 무인 항공기 노드(120)에서, 제1 비밀키(SK3)와 제1 현재 타임 스탬프(CTS3)로 생성한 제1 해시 인증 데이터(Hash(SK3 || CTS3)) 및 제1 현재 타임 스탬프(CTS3)를 포함하는 메시지를 RSU(130)로 전송할 수 있다(S220). 상기 제1 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기 제1 현재 타임 스탬프(CTS3)는 무인 항공기 노드(120)에서 측정한 현재 시각, 즉, 상기 제1 해시 인증 데이터를 생성할 때의 시각이다.

[0038] RSU(130)는 무인 항공기 노드(120)로부터 수신한 메시지에 대해 상술한 식별자를 확인하여 무인 항공기 노드(120)의 등록 여부를 확인하고(S230), 등록이 안된 경우라면(S240) 다시한번 식별자를 요구하는 메시지(AREQ)를 무인 항공기 노드(120)로 전송한 후, 무인 항공기 노드(120)로부터 응답 메시지에 포함된 식별자를 수신하여(S241), RSU(130)는 수신된 식별자가 인증 서버(150)로부터 수신한 식별자 목록에 있는 경우라면, 해당 무인 항공기 노드(120)를 등록하고, 세션 설정 절차를 하기와 같이 이어갈 수 있다(S250).

[0039] 즉, RSU(130)는 제1 비밀키(SK3)를 미리 메모리에 저장하여 유지하고 있으며, RSU(130)는 등록이 확인된 무선 이동 노드로서의 무인 항공기 노드(120)에 대하여(S250), 제1 비밀키(SK3)와 수신한 메시지의 제1 현재 타임 스탬프(CTS3)를 이용해 제1 해시 인증 데이터(Hash(SK3 || CTS3))를 인증한 후, 제1 현재 타임 스탬프(CTS3)의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키(SK4)와 제2 현재 타임 스탬프(CTS4)로 생성한 제2 해시 인증 데이터(Hash(SK4 || CTS4)) 및 제2 현재 타임 스탬프(CTS4)를 네트워크 상의 인증 서버(150)로 전송한다(S251). 상기 제2 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기

제2 현재 타임 스탬프(CTS4)는 RSU(130)에서 측정한 현재 시각, 즉, 상기 제2 해시 인증 데이터를 생성할 때의 시각이다.

[0040] 이에 따라, 인증 서버(150)는 제2 비밀키(SK4)를 미리 메모리에 저장하여 유지하고 있으며, 인증 서버(150)에서, 등록이 확인된 RSU(130)에 대하여, 제2 비밀키(SK4)와 수신된 메시지의 제2 현재 타임 스탬프(CTS4)를 이용해 상기 제2 해시 인증 데이터를 인증한 후, 제2 현재 타임 스탬프(CTS4)의 시각으로부터 소정의 시간 이내일 때, 제2 비밀키(SK4)와 슈도 식별자(PI2)로 생성한 제3 해시 인증 데이터(Hash(SK4 || PI2)) 및 슈도 식별자(PI2)를 세션키(SSK2)와 함께 RSU(130)로 회신할 수 있다(S252). 상기 제3 해시 인증 데이터의 생성과 인증은 하기의 도 4에 대한 부연 설명을 참조하기로 한다. 상기 슈도 식별자(PI2)는 인증 서버(150)가 세션 설정을 위해 생성하는 임시 식별자 정보이며, 세션키(SSK2)는 인증 서버(150)가 세션 설정을 위해 생성하는 세션키 정보이다.

[0041] 이후, RSU(130)는, 제2 비밀키(SK4)와 슈도 식별자(PI2)를 이용해 제3 해시 인증 데이터(Hash(SK4 || PI2))를 인증한 후, 슈도 식별자(PI2)와 RSU(130)의 식별자를 합성한 뉴 식별자(NID2)를 생성하여, 무선 이동 노드로서의 무인 항공기 노드(120) 및 인증 서버(150)로 통보함으로써, 무인 항공기 노드(120), RSU(130), 및 인증 서버(150) 간에 통신을 위한 세션이 설정된다(S253, S254). RSU(130)는 무인 항공기 노드(120)로 뉴 식별자(NID2)를 전송할 때 세션키(SSK2)를 더 전송할 수도 있다. 상기 뉴 식별자(NID2)는 슈도 식별자(PI2)와 RSU(130)의 식별자에 대한 소정의 연산(예, 곱셈, 덧셈, 배타적 논리합(XOR) 등)을 통해 합성되는 값일 수 있다.

[0042] 이와 같은 절차를 통해 세션 설정이 이루어진 후 상호 간에 상기 세션키를 주고받으면서, 무인 항공기 노드들(120)은 RSU(130)의 중계를 통해 위와 같은 무선 통신 방식으로 연결될 수 있다. 즉, RSU(130)는 상기 통신을 위해 무인 항공기 노드들(120) 사이의 신호 중계를 수행할 수 있다.

[0043] 또한, 도 2, 및 도 3과 같은 세션 설정이 이루어진 후 상호 간에 상기 세션키를 주고받으면서, 무선 이동 노드들(110, 120)은 RSU(130)의 중계를 통해 위와 같은 무선 통신 방식으로 연결될 수 있다. 즉, RSU(130)는 상기 통신을 위해 차량 노드들(110) 사이, 무인 항공기 노드들(120) 사이, 및 하나 이상의 차량 노드(110)와 하나 이상의 무인 항공기 노드(120) 사이의 신호 중계를 수행할 수 있다.

[0044] 도 4는 본 발명의 일 실시예에 따른 해시 인증 방식을 설명하기 위한 도면이다.

[0045] 도 4를 참조하면, 송신 노드(Alice)가 비밀키(K)와 타임 스탬프나 슈도 식별자 등 메시지(M)로 소정의 해쉬 함수(Hash)를 이용해 해시 인증 데이터(MAC)을 생성하여, 해시 인증 데이터(MAC)와 메시지(M)를 수신 노드(Bob)로 전송하고, 수신 노드(Bob)는 해시 인증 데이터(MAC)를 인증하기 위하여, 가지고 있는 비밀키(K)와 수신된 메시지(M)에 대해 송신 노드(Alice)에서 해시 인증 데이터(MAC)을 생성하는 절차와 동일한 절차로 소정의 해쉬 함수(Hash)를 이용해 임시 해시 인증 데이터(MAC')를 생성한 후, 상기 임시 해시 인증 데이터(MAC')가 송신 노드(Alice)로부터 수신한 해시 인증 데이터(MAC)와 동일한지 여부를 판단한다. 즉, 동일하면 인증이 완료되며 그렇지 않으면 인증되지 않은 것이다.

[0046] 이와 같은 해시 인증 데이터의 생성과 인증 방식은 도 2의 S120 단계, S151 단계, S152 단계에서의 각각의 해시 인증 데이터의 생성과 인증에 적용될 수 있다. 또한, 이와 같은 해시 인증 데이터의 생성과 인증 방식은 도 3의 S220 단계, S251 단계, S252 단계에서의 각각의 해시 인증 데이터의 생성과 인증에 적용될 수 있다.

[0047] 도 5는 본 발명(510)과 종래 기술들(520, 530)의 차량 노드들에서의 세션 설정 완료에 소요되는 시간 비용에 대한 예이다.

[0048] 도 5를 참조하면, 본 발명(510)의 경우가 종래 HCPA-GKA(Hash function based Conditional Privacy Authentication and GroupKey Agreement) 방식(520)이나, 종래 PW-CPPA-GKA(PassWord based Conditional Privacy Preserving Authentication and Group Key Agreement) 방식(530) 보다, 차량의 수에 대한 차량 노드에서의 세션 설정 완료에 소요되는 시간 비용(Time Codt)이, 훨씬 작아지는 것을 확인하였다.

[0049] 도 6은 본 발명(610)과 종래 기술들(620, 630)의 차량 노드들에서의 세션 설정 완료에 소요되는 시간 비용에 대한 다른 예이다.

[0050] 도 6과 같이, 도 5 에서 보다 RSU(130) 주위에 더 많은 차량이 주행 중인 환경에서도, 본 발명(610)의 경우가 종래 HCPA-GKA(Hash function based Conditional Privacy Authentication and GroupKey Agreement) 방식(620)이나, 종래 PW-CPPA-GKA(PassWord based Conditional Privacy Preserving Authentication and Group Key Agreement) 방식(630) 보다, 차량의 수에 대한 차량 노드에서의 세션 설정 완료에 소요되는 시간 비용(Time

Codt)이, 훨씬 작아지는 것을 확인하였다.

[0051] 도 7은 본 발명의 일 실시예에 따른 지능형 교통 시스템(100)에서 노드들 간의 통신을 위한 세션의 설정을 위한 인증 방법을 처리하는 장치의 구현 방법의 일례를 설명하기 위한 도면이다.

[0052] 도 7을 참조하면, 본 발명의 일 실시예에 따른 지능형 교통 시스템(100)에서의 인증 방법을 처리하는 무선 이동 노드들(110, 120), RSU(130), 인증 서버(150)의 장치(또는 모듈)는, 하드웨어, 소프트웨어, 또는 이들의 결합으로 이루어질 수 있다. 예를 들어, 본 발명의 지능형 교통 시스템(100)에서 인증 방법을 처리하는 장치는, 위와 같은 기능/단계/과정들을 수행하기 위한 적어도 하나의 프로세서를 갖는 도 7과 같은 컴퓨팅 시스템(1000) 또는 인터넷 상의 서버 형태로 구현될 수 있다.

[0053] 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. 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 불휘발성 저장 매체를 포함할 수 있다. 예를 들어, 메모리(1300)는 ROM(Read Only Memory)(1310) 및 RAM(Random Access Memory)(1320)을 포함할 수 있다. 또한, 네트워크 인터페이스(1700)는 스마트폰, 노트북 PC, 데스크탑 PC 등 해당 장치에서의 유선 인터넷 통신이나 WiFi, WiBro 등 무선 인터넷 통신, WCDMA, LTE 등 이동통신을 지원하는 모뎀 등의 통신 모듈이나, 근거리 무선 통신 방식(예, 블루투스, 지그비, 와이파이 등)의 통신을 지원하는 모뎀 등의 통신모듈을 포함할 수 있다.

[0054] 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 같이 컴퓨터 등 장치로 판독 가능한 저장/기록 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 정보(코드)를 판독할 수 있고 저장 매체에 정보(코드)를 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.

[0055] 상술한 바와 같이, 본 발명에 따른 지능형 교통 시스템(100)에서의 인증 방법은, 지능형 교통 시스템(100)이 운용되는 네트워크에서 지상의 차량 또는 드론 등 무인 항공기와 같은 무선 이동 노드들에 대한 효과적인 인증이 이루어져 안전하고 빠른 통신이 가능하다. 따라서, 무선 이동 노드들은 무차별 공격, 중간자 공격, 재생 공격, 가장 공격, 메시지 조작 공격 등을 시도하는 공격자로부터 안전하게 데이터를 주고받을 수 있으며 무선 이동 노드들의 높은 이동성을 보장할 수 있다.

[0056] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0057] 차량 노드(110)

무인 항공기 노드(120)

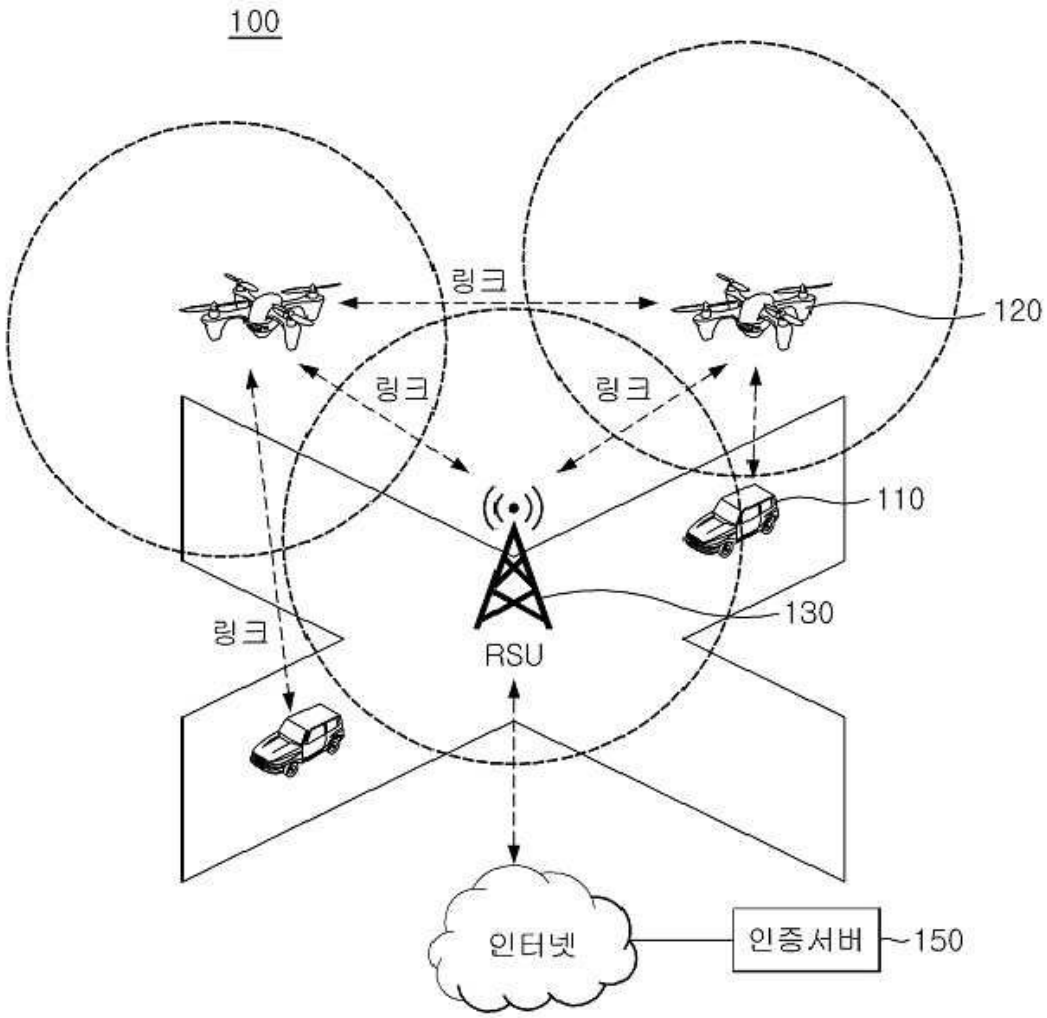
무선 이동 노드(110, 120)

RSU(130)

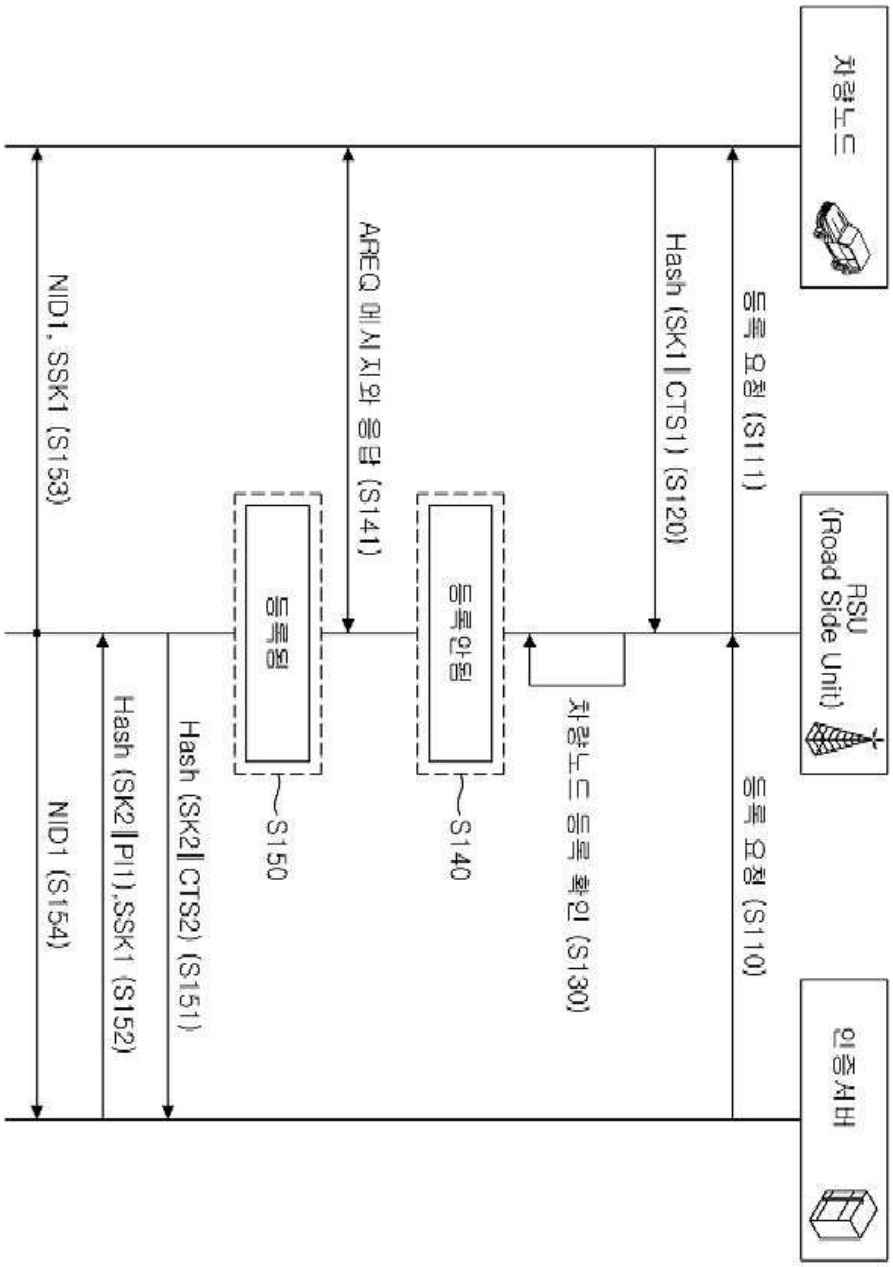
인증 서버(150)

도면

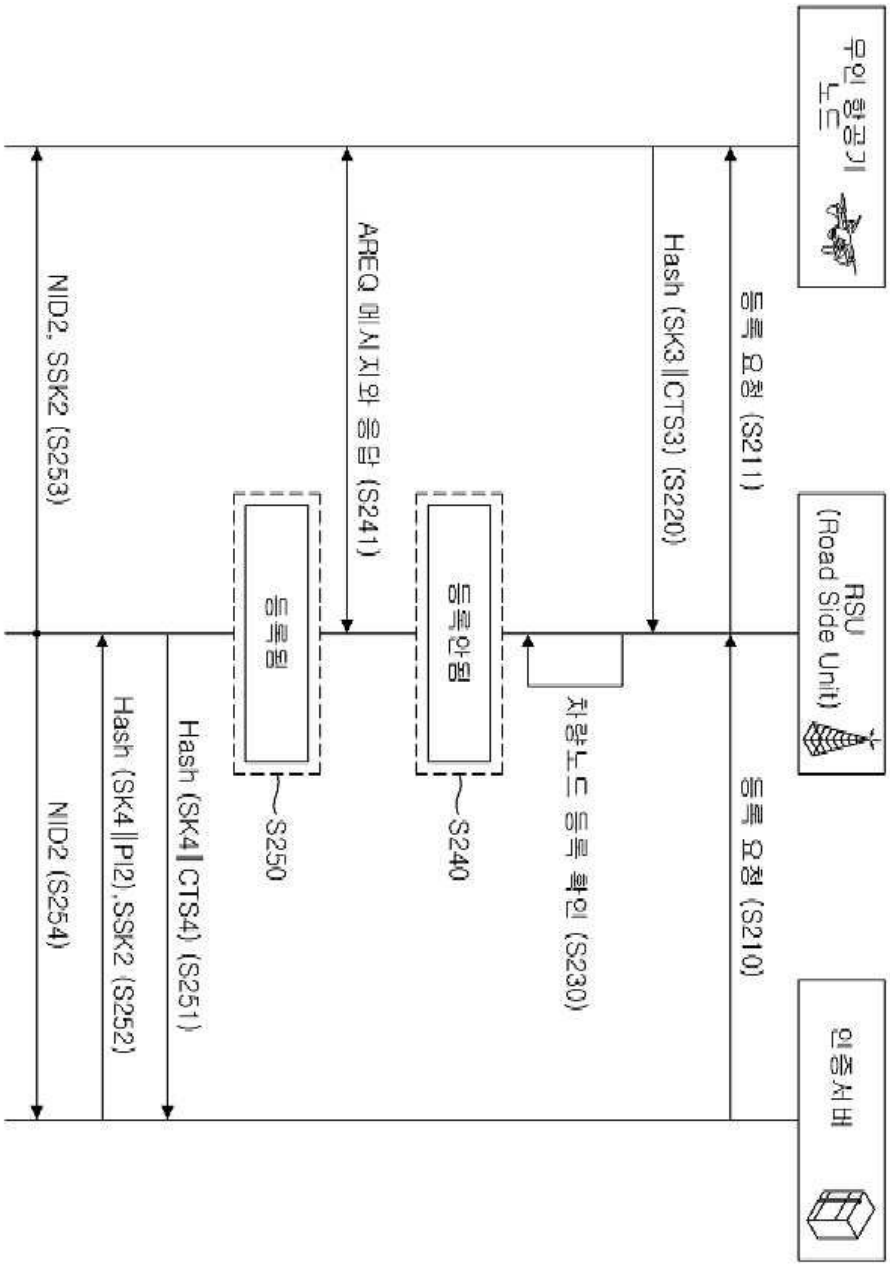
도면1



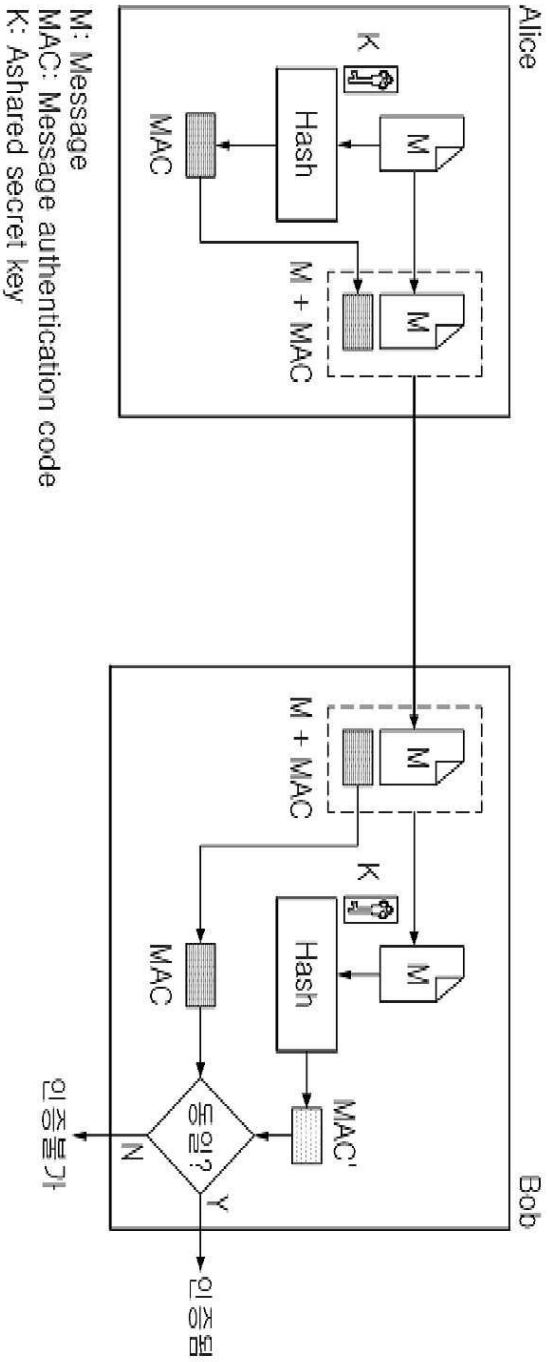
도면2


차량노드
RSU
(Road Side Unit)
인증서버
등록 요청 (S111)
Hash (SK1‖CTS1) (S120)
AREQ 메시지와 응답 (S141)
NID1, SSK1 (S153)
등록안됨
S140
차량노드 등록 확인 (S130)
등록 요청 (S110)
등록됨
S150
Hash (SK2‖CTS2) (S151)
Hash (SK2‖PI1),SSK1 (S152)
NID1 (S154)

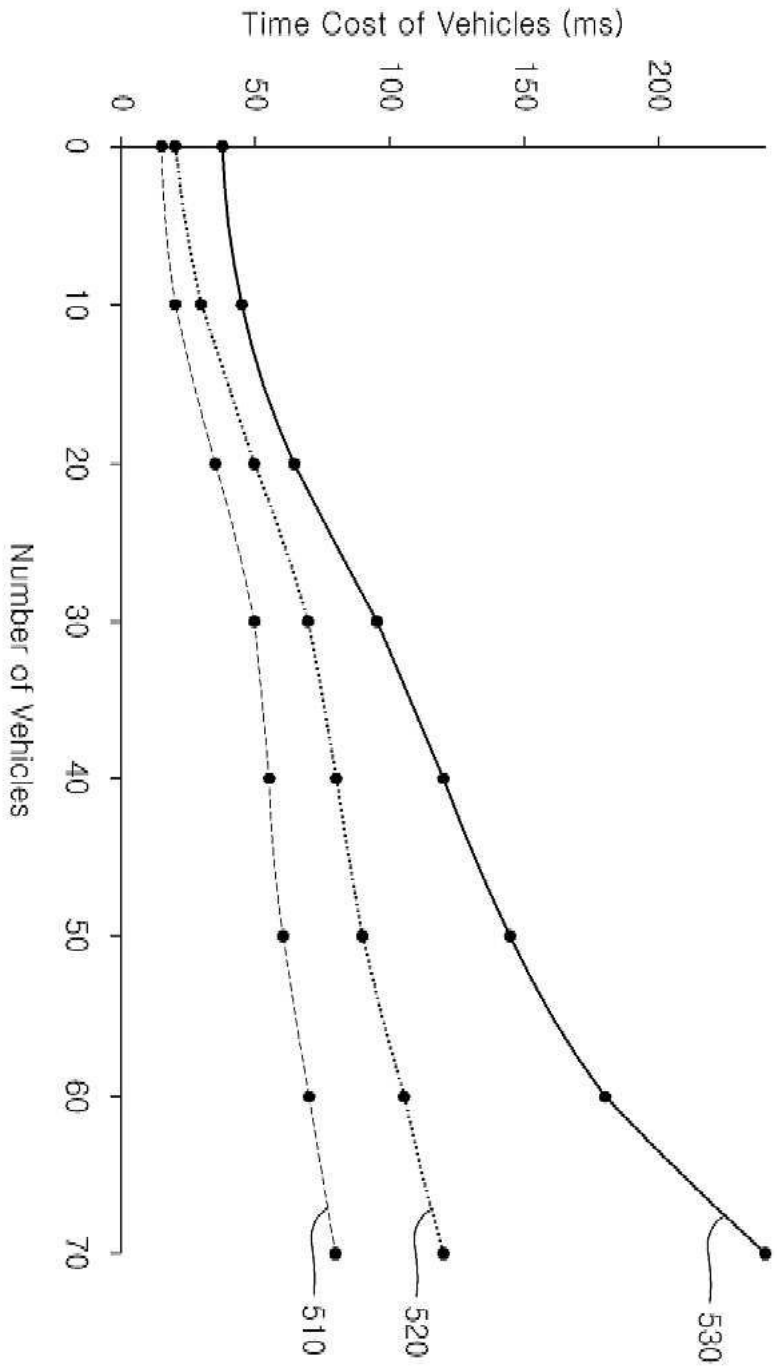
도면3


무인 항공기 노드
RSU (Road Side Unit)
인증서버
등록 요청 (S211)
Hash (SK3||CTS3) (S220)
AREQ 메시지와 응답 (S241)
NID2, SSK2 (S253)
등록 요청 (S210)
차량노드 등록 확인 (S230)
등록안됨
S240
등록됨
S250
Hash (SK4||CTS4) (S251)
Hash (SK4||PI2),SSK2 (S252)
NID2 (S254)

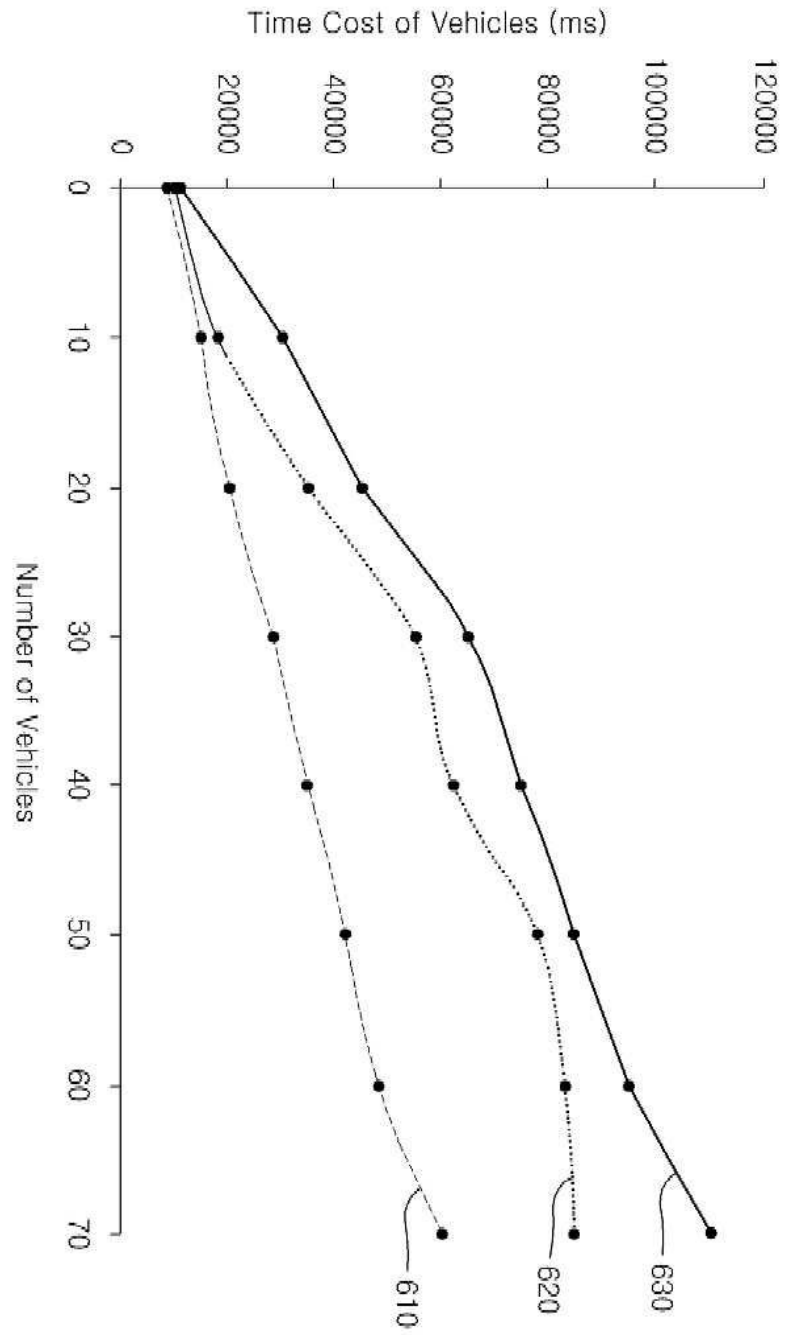
도면4


M: Message
MAC: Message authentication code
K: Ashared secret key
Alice
K
Hash
M
MAC
M + MAC
M
Bob
M + MAC
M
K
Hash
M
MAC
MAC'
동일?
N
Y
인증불가
인증됨

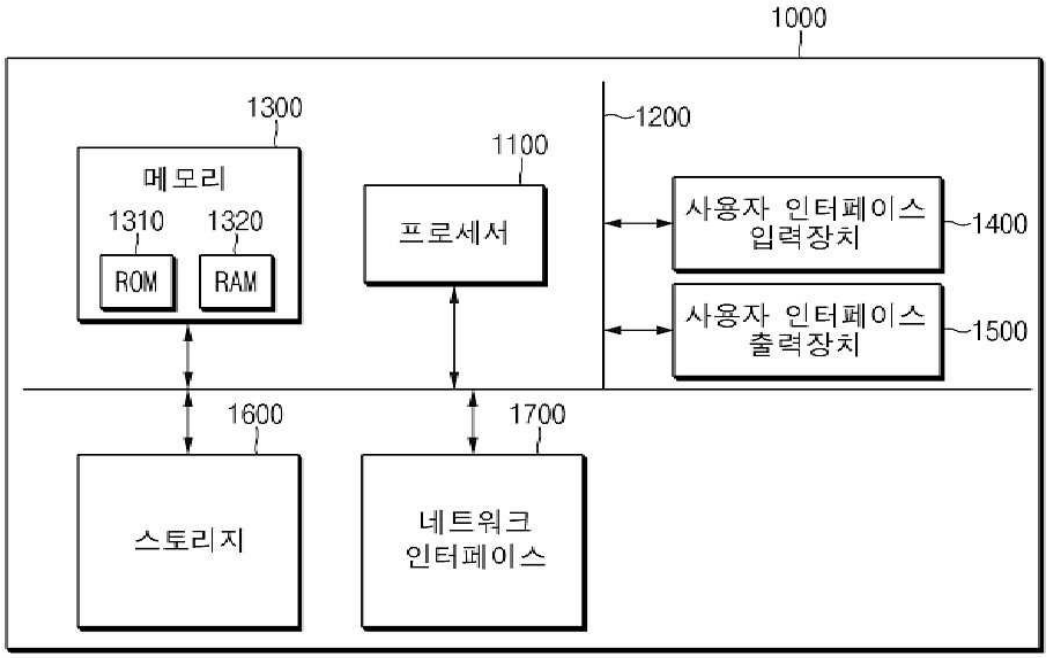
도면5


Time Cost of Vehicles (ms)
0
50
100
150
200
Number of Vehicles
0
10
20
30
40
50
60
70
510
520
530

도면6


Time Cost of Vehicles (ms)
0
20000
40000
60000
80000
100000
120000
Number of Vehicles
0
10
20
30
40
50
60
70
610
620
630

도면7


1000
1300
메모리
1310
1320
ROM
RAM
1100
프로세서
1200
사용자 인터페이스
입력장치
1400
사용자 인터페이스
출력장치
1500
1600
스토리지
1700
네트워크
인터페이스