



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0063209
(43) 공개일자 2019년06월07일

(51) 국제특허분류(Int. Cl.)
B60W 50/02 (2006.01) B60R 16/023 (2006.01)
B60R 16/03 (2006.01) G07C 5/00 (2006.01)
G07C 5/02 (2006.01) G07C 5/08 (2006.01)

(52) CPC특허분류
B60W 50/0205 (2013.01)
B60R 16/023 (2013.01)

(21) 출원번호 10-2017-0162129

(22) 출원일자 2017년11월29일

심사청구일자 2017년11월29일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

서은비

경기도 김포시 고촌읍 신곡리 48, 504동 1103

이현승

경기도 고양시 덕양구 화신로 291, 1011동 1502호
(화정동, 별빛마을10단지아파트)

(뒷면에 계속)

(74) 대리인

김동용, 김홍석

전체 청구항 수 : 총 9 항

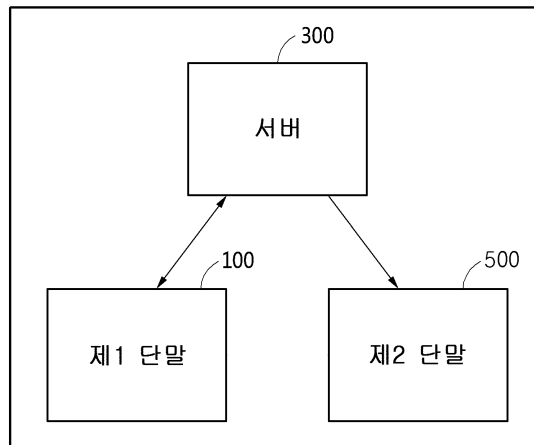
(54) 발명의 명칭 차량의 상태 검증과 이상 징후 탐지 장치 및 이를 포함하는 시스템

(57) 요약

차량의 이상 징후를 탐지하거나 차량의 상태 이상을 검증하는 탐지 장치가 개시된다. 상기 탐지 장치는 차량에 탑재된 제1 단말로부터 복수의 CAN(Controller Area Network) 메시지들을 수신하는 수신부, 상기 복수의 CAN 메시지들을 이용하여 상기 차량의 이상 징후 유무를 판단하는 이상 징후 탐지부 및 상기 이상 징후 탐지부의 판단 결과를 제2 단말로 송신하는 송신부를 포함하고, 상기 이상 징후 탐지부는 상기 복수의 CAN 메시지들 중 제1 그룹의 CAN 메시지들의 CAN ID 엔트로피를 계산하고, 계산된 엔트로피가 미리 정해진 범위를 벗어나는 경우 이상 징후가 발생한 것으로 판단한다..

대표도 - 도1

10



(52) CPC특허분류

B60R 16/0315 (2013.01)

G07C 5/008 (2013.01)

G07C 5/02 (2013.01)

G07C 5/0808 (2013.01)

(72) 발명자

송현민

서울특별시 성북구 안암로9가길 87-6 (안암동5가)

정성훈

서울특별시 동대문구 고미술로 71, 505호

강태운

충청북도 청주시 서원구 창신로 7-7, 3층

강수인

대전광역시 유성구 반석동로 82, 807동 1902호

김휘강

서울특별시 서초구 우면동 네이처힐4단지 404동 302호

이 발명을 지원한 국가연구개발사업

과제고유번호 1711054966

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 ICT융합산업원천기술개발사업

연구과제명 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2017.01.01 ~ 2017.12.31

명세서

청구범위

청구항 1

차량에 탑재된 제1 단말로부터 복수의 CAN(Controller Area Network) 메시지들을 수신하는 수신부;
상기 복수의 CAN 메시지들을 이용하여 상기 차량의 이상 징후 유무를 판단하는 이상 징후 탐지부; 및
상기 이상 징후 탐지부의 판단 결과를 제2 단말로 송신하는 송신부를 포함하고,
상기 이상 징후 탐지부는 상기 복수의 CAN 메시지들 중 제1 그룹의 CAN 메시지들의 CAN ID 엔트로피(H')를 계산하고, 계산된 엔트로피(H')가 미리 정해진 범위를 벗어나는 경우 이상 징후가 발생한 것으로 판단하는,
탐지 장치.

청구항 2

제1항에 있어서,
상기 이상 징후 탐지부는 수학적식을 이용하여 상기 CAN ID 엔트로피(H')를 계산하고,

$$H' = - \sum_{i=1}^n p_i \log p_i$$

상기 수학적식은 이고,

상기 n 은 상기 제1 그룹의 CAN 메시지들에 포함된 CAN ID의 개수를 의미하고, 상기 p_i 는 상기 n 개의 CAN ID 중 i 번째 CAN ID의 분포 확률을 의미하는,
탐지 장치.

청구항 3

제2항에 있어서,
상기 이상 징후는 상기 차량을 대상으로 한 제밍(jamming) 공격 또는 스푸핑(spoofing) 공격을 의미하는,
탐지 장치.

청구항 4

제1항에 있어서,
상기 탐지 장치는 상태 검증부를 더 포함하고,
상기 수신부는 상기 차량으로부터 상기 차량의 상태 정보를 더 수신하고,
상기 상태 검증부는 상기 상태 정보로부터 엔진 rpm(revolutions per minute), 엔진 오일 온도(engine oil temperature), 차량 속도(vehicle speed) 및 냉각수 온도(engine coolant temperature) 중 적어도 하나를 포함하는 차량 데이터를 생성하고, 생성된 차량 데이터가 미리 정해진 제2 범위를 벗어나는 경우 상기 차량의 상태에 이상이 생긴 것으로 판단하는,

탐지 장치.

청구항 5

제4항에 있어서,

상기 송신부는 상기 상태 검증부의 판단 결과를 상기 제2 단말로 송신하는,

탐지 장치.

청구항 6

제1항에 있어서,

상기 제1 그룹의 CAN 메시지들은 미리 정해진 시간 구간 동안에 생성되거나 상기 미리 정해진 시간 구간 동안에 수신된 CAN 메시지들인,

탐지 장치.

청구항 7

제1항에 기재된 탐지 장치;

상기 제1 단말; 및

상기 제2 단말을 포함하는 탐지 시스템.

청구항 8

제7항에 있어서,

상기 제1 단말은,

상기 차량의 CAN 버스를 통해 브로드캐스트되는 상기 복수의 CAN 메시지들을 수집하는 수집부; 및

상기 복수의 CAN 메시지들을 상기 서버로 송신하는 송신부를 포함하는,

탐지 시스템.

청구항 9

제4항에 기재된 탐지 장치, 상기 제1 단말 및 상기 제2 단말을 포함하는 탐지 시스템에 있어서,

상기 제1 단말은,

상기 차량의 CAN 버스를 통해 브로드캐스트되는 상기 복수의 CAN 메시지들과 상기 차량의 상태 정보를 수집하는 수집부; 및

상기 복수의 CAN 메시지들과 상기 상태 정보를 상기 서버로 송신하는 송신부를 포함하고,

상기 수집부는 상기 차량의 OBD-2(On-board diagnostics-2) 단자를 통해 송신한 질의 메시지에 대한 응답으로 상기 상태 정보를 수신하는,

탐지 시스템.

발명의 설명

기술분야

- [0001] 본 발명은 다종 차량을 대상으로 낮은 성능이 차량 내부 장치를 대신하여 원격에서 차량 상태를 검증하고 신속한 이상 징후를 탐지하기 위한 방법에 관한 것이다.

배경기술

- [0003] 사물 인터넷(Internet of Things, IoT) 기술의 발전과 함께 운전자의 편의성을 증대시키는 자율 주행 자동차의 시장이 확대되고 있으며, 이에 따라 보안 기술은 자율 주행 자동차의 사용화를 위한 선결 조건이 되었다. NHATSA(National Highway Traffic Safety Administration, 미국 고속도로 교통안전국)는 Automotive Electronic Control and Security에서 차량의 전자 시스템과 관련된 안전 표준의 필요성을 검토하고 있으며, 이를 위한 침입 탐지의 연구를 강조하고 있다.
- [0004] 최근 출시된 자율 주행 기반의 자동차는 크게 센싱, 신호 처리(인지), 판단, 제어 프로세스로 구성된다. 차량 외부에서는 ADAS(Advanced Driver Assistance Systems) 센서 및 무선 통신을 통해 차량 주변 정보를 제공받으며, 차량 내부의 판단 프로세스는 위험 상황 유무 등의 상황 판단에 따라 주행 전략을 결정한다. 차량 내부의 제어 시스템에서는 판단 프로세스에 의해 결정된 주행 전략에 따라 최종적으로 차량을 제어하게 된다.
- [0005] 그러나, 자율 주행 자동차의 최종 제어권은 내부 네트워크의 ECU(Electronic Control Unit)에 있으므로 차량 내부의 통신 네트워크를 악의적으로 조작하는 등의 공격으로부터 취약한 실정이다. V2X(Vehicle to Everything) 등의 외부 통신 기술 및 VANET(Vehicular ad hoc network) 등의 개방형 네트워크의 도입으로 인해 차량 내부 네트워크의 접근이 용이해 졌으며, 이는 차량이 최종 제어권을 갖고 있는 내부 시스템을 악의적으로 조작함으로써 운전자의 안전에 영향을 미치는 공격이 수행될 수 있다.
- [0006] 또한, 자동차의 외부 및 내부 장치 간 효율적인 통신을 위해 수많은 전자 제어 시스템 및 소프트웨어가 탑재되고 있으며, 이에 따라 차량 내부 시스템의 복잡성은 지속적으로 증가하고 있다. 차량 내부 전자 장치의 컴퓨팅 성능은 이러한 다수의 전자 시스템을 포괄하기에 한계가 있으며, 따라서 Compromised ECU 장치에 적용 가능한 높은 컴퓨팅 성능의 이상 징후 탐지 모듈의 연구가 요구된다.
- [0007] 최근 출시되는 차량에는 수많은 전자 제어 시스템 및 소프트웨어, 그리고 차량 주변 정보를 인지하기 위한 다양한 ADAS 센서 모듈이 탑재되어 있다. 차량 내부 네트워크 통신은 CAN(Controller Area Network), FlexRay, LIN(Local Interconnect Network) 프로토콜을 통해 이루어지며, 공격자가 해당 프로토콜 버스(bus)에 진입 가능할 경우 차량 제어를 통해 운전자의 안전에 직결되는 공격이 발생할 수 있다.
- [0008] 이에 본 발명에서는 원격에서 신속한 이상 징후 탐지가 가능하며, 수집된 여러 차종의 정보 데이터를 쉽게 비교, 분석할 수 있으므로 차량 침입 탐지 기술 연구에 활용 가능할 것으로 전망된다.

선행기술문헌

특허문헌

- [0010] (특허문헌 0001) 미합중국 등록특허 제9,703,955호
(특허문헌 0002) 대한민국 공개특허 제2016-0071980호
(특허문헌 0003) 대한민국 등록특허 제1789734호

발명의 내용

해결하려는 과제

- [0011] 최근 출시된 자동차는 기존의 ADAS 시스템을 조합하거나 개선하여 발전하므로 복잡한 형태의 내부 시스템 구조를 갖는다. 따라서, 이상 징후 탐지 방법이 한 차종에 국한된다면 해당 차종의 전자 장치에 의존적인 방법이 될

수 있다.

[0012] 현재 상용화된 차량 내부의 ECU 장치는 이상 징후 탐지와 같은 대용량의 연산을 처리하기에는 부족한 성능을 갖는다. 즉, 현재 고도화되고 있는 차량의 다양한 내부 장치들을 차량에서 제어하기에는 현실적인 어려움이 따른다.

[0013] 본 발명은 상용화된 다양한 차종이 통신 네트워크 및 전자 장치 기술에 적합한 침입 탐지 방법과 장치를 제안하여, 차량의 내부 시스템에 대한 공격을 신속히 탐지할 수 있는 방법을 제공하고자 한다.

과제의 해결 수단

[0015] 본 발명의 실시 예에 따른 탐지 장치는 차량에 탑재된 제1 단말로부터 복수의 CAN 메시지들을 수신하는 수신부, 상기 복수의 CAN 메시지들을 이용하여 상기 차량의 이상 징후 유무를 판단하는 이상 징후 탐지부, 및 상기 이상 징후 탐지부의 판단 결과를 제2 단말로 송신하는 송신부를 포함하고, 상기 이상 징후 탐지부는 상기 복수의 CAN 메시지들 중 제1 그룹의 CAN 메시지들의 CAN ID 엔트로피를 계산하고, 계산된 엔트로피가 미리 정해진 범위를 벗어나는 경우 이상 징후가 발생한 것으로 판단한다.

[0016] 또한, 본 발명의 실시 예에 따른 탐지 시스템은 상기 탐지 장치, 상기 제1 단말 및 상기 제2 단말을 포함한다.

발명의 효과

[0018] 본 발명의 실시 예에 의할 경우, 원격에서 차량의 이상 징후를 신속하게 탐지 가능하며, 수집된 여러 차종의 정보 데이터를 쉽게 비교, 분석할 수 있는 효과가 있다.

도면의 간단한 설명

[0020] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 시스템을 도시한다.

도 2는 도 1에 도시된 제1 단말의 기능 블록도이다.

도 3은 도 1에 도시된 서버의 기능 블록도이다.

도 4는 도 3에 도시된 수신부에 의해 수신된 CAN 메시지들 또는 도 2에 도시된 수집부에 의해 수집된 CAN 메시지들의 예시를 도시한다.

도 5는 도 3에 도시된 수신부에 의해 수신된 상태 정보(또는 상태 검증부에 의해 생성된 차량 데이터) 또는 도 2에 도시된 수집부에 의해 수집된 상태 정보의 예시를 도시한다.

도 6은 도 1에 도시된 제2 단말의 기능 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 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.

[0022] 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.

[0023] 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 명명

될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

- [0024] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0025] 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.
- [0026] 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.
- [0027] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.
- [0029] 도 1은 본 발명의 일 실시 예에 따른 시스템을 도시한다.
- [0030] 차량 시스템, 탐지 시스템, 상태 검증 및 이상 징후 탐지 시스템, 원격 차량 상태 검증 및 이상 징후 탐지 시스템 등으로 명명될 수도 있는 시스템(10)은 제1 단말(100), 서버(300) 및 제2 단말(500)을 포함한다.
- [0031] 제1 단말(100)은 차량 내에 설치되어 차량 내부 네트워크 상에서 전송되는 메시지들(예컨대, CAN(Controller Area Network) 메시지들) 및/또는 상태 정보를 수집하고, 수집된 CAN 메시지들 및/또는 상태 정보를 서버(300)로 송신할 수 있다.
- [0032] 서버(300)는 제1 단말(100)로부터 메시지들을 수신하고, 수신된 메시지들을 이용하여 차량의 이상 징후 유무를 판단할 수 있다. 또한, 서버(300)는 제1 단말(100)로부터 상태 정보를 수신하고, 수신된 상태 정보를 이용하여 차량의 상태를 검증(즉, 차량의 상태의 이상 유무를 판단)할 수 있다. 서버(300)의 판단 결과는 제2 단말(500)로 송신될 수 있다.
- [0033] 제2 단말(500)은 서버(300)로부터 판단 결과를 수신하고, 수신된 판단 결과를 소정의 표시부를 통하여 표시할 수 있다. 제2 단말(500)은 차량 운전자의 휴대용 단말일 수 있으나, 본 발명이 이에 제한되는 것은 아니다. 실시 예에 따라 제2 단말은 제1 단말(100)을 의미할 수도 있다.
- [0035] 도 2는 도 1에 도시된 제1 단말의 기능 블록도이다.
- [0036] 도 1과 도 2를 참조하면, 제1 단말(100)은 수집부(110)와 송신부(130)를 포함한다. 실시 예에 따라 제1 단말(100)은 저장부(150)를 더 포함할 수도 있다.
- [0037] 수집부(110)는 차량 네트워크 내에서 전송되는 복수의 메시지들을 수집할 수 있다. 예컨대, 수집부(110)는 차량의 CAN에서 브로드캐스트되는 복수의 CAN 메시지들을 수집할 수 있다. 이를 위해 수집부(110)는 CAN 버스 또는 BCM(Body Control Unit)에 연결되어 있거나 OBD-2(On-board diagnostics-2) 단자와 연결되어 있을 수 있다. 실시 예에 따라, 수집부(110)는 CAN 버스, BCM 또는 OBD-2 단자에 연결된 인터페이스부를 포함할 수도 있다. 수집부(110)에 의해 수집된 복수의 CAN 메시지들은 저장부(150)에 적어도 일시적으로 저장될 수 있다.
- [0038] 또한, 수집부(110)는 차량의 상태 정보를 수집하고 수집된 상태 정보를 저장부(150)에 저장할 수도 있다. 예컨대, 수집부(110)는 OBD-2 단자를 통해 차량의 현재 상태에 관한 질의(쿼리) 메시지를 송신하고, 차량으로부터

상태 정보를 수신할 수 있다.

[0040] 송신부(130)는 수집부(110)에 의해 수집된 복수의 메시지들 및/또는 상태 정보 또는 저장부(150)에 저장되어 있는 복수의 메시지들 및/또는 상태 정보를 서버(300)로 송신할 수 있다. 이때, 무선 통신망이 이용될 수 있으나, 본 발명이 이에 제한되는 것은 아니다.

[0042] 저장부(150)에는 수집부(110)에 의해 수집된 복수의 메시지들 및/또는 차량의 상태 정보가 적어도 일시적으로 저장될 수 있다.

[0044] 도 3은 도 1에 도시된 서버의 기능 블록도이다.

[0045] 도 3을 참조하면, 탐지 장치, 탐지 서버 등으로 명명될 수도 있는 서버(300)는 수신부(310), 이상 징후 탐지부(330) 및 송신부(370)를 포함한다. 실시 예에 따라, 서버(300)는 상태 검증부(350) 및 저장부(390) 중 적어도 하나를 더 포함할 수도 있다.

[0046] 수신부(310)는 제1 단말(100)로부터 CAN 메시지들 및/또는 차량 상태 정보를 수신하고, 수신된 CAN 메시지들 및/또는 차량 상태 정보는 저장부(390)에 저장될 수 있다. 수신부(310)에 의해 수신된 CAN 메시지들 또는 수집부(110)에 의해 수집된 CAN 메시지들의 예시는 도 4에 도시되어 있다. 도 4를 참조하면, CAN 메시지에는 메시지 생성 시간을 나타내는 타임스탬프(timestamp), 메시지의 우선 순위 및 식별을 위한 CAN ID, 및 데이터 정보 등을 포함하는 CAN 메시지 필드 등이 포함될 수 있다.

[0048] 이상 징후 탐지부(330)는 수신부(310)에 의해 수신된 CAN 메시지들 또는 저장부(390)에 저장되어 있는 CAN 메시지들을 이용하여 차량의 이상 여부(예컨대, 제밍(jamming) 공격이나 스푸핑(spoofing) 공격과 같이 차량을 상대로 한 악의적인 공격 발생 여부)를 판단할 수 있다. 예컨대, 이상 징후 탐지부(330)는 엔트로피 기반의 이상 징후 탐지 동작을 수행할 수 있다. 구체적으로, 이상 징후 탐지부(330)는 Shannon's diversity index 수식인 수학식 1을 이용하여 CAN ID의 엔트로피(H')를 계산하고, 계산된 엔트로피(H')에 기초하여 차량의 이상 여부를 결정(또는 탐지)할 수 있다. 즉, 이상 징후 탐지부(330)는 계산된 엔트로피(H')가 미리 정해진 범위(정상 범위)를 벗어나는 경우(초과하거나 미만되는 경우) 차량에 이상이 발생한 것으로 판단할 수 있다. 기존에 발견되지 않았던 많은 종류의 CAN ID가 유입될 경우 다양성 지수가 상승하여 엔트로피 값이 증가하며, 특정 CAN ID가 유입될 경우 다양성 지수가 급격하게 낮아지기 때문에, 이를 반영하면 차량의 이상 여부를 판단할 수 있다.

수학식 1

$$H' = - \sum_{i=1}^n p_i \log p_i$$

[0049]

[0050] 수학식 1에서 n 은 미리 정해진 시간 구간 동안에 출현한 CAN ID의 개수를 의미하고, p_i 는 상기 미리 정해진 시간 구간 동안에 n 개의 CAN ID 중 i 번째 CAN ID의 분포 확률(또는, 상기 미리 정해진 시간 구간 동안에 발생한 CAN 메시지의 개수 중 상기 i 번째 CAN ID를 포함하는 CAN 메시지의 비율)을 의미할 수 있다.

[0051] CAN ID의 엔트로피(H')는 주기적으로 계산될 수 있고, 상기 미리 정해진 시간 구간은 계산되는 주기와는 다를 수 있다. 예컨대, CAN ID 엔트로피(H')는 매초(또는 매 2초)마다 계산될 수 있고, 계산에 이용되는 CAN 메시지들은 2초(또는 1초) 동안 생성되거나 수신된 CAN 메시지들일 수 있다. 다른 예로, CAN ID 엔트로피(H')는

매초마다 계산될 수 있고, 계산에 이용되는 CAN 메시지들은 1초 동안 생성되거나 수신된 CAN 메시지들일 수도 있다.

[0053] 상태 검증부(350)는 차량으로부터 수신된 차량의 상태 정보를 이용하여 차량 데이터를 생성할 수 있다. 차량으로부터 수신된 차량의 상태 정보는 엔진 RPM 등에 관한 직접적인 수치를 제공하지 않기 때문에 추가적인 가공을 통해 엔진 RPM 등, 즉 차량 데이터를 생성할 수 있다. 상태 검증부(350)에 의해 생성 가능한 차량 데이터는 엔진 RPM(engine rpm), 엔진 오일 온도(engine oil temperature) 미션 오일 온도(transmission oil temperature), 차량 속도(vehicle speed), 냉각수 온도(engine coolant temperature) 중 적어도 하나를 포함할 수 있다. 수신부(310)에 의해 수신된 상태 정보(또는 상태 검증부(350)에 의해 생성된 차량 데이터) 또는 수집부(110)에 의해 수집된 상태 정보의 예시는 도 5에 도시되어 있다.

[0055] 또한, 상태 검증부(350)는 생성된 차량 데이터 각각을 미리 정해진 범위(정상 범위)와 비교하여 미리 정해진 범위를 벗어나는 경우(초과하거나 미만되는 경우), 예컨대, 상태 검증부(350)는 엔진 rpm(revolutions per minute)이 0~6000의 범위를 벗어나는 경우, 냉각수 온도가 0~110℃의 범위를 벗어나는 경우, 차량의 속도가 -20~110m/s의 범위를 벗어나는 경우 등을 차량의 상태에 이상이 생긴 것으로 결정할 수 있다.

[0057] 송신부(370)는 이상 징후 탐지부(330)의 탐지 결과(차량의 이상 여부 또는 차량을 상대로 한 악의적인 공격 발생 여부) 및/또는 상태 검증부(350)의 검증 결과(차량 상태의 이상 여부)를 제2 단말기(500)로 송신할 수 있다.

[0059] 저장부(390)에는 수신부(310)에 의해 수신된 차량 메시지들(CAN 메시지들), 차량의 상태 정보, 이상 징후 탐지부(330)의 탐지 결과, 상태 검증부(350)의 검증 결과 등이 저장될 수 있다.

[0061] 도 6은 도 1에 도시된 제2 단말의 기능 블록도이다.

[0062] 차량의 운전자에 의해 휴대되는 이동 단말이거나 차량에 탑재된 단말일 수 있는 제2 단말(500)은 수신부(510)와 표시부(530)를 포함한다.

[0063] 수신부(510)는 서버(300)로부터 차량의 이상 여부에 대한 정보, 즉 이상 징후 판단부(330)의 판단 결과를 수신할 수 있다.

[0065] 표시부(530)는 수신부(510)에 의해 수신된 차량의 이상 여부를 디스플레이할 수 있다. 상술한 바와 같이, 차량의 이상 여부는 표시부에 디스플레이되어 운전자에게 신속히 전달되므로, 신속한 대응이 가능하다. 실시 예에 따라, 표시부(530)는 차량의 이상을 알리기 위해 경고 알람을 출력할 수도 있다. 또한, 표시부(530)는 차량의 현재 상태를 표나 그래프 형태로 출력할 수도 있다.

[0067] 실시 예에 따라, 제2 단말(500)은 제1 단말(300)을 의미할 수 있는데, 이 경우, 제1 단말(100) 또는 제2 단말(500)은 수집부(110), 송신부(130), 저장부(150), 수신부(510) 및 표시부(530)를 모두 포함하는 것으로 이해될 수도 있다.

[0068] 또한, 도 2, 도 3 및 도 6에 도시된 제1 단말(100), 서버(300) 및 제2 단말(500)의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.

[0069] 또한, 본 명세서에서 "~부"라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 "~부"는 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된

코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0071] 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.

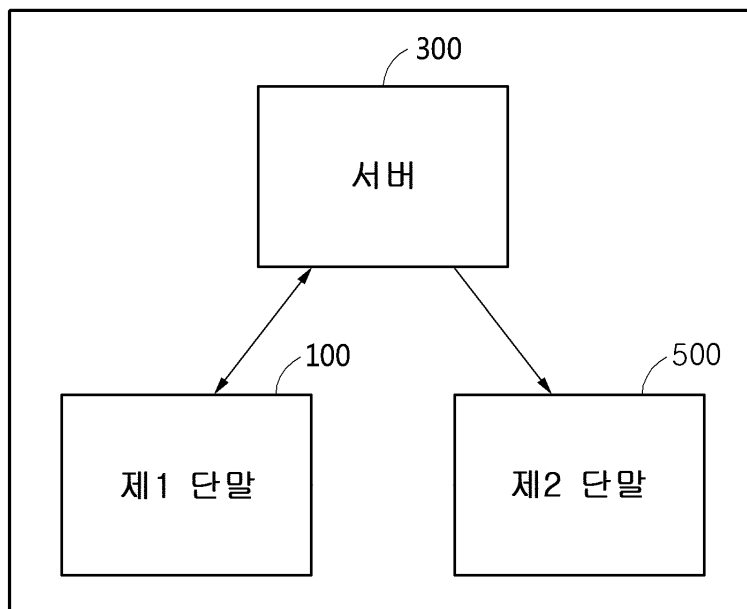
부호의 설명

[0073] 10 : 시스템 100 : 제1 단말
110 : 수집부 130 : 송신부
150 : 저장부 300 : 서버
310 : 수신부 330 : 이상 징후 탐지부
350 : 상태 검증부 370 : 송신부
390 : 저장부 500 : 제2 단말
510 : 수신부 530 : 표시부

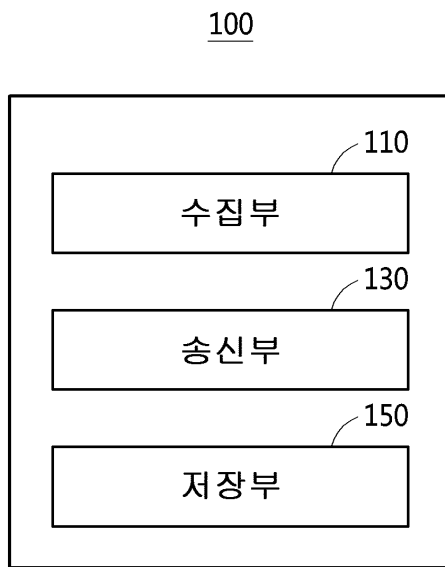
도면

도면1

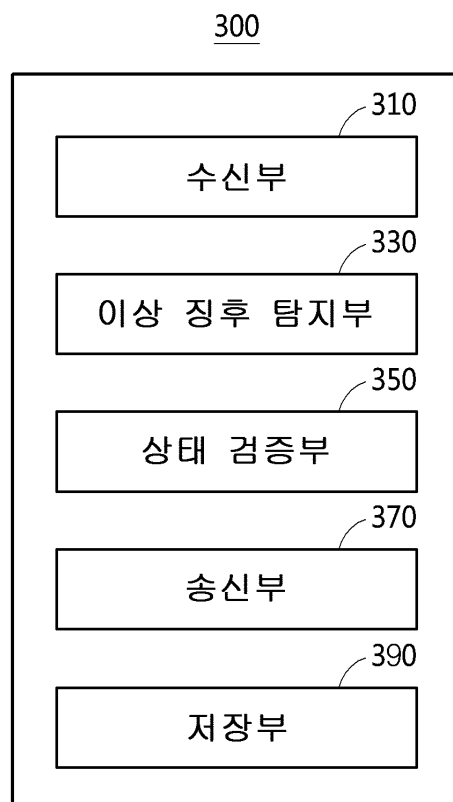
10



도면2



도면3



도면4

Timestamp	Vehicle ID	Entropy per second	Can id	Data[0]	Data[1]	Data[2]	...	Data[7]	...
2017-07-17 06:03:40	Car1	3.04011	7de	19	00	03		01	...
2017-07-17 06:03:41	Car1	3.06084	47F	10	FF	FA		00	...
2017-07-17 06:03:42	Car1	3.03791	220	E3	83	3C		08	...
...	...		...	...	...	...	...	...	...

도면5

Timestamp	Vehicle ID	Entropy per second	OBD Data 1 (Engine rpm)	OBD Data 2 (Transmission oil temperature)	OBD Data 3 (Vehicle speed)	...	OBD Data N (Engine coolant temperature)	...
2017-07-17 06:03:40	Car1	3.04011	809	0	51		32	...
2017-07-17 06:03:41	Car1	3.06084	800	2	61			...
2017-07-17 06:03:42	Car1	3.03791	802	4	71			...
...	...	...	...	...	...	...	...	...

도면6

500

