(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0086174
(43) 공개일자 2017년07월26일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/58* (2006.01)
(52) CPC특허분류
H04L 63/123 (2013.01)
H04L 51/30 (2013.01)
(21) 출원번호 10-2016-0005541
(22) 출원일자 2016년01월15일
심사청구일자 2016년01월15일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
조효진
서울특별시 성북구 안암로 145 자연계캠퍼스 로봇융합관 403호 (안암동5가,고려대학교안암캠퍼스)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
우사무엘
서울특별시 송파구 오금로53길 7 403호 (거여동, 명산주택)
(74) 대리인
김등용, 김홍석

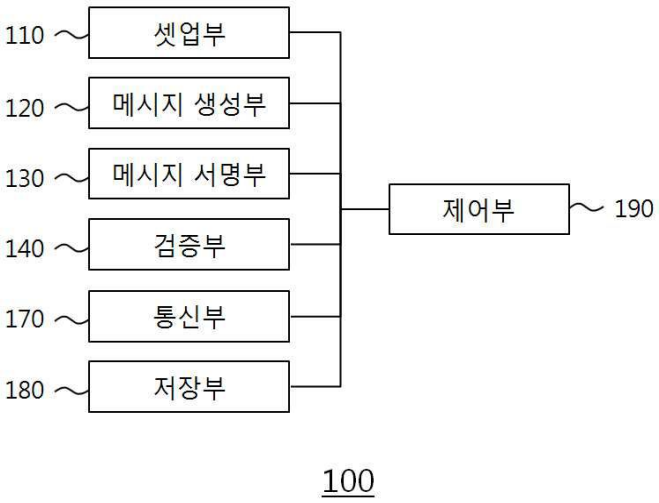
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **VANET 환경에서 익명 ID를 이용한 메시지 협력 검증 방법 및 장치**

(57) 요 약

VANET 환경에서 협력 검증 장치가 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 방법이 개시된다. 상기 메시지 협력 검증 방법은 다른 차량으로부터 적어도 안전 메시지를 포함하는 제1 메시지들을 수신하는 단계, 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 검증 대상 제1 메시지를 선택하여 검증하는 제1 메시지 검증 단계, 상기 검증 결과를 포함하는 제2 메시지를 생성하여 서명하고 전송하는 단계, 다른 차량으로부터 적어도 하나 이상의 제2 메시지들을 수신하는 단계, 및 다른 차량으로부터 수신한 상기 제2 메시지들 중에서 검증 대상 제2 메시지를 선택하고 선택한 제2 메시지에 포함된 검증 결과를 이용하여 검증을 수행하는 제2 메시지 검증 단계를 포함한다.

대 표 도 - 도2



100

(52) CPC특허분류
H04L 63/0421 (2013.01)
H04L 63/08 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 B01011505530003003
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송연구개발사업
연구과제명 자동차 전장 ECU간 보안전송기술 개발
기 여 율 1/1
주관기관 인포뱅크
연구기간 2015.03.01 ~ 2016.02.29

명 세 서

청구범위

청구항 1

VANET 환경에서 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 각각의 차량에 포함된 협력 검증 장치에 있어서,

제1 메시지 생성부 및 제2 메시지 생성부를 포함하는 메시지 생성부,

생성된 메시지를 익명 ID 및 이에 대응하는 서명키를 이용하여 서명을 수행하는 메시지 서명부,

상기 메시지 생성부에서 생성한 제1 메시지 또는 제2 메시지를 다른 차량의 협력 검증 장치로 송신하고, 다른 차량의 협력 검증 장치로부터 제1 메시지 또는 제2 메시지를 수신하는 통신부, 및

상기 다른 차량의 협력 검증 장치로부터 수신한 제1 메시지 또는 제2 메시지를 검증하는 검증부를 포함하되,

상기 제1 메시지는 상기 제1 메시지를 생성한 차량의 익명 ID, 상기 익명 ID를 이용하여 서명을 수행한 횟수, 및 안전 메시지를 포함하고, 상기 제2 메시지는 다른 차량으로부터 수신한 적어도 하나 이상의 제1 메시지의 검증 결과를 포함하는 협력 검증 장치.

청구항 2

제1항에 있어서,

차량의 실제 ID를 신뢰기관에 등록하고, 실제 ID에 대응하는 복수의 익명 ID들과 복수의 서명키들을 발급받는 셋업부를 더 포함하는 협력 검증 장치.

청구항 3

VANET 환경에서 협력 검증 장치가 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 방법에 있어서,

(1) 협력 검증 장치가 안전 메시지를 포함하는 제1 메시지를 생성하여 서명하고 전송하는 단계;

(2) 다른 차량으로부터 적어도 하나 이상의 제1 메시지들을 수신하는 단계;

(3) 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 검증 대상 제1 메시지를 선택하는 과정, 및

상기 검증 대상 제1 메시지에 포함된 제1 안전 메시지들을 검증하여 검증 결과를 생성하는 과정을 포함하는, 제1 메시지 검증 단계;

(4) 상기 검증 결과를 포함하는 제2 메시지를 생성하여 서명하고 전송하는 단계;

(5) 다른 차량으로부터 적어도 하나 이상의 제2 메시지들을 수신하는 단계; 및

(6) 다른 차량으로부터 수신한 상기 제2 메시지들 중에서 검증 대상 제2 메시지를 선택하는 과정,

상기 검증 대상 제2 메시지에 포함된 검증 결과를 이용하여, 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 상기 제1 안전 메시지로 선택하지 않고 상기 검증 대상 제2 메시지에 검증 결과가 포함되어 있는 제2 안전 메시지에 대한 검증 결과를 획득하는 과정, 및

다른 차량으로부터 수신한 상기 제1 메시지들 중에서 상기 제1 안전 메시지로 선택하지 않고 상기 검증 대상 제2 메시지에 검증 결과가 포함되어 있지 않은 제3 안전 메시지에 대한 검증을 수행하여 검증 결과를 생성하는 과정을 포함하는, 제2 메시지 검증 단계;를 포함하는 메시지 협력 검증 방법.

청구항 4

제3항에 있어서,

차량의 실제 ID를 신뢰기관에 등록하고, 신뢰기관으로부터 복수의 익명 ID 및 복수의 서명키를 발급받는 셋업

단계를 더 포함하는 메시지 협력 검증 방법.

청구항 5

제4항에 있어서,

상기 제1 메시지 및 상기 제2 메시지에 대한 서명은 상기 복수의 익명의 ID 중 어느 하나의 익명 ID 및 상기 익명 ID에 대응하는 서명키를 이용하여 서명을 수행하며,

상기 제1 메시지는 상기 안전 메시지, 상기 익명 ID, 및 상기 익명 ID가 서명에 사용된 횟수 정보를 포함하는, 메시지 협력 검증 방법.

청구항 6

제3항에 있어서,

상기 검증 대상 제1 메시지 선택 과정은, 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 미리 설정된 검증 확률에 의하여 상기 검증 대상 제1 메시지를 선택하는 것을 특징으로하고,

상기 검증 대상 제2 메시지 선택 과정은, 다른 차량으로부터 수신한 상기 제2 메시지들 중에서 미리 설정된 검증 개수에 의하여 상기 검증 대상 제2 메시지를 선택하는 것을 특징으로 하는, 메시지 협력 검증 방법.

청구항 7

제3항에 있어서,

상기 (1) 단계 내지 상기 (6) 단계를 반복하여 수행하는 메시지 협력 검증 방법.

청구항 8

제7항에 있어서,

상기 (2) 제1 메시지 수신 단계에서,

다른 차량으로부터 수신한 상기 제1 메시지들은 현재 제1 메시지 검증 시간(△ST) 동안 수신한 제1 메시지 및 직전 리포트 메시지 검증 시간(△RT) 동안 수신한 제1 메시지를 포함하는 메시지 협력 검증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 VANET 환경에서 익명 ID를 이용한 메시지 협력 검증 방법 및 장치에 관한 것으로, 특히, 수신한 안전 메시지들 중 일부를 검증하여 리포트 메시지를 생성하고, 수신한 리포트 메시지를 검증하여 나머지 안전 메시지의 검증을 수행하는 익명 ID를 이용한 메시지 협력 검증 장치 및 그 방법에 관한 것이다.

배 경 기 술

[0002] IT 기술의 발전과 함께 차량에는 다양한 통신 기술들이 접목되고 있다. 현재 자동차에는 CAN(Controller Area networks), LIN (Local Interconnect Network), FlexRay 등 다양한 제어 네트워크 기술들이 적용되고 있다. 향후에는 무인자동차 발전과 함께 자동차에 외부 네트워크 통신이 가능한 VANET (Vehicular Ad-Hoc Network) 기술이 적용될 것으로 예상되고 있다. VANET은 MANET(Mobile Ad-hoc Network)의 한 형태로, 차량에 설치된 통신 장치 OBU(On Board Units), 도로에 설치된 RSU(Road Side Unit), 그리고 애드-혹 네트워크(Ad-hoc network) 기술로 이루어져 있다. 각 차량은 자신의 위치, 속도, 방향, 시간, 감속/가속 정보, 교통 정보 등으로 이루어진 안전 메시지(Safety Message)를 주기적으로 주변의 자동차들에게 전송한다. 주기적으로 전송되는 교통상황 메시지를 통해 운전자는 주위 환경에 대한 빠른 대응이 가능하므로 안전하고 효율적인 차량 운행이 가능하다. 현재 IEEE 1609 표준인 WAVE (Wireless Access in Vehicular Environments)에 대한 표준화가 진행중이다.

[0003] VANET에서 주기적으로 전송되는 안전메시지에는 자동차의 위치정보가 포함되어 있다. 따라서 VANET 통신에서는 주기적인 위치정보 노출로 인한 불법적인 위치 추적을 방지하기 위해 익명성을 제공하는 인증 기술들이 활발히 연구되고 있다. 최근에 진행된 VANET환경에 적용할 수 있는 익명인증 기법 연구는 그룹 서명을 사용하는 인증

기법과 다수의 익명아이디를 사용하는 인증 기법으로 나누어진다.

[0004] 하지만, 그룹서명과 익명아이디를 사용하는 기법들 모두 차량이 밀집된 환경에서 가용성이 확보되지 않는다. 예를 들어 임의의 자동차의 통신 범위에 100~300대의 차량이 존재한다면, 해당 차량이 검증해야 하는 메시지는 초당 100~300개이다. 따라서 인증 효율성을 향상시킬 수 있는 일괄서명 검증 알고리즘 (Batch verification), 협력 검증 알고리즘 (Cooperative authentication) 등 다양한 기법들이 제안되고 있고, 최근에는 협력검증 알고리즘들이 제안되고 있다.

[0005] 본 발명에서는, 밀집한 환경에서 다수의 차량 간 통신 시에 보다 효율적인 메시지 검증을 위한 다수의 익명 ID 기반의 메시지 협력 검증 기법을 제안한다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는 지능형 자동차 네트워크 기술인 VANET에 적용할 수 있는 효율적이고 안전한 협력 검증 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 실시 예에 따른 VANET 환경에서 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 각각의 차량에 포함된 협력 검증 장치는 제1 메시지 생성부 및 제2 메시지 생성부를 포함하는 메시지 생성부, 생성된 메시지를 익명 ID 및 이에 대응하는 서명키를 이용하여 서명을 수행하는 메시지 서명부, 상기 메시지 생성부에서 생성한 제1 메시지 또는 제2 메시지를 다른 차량의 협력 검증 장치로 송신하고, 다른 차량의 협력 검증 장치로부터 제1 메시지 또는 제2 메시지를 수신하는 통신부, 및 상기 다른 차량의 협력 검증 장치로부터 수신한 제1 메시지 또는 제2 메시지를 검증하는 검증부를 포함하되, 상기 제1 메시지는 상기 제1 메시지를 생성한 차량의 익명 ID, 상기 익명 ID를 이용하여 서명을 수행한 횟수, 및 안전 메시지를 포함하고, 상기 제2 메시지는 다른 차량으로부터 수신한 적어도 하나 이상의 제1 메시지의 검증 결과를 포함한다.

[0008] 본 발명의 실시 예에 따른 VANET 환경에서 협력 검증 장치가 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 방법은 협력 검증 장치가 안전 메시지를 포함하는 제1 메시지를 생성하여 서명하고 전송하는 단계; 다른 차량으로부터 적어도 하나 이상의 제1 메시지들을 수신하는 단계; 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 검증 대상 제1 메시지를 선택하는 과정, 및 상기 검증 대상 제1 메시지에 포함된 제1 안전 메시지들을 검증하여 검증 결과를 생성하는 과정을 포함하는, 제1 메시지 검증 단계; 상기 검증 결과를 포함하는 제2 메시지를 생성하여 서명하고 전송하는 단계; 다른 차량으로부터 적어도 하나 이상의 제2 메시지들을 수신하는 단계; 및 다른 차량으로부터 수신한 상기 제2 메시지들 중에서 검증 대상 제2 메시지를 선택하는 과정, 상기 검증 대상 제2 메시지에 포함된 검증 결과를 이용하여, 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 제1 안전 메시지로 선택하지 않고 상기 검증 대상 제2 메시지에 검증 결과가 포함되어 있는 제2 안전 메시지에 대한 검증 결과를 획득하는 과정, 및 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 제1 안전 메시지로 선택하지 않고 상기 검증 대상 제2 메시지에 검증 결과가 포함되어 있지 않은 제3 안전 메시지에 대한 검증을 수행하여 검증 결과를 생성하는 과정을 포함하는, 제2 메시지 검증 단계;를 포함한다.

발명의 효과

[0009] 본 발명의 실시 예에 따른 익명 ID 기반의 메시지 협력 검증 방법 및 장치에 의하면, 차량이 밀집된 환경에서 효율적으로 메시지들 검증하고, 검증의 신뢰도를 향상시키는 효과가 있다.

도면의 간단한 설명

[0010] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 협력 검증 시스템의 개념도이다.

도 2는 메시지 협력 검증 장치의 기능 블럭도이다.

도 3은 본 발명의 일 실시예에 의한 리포트 메시지 구조를 도시한다.

도 4는 도 2에 도시한 메시지 협력 검증 장치에서의 메시지 협력 검증 방법을 설명하기 위한 흐름도이다.

도 5는 도 4에 도시된 도 4는 도 3에 도시된 안전 메시지 및 리포트 메시지 검증 과정을 보다 세부적으로 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0011] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0012] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0013] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0014] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0015] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0016] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0017] 도 1은 본 발명의 협력 검증 시스템(10)의 개념도이다.

[0018] 도 1을 참조하면, 협력 검증 시스템(10)은 복수의 협력 검증 장치(100)들과 신뢰기관(Trusted Authority, TA, 200)를 포함한다.

[0019] 각각의 협력 검증 장치(100)는 네트워크 망을 통하여 협력 검증 장치(100) 또는 신뢰기관(200)와 통신할 수 있다. 일 실시예에 따른 네트워크 망은, 개방형 인터넷, 폐쇄형 인트라넷을 포함한 유선 인터넷망, 이동 통신망과 연동된 무선 인터넷 통신망뿐만 아니라, 각종 데이터 통신이 가능한 컴퓨터 네트워크 등의 가능한 통신 수단을 포함하는 넓은 개념이다. 바람직하게는 각각의 협력 검증 장치(100)는 VANET 네트워크를 이용하여 다른 협력 검증 장치(100)와의 통신을 수행한다.

[0020] 도 2는 본 발명에 따른 메시지 협력 검증 장치(100)의 기능 블럭도이다.

[0021] 도 2을 참조하면, 메시지 협력 검증 장치(100)는 셋업부(110), 메시지 생성부(120), 메시지 서명부(130), 검증부(140), 통신부(170), 저장부(180), 및 제어부(190)을 포함한다.

[0022] 셋업부(110)는 제어부(190)의 제어 하에, 차량의 실제 ID를 신뢰기관(200)에 등록한 후, 복수의 익명 ID(Psedo ID, PID)들과 서명키들을 발급받는다.

[0023] 메시지 생성부(120)는 안전 메시지 생성부 및 리포트 메시지 생성부를 포함하며, 안전 메시지 생성부는 안전 메시지(Safety Message) 및 이를 포함하는 메시지를 생성할 수 있다. 안전 메시지는 각각의 차량의 위치, 속도, 방향, 시간, 감속/가속 정보, 교통 정보 등을 포함할 수 있다. 리포트 메시지 생성부는 안전 메시지 검증 결과에 대한 리포트 메시지(Report Message)를 생성할 수 있다.

[0024] 도 3은 리포트 메시지의 구조를 예시한다. 리포트 메시지는 익명 아이디, 카운터(Counter) 값, 및 검증 결과를

포함한다. 리포트 메시지에 안전 메시지를 대신하여 해당 메시지의 카운터 값을 포함함으로써 리포트 메시지의 크기를 줄일 수 있다.

[0025] 메시지 서명부(130)는 제어부(190)의 제어 하에, 상기 메시지 생성부(120)에서 생성된 메시지를 셋업부(110)에서 발급된 임의의 익명 ID 및 이에 대응하는 서명키를 이용하여 서명을 수행할 수 있다. 서명되는 메시지에는 해당 익명 아이디가 서명에 사용된 횟수(Counter)를 포함한다.

[0026] 검증부(140)는 제어부(190)의 제어 하에, 다른 차량으로부터 수신한 안전 메시지의 검증을 수행한다. 또한, 다른 차량으로부터 수신한 리포트 메시지를 이용하여 안전 메시지의 검증을 수행할 수 있다. 자세한 검증 방법은 아래의 협력 검증 방법에서 상세히 설명한다.

[0027] 통신부(170)는 제어부(190)의 제어 하에, 협력 검증 장치를 포함하는 다른 차량과 통신을 수행할 수 있다. 또한, 네트워크 망을 이용하여 신뢰기관(TA)과 통신을 수행할 수 있다.

[0028] 저장부(180)는 저장부(180)는 프로그램 저장부와 데이터 저장부를 포함할 수 있으며, 상기 프로그램 저장부에는 협력 검증 장치(100)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 저장부에는 상기 프로그램들을 수행하는 과정 중에 발생되는 데이터들이 저장될 수 있다.

[0029] 제어부(190)는 협력 검증 장치(100)의 전반적인 동작을 제어한다. 즉, 셋어업부(110), 메시지 생성부(120), 메시지 서명부(130), 검증부(140), 통신부(170) 및 저장부(180)의 동작을 제어할 수 있다.

[0030] 도 3은 본 발명의 일 실시예에 따른 메시지 협력 검증 장치에서 안전 메시지의 협력 검증을 수행하는 방법을 설명하기 위한 흐름도이다.

[0031] 먼저, 안전 메시지의 생성에 앞서서, 각 자동차의 메시지 협력 검증 장치(100)는 셋업(Set-up) 단계를 수행한다(S100). 각 자동차의 메시지 협력 검증 장치(100)는 각 자동차가 VANET 통신에 사용할 다수의 익명 ID(PID)들과 이에 부합하는 서명 키들을 발급받는다. 구체적으로, 각 차량은 자신의 실제 ID를 신뢰기관(TA, 200)에 등록한 후, 복수의 익명 ID들과 서명키들을 발급받고, 신뢰기관(TA, 200)은 자신이 발급한 정보들을 안전한 저장소에 저장한다.

[0032] 다음, 안전 메시지의 협력 검증에 앞서서, 각 차량의 메시지 협력 검증 장치(100)는 안전 메시지(Safety Message)를 생성하여 다른 차량 또는 다른 차량의 협력 검증 장치로 전송한다(S200). 구체적으로, 각각의 차량은 각각의 차량의 위치, 속도, 방향, 시간, 감속/가속 정보, 교통 정보 등을 포함하는 안전 메세지를 생성하고, 안전메시지, 익명 아이디, 및 카운터 값을 포함하는 메시지(이하, '제1 메시지'라고 함)를 아래와 같이 생성한다.

[0033] $$Message = PID, Satey\,Message, Counter$$

[0034] 생성된 제1 메시지는 셋업 단계에서 발급된 임의의 익명 ID와 이에 대응하는 서명키를 이용하여 서명한다. 서명되는 메시지에는 해당 익명 아이디가 서명에 사용된 횟수(Counter)를 포함한다.

[0035] 다음, 각 차량은 메시지 협력 검증 장치(100)는 아래와 같이 안전 메시지를 포함하는 제1 메시지와 제1 메시지의 서명 값을 주변의 차량(또는 차량의 메시지 협력 검증 장치)들에게 전송한다.

[0036] $$Message, Sign_{PID}(Message)$$

[0037] 여기서, $Sign_{PID}()$는 PID를 사용하는 아이디(ID) 기반 서명 알고리즘 함수를 의미한다.

[0038] 다음, 각 차량의 메시지 협력 검증 장치(100)들은 협력 검증을 수행한다(S310-S600). 주변의 차량들로부터 주기적으로 발생하는 안전 메시지를 수신한 차량은 주변의 차량들과 서로 협력하여 서명 검증을 수행한다. 협력 검증 단계는 안전 메시지를 포함하는 제1 메시지의 검증 단계와 리포트 메시지를 의미하는 제2 메시지의 검증 단계로 나누어진다. 각 검증 단계는 미리 설정된 시간동안 주기적으로 수행될 수 있다.

[0039] 먼저, 제1 메시지 검증 단계를 상세히 설명한다.

[0040] 차량의 협력 검증 장치(100)는 주변 차량으로부터 안전 메시지, 해당 차량의 익명 ID(PID), 및 카운터를 포함하는 제1 메시지를 수신(S310)하고, 수신한 제1 메시지 중에서 검증 대상 제1 메시지를 선택한다(S330). 카운터는 익명 ID(PID)가 서명에 사용된 횟수를 의미한다.

[0041] 관리자에 의하여 미리 설정된 검증 확률(P_v)로 검증 대상 안전 메시지(이하, '제1 안전 메시지'라 함)를 포함하는 제1 메시지를 선택한다. 이때, 안전 메시지 검증 단계 직전에 리포트 메시지 검증 단계를 수행한 경우, 안전 메시지 검증 단계 이전의 리포트 메시지 검증 시간(△RT) 동안 발생한 안전 메시지 및 현재의 안전 메시지 검증 시간(△ST) 동안 발생한 안전 메시지들 중에서 제1 안전 메시지를 선택한다. 검증 대상 안전 메시지(제1 안전 메시지)를 선택한 협력 검증 장치(100)는 메시지 검증을 수행(S350)하고, 검증 결과를 저장한다. 모든 차량의 협력 검증 장치(100)는 안전 메시지 검증 시간(△ST) 동안 위의 과정을 반복하여 수신한 안전 메시지 중 제1 안전 메시지를 검증한다.

[0042] 다음, 제1 안전 메시지 검증이 완료되면, 협력 검증 장치(100)는 리포트 메시지를 생성하여 전송한다(S400). 구체적으로, 안전 메시지 검증 시간(△ST)이 지나면, 모든 차량의 협력 검증 장치(100)는 안전 메시지 검증 시간(△ST) 동안 검증하여 저장한 검증 결과에 대한 리포트 메시지를 생성한 후, 해당 리포트 메시지를 서명하여 주변 차량(또는 주변 차량의 협력 검증 장치)들에게 리포트 메시지(이하, '제2 메시지'라고도 함)를 전송한다.

$$Report\,Message\,,\,Sign_{PID}(Report\,Message)$$

$$Report\,Message = \begin{matrix}(PID_x,\ Counter_x,\ Valid)\\ (PID_y,\ Counter_y,\ Invalid)\\ \cdots\end{matrix}$$

[0043]

[0044] 이하, 제2 메시지 검증 단계에 대하여 상세히 설명한다.

[0045] 차량의 협력 검증 장치(100)는 주변 차량으로부터 제2 메시지를 수신(S510)하고, 수신한 제2 메시지 중에서 검증 대상 제2 메시지를 선택한다(S530). 구체적으로, 모든 차량의 협력 검증 장치(100)는 리포트 메시지 검증 시간(△RT) 동안 주변 노드들로부터 수신한 리포트 메시지(제2 메시지)들 중 N_R개의 리포트 메시지(제2 메시지)를 선택하여 검증한다. N_R개의 리포트 메시지들로부터 자신이 제1 메시지 검증 단계에서 선택하지 않았던 안전 메시지(이하, '제2 안전 메시지'라고 함)들에 대한 검증을 처리한다(S550).

[0046] 다음, 제1 메시지 검증 단계에서 선택되지 않았던 안전 메시지 중 N_R 개의 리포트 메시지들로 확인되지 않은 나머지 메시지(이하, '제3 안전 메시지'라고 함)들에 대한 검증을 수행한다. 바람직하게는, 남은 리포트 메시지 검증 시간(△RT)동안 제3 안전 메시지에 대한 검증을 수행한다.

[0047] 효율성 향상을 위해 리포트 메시지 검증 시간(△RT) 동안 발생한 안전메시지들은 리포트 메시지 검증 시간(△RT) 직후에 진행되는 안전 메시지 검증 시간(△ST) 동안에 처리한다.

[0048] 도 5는 도 4에 도시된 도 4는 도 3에 도시된 안전 메시지 및 리포트 메시지 검증 과정을 보다 세부적으로 도시한 도면이다.

[0049] 협력 검증 장치(100)는 직전 리포트 메시지 검증 시간(△RT) 및 현재 안전 메시지 검증 시간(△ST) 동안 수신한 메시지(예를 들어, SM1)에 중에서 미리 설정된 검증 확률(P_v)로 검증 대상 안전 메시지(제1 안전 메시지)를 선택하여 현재 안전 메시지 검증 시간(△RT) 동안 제1 안전 메시지 검증을 수행하고, 이에 따른 리포트 메시지(예를 들어, RM1)를 생성하여 전송한다.

[0050] 다음, 협력 검증 장치(100)는 수신한 리포트 메시지(예를 들어, RM1) 중 N_R개의 리포트 메시지를 선택하여 검증한다. N_R개의 리포트 메시지에 포함된 검증 결과를 이용하여, 해당 협력 검증 장치(100)가 직전 리포트 메시지 검증 시간(△RT) 및 현재 안전 메시지 검증 시간(△ST) 동안 수신한 메시지(예를 들어, SM1)들 중에서 제1 안전 메시지로 선택되지 않았던 안전 메시지 중 해당 안전 메시지의 검증 결과가 상기 N_R개의 리포트 메시지에 포함되어 있는 메시지(이하, '제2 안전 메시지'라고 함)들에 대한 검증을 처리한다.

[0051] 또한, 직전 리포트 메시지 검증 시간(△RT) 및 현재 안전 메시지 검증 시간(△ST) 동안 수신한 메시지(예를 들어, SM1)들 중에서 제1 안전 메시지 및 제2 안전 메시지를 제외한 나머지 메시지(제3 안전 메시지)에 대한 검증을 남은 리포트 메시지 검증 시간(△RT)동안 수행한다.

[0052] 상술한 VANET 환경에서 협력 검증 장치가 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검

증을 수행하는 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0053] 구체적으로, 기록매체에 저장되며 익명 ID를 이용하여 복수의 차량에서 발생하는 안전 메시지의 협력 검증을 수행하는 프로그램으로서, 상기 프로그램은 컴퓨팅 시스템에서 실행되는 차량으로부터 적어도 안전 메시지를 포함하는 제1 메시지들을 수신하는 명령어 세트, 다른 차량으로부터 수신한 상기 제1 메시지들 중에서 검증 대상 제1 메시지를 선택하여 검증하는 제1 메시지 검증 명령어 세트, 상기 검증 결과를 포함하는 제2 메시지를 생성하여 서명하고 전송하는 명령어 세트, 다른 차량으로부터 적어도 하나 이상의 제2 메시지들을 수신하는 명령어 세트, 및 다른 차량으로부터 수신한 상기 제2 메시지들 중에서 검증 대상 제2 메시지를 선택하고 선택한 제2 메시지에 포함된 검증 결과를 이용하여 검증을 수행하는 제2 메시지 검증 명령어 세트를 포함할 수 있다.

[0054] 상기 메시지의 협력 검증 프로그램은 상기 기록매체에 저장되며, 상기 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)와 같은 저장매체를 포함한다. 또한, 상기 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 명령어 세트가 저장되고 실행될 수 있다.

[0055] 본 발명에서 개시된 블록도들은 본 발명의 원리들을 구현하기 위한 회로를 개념적으로 표현한 형태라고 당업자에게 해석될 수 있을 것이다. 유사하게, 임의의 흐름 차트, 흐름도, 상태 전이도, 의사코드 등은 컴퓨터 판독가능 매체에서 실질적으로 표현되어, 컴퓨터 또는 프로세서가 명시적으로 도시되든지 아니든지 간에 이러한 컴퓨터 또는 프로세서에 의해 실행될 수 있는 다양한 프로세스를 나타낸다는 것이 당업자에게 인식될 것이다.

[0056] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

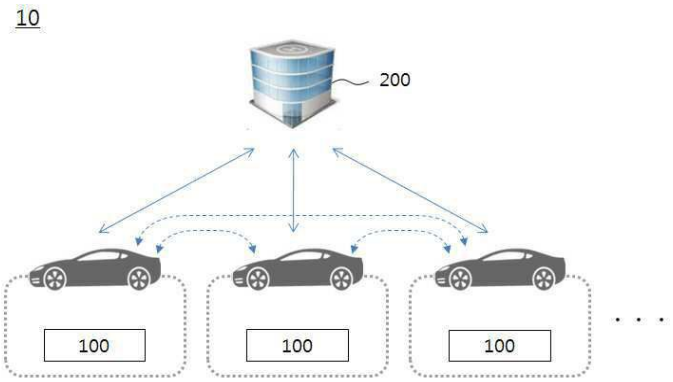
부호의 설명

[0057] 10 : 협력 검증 시스템

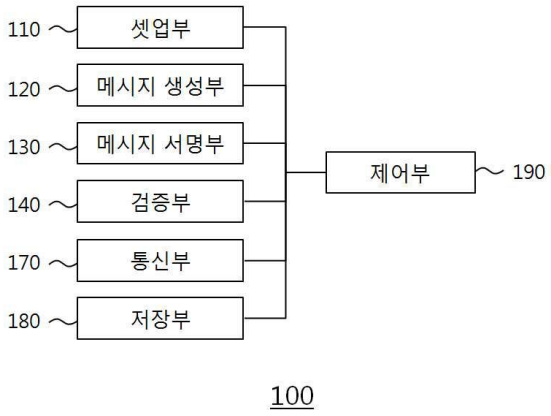
100 : 협력 검증 장치 200 : 신뢰기관

도면

도면1



도면2

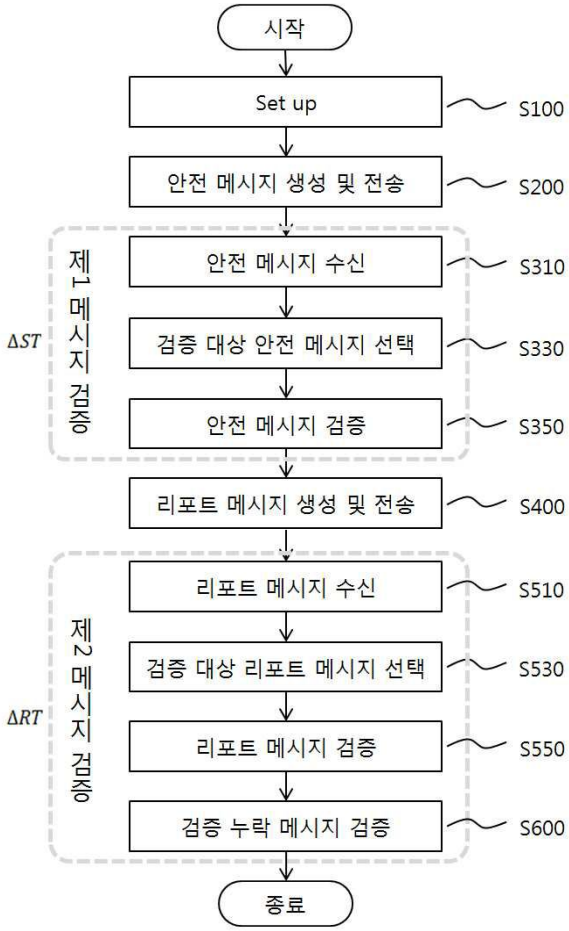


도면3

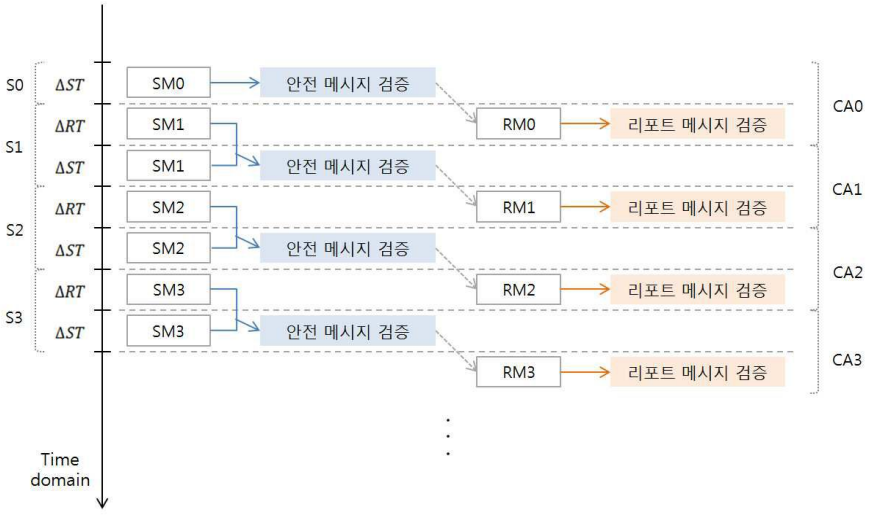
Report Message

익명 ID	Counter	검증 결과
$Pseudo\ ID_x$	$Counter_x$	$Valid$
$Pseudo\ ID_y$	$Counter_y$	$Valid$
$Pseudo\ ID_z$	$Counter_z$	$Invalid$
...	...	...

도면4


시작
Set up
S100
안전 메시지 생성 및 전송
S200
제1메시지검증
ΔST
안전 메시지 수신
S310
검증 대상 안전 메시지 선택
S330
안전 메시지 검증
S350
리포트 메시지 생성 및 전송
S400
제2메시지검증
ΔRT
리포트 메시지 수신
S510
검증 대상 리포트 메시지 선택
S530
리포트 메시지 검증
S550
검증 누락 메시지 검증
S600
종료

도면5


S0
S1
S2
S3
ΔST
ΔRT
SM0
SM1
SM2
SM3
안전 메시지 검증
RM0
RM1
RM2
RM3
리포트 메시지 검증
CA0
CA1
CA2
CA3
Time domain