



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2021년05월06일

(11) 등록번호 10-2248287

(24) 등록일자 2021년04월28일

(51) 국제특허분류(Int. Cl.)

H04L 12/40 (2006.01) H04L 12/26 (2006.01)

H04L 29/06 (2006.01)

(52) CPC특허분류

H04L 12/40104 (2013.01)

H04L 43/0852 (2013.01)

(21) 출원번호 10-2019-0172992

(22) 출원일자 2019년12월23일

심사청구일자 2019년12월23일

(56) 선행기술조사문헌

KR1020180057503 A*

KR1020180137306 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이동훈

서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희국의아침3단지아파트)

박승범

경기도 안산시 상록구 정재로9길 5 (부곡동)

(74) 대리인

김홍석

전체 청구항 수 : 총 6 항

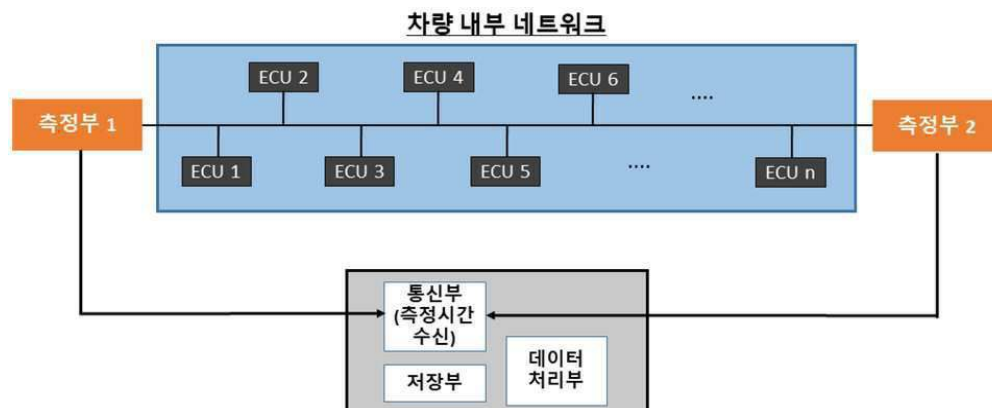
심사관 : 이철수

(54) 발명의 명칭 차량의 내부 네트워크 노드의 위치 추정 장치 및 방법

(57) 요약

노드 위치 추정 장치가 개시된다. 상기 노드 위치 추정 장치는, 각각이 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들, 상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부, 상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함한다.

대표도 - 도2



(52) CPC특허분류

H04L 43/16 (2013.01)

H04L 63/1408 (2013.01)

H04L 2012/40215 (2013.01)

H04L 2012/40273 (2013.01)

명세서

청구범위

청구항 1

각각이, 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들;

상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부;

상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함하고,

상기 복수의 측정부들 각각은 버스(bus) 상의 아날로그 신호의 전압이 임계치에 도달하는 시점을 상기 메시지의 도달 시간으로 측정하는,

노드 위치 추정 장치.

청구항 2

제1항에 있어서,

상기 차량의 내부 네트워크는 CAN(Controller Area Network)이고,

상기 메시지는 CAN 메시지이고,

상기 메시지의 ID는 CAN ID인,

노드 위치 추정 장치.

청구항 3

삭제

청구항 4

각각이, 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들;

상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부;

상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함하고,

상기 복수의 측정부들은 제1 측정부와 제2 측정부를 포함하고,

상기 데이터 처리부는 상기 제1 측정부에 의한 측정 시간과 상기 제2 측정부에 의한 측정 시간의 차이가 미리 정해진 범위를 벗어나는 경우 상기 메시지를 악의적인 메시지로 판단하는,

노드 위치 추정 장치.

청구항 5

각각이, 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들;

상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부;

상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함하고,

상기 차량의 내부 네트워크는 적어도 하나의 서브네트워크를 포함하고,

상기 복수의 측정부들은 상기 차량의 내부 네트워크 상에서 상기 메시지의 도달 시간을 측정하는 제1 측정부와 제2 측정부 및 상기 서브네트워크 상에서 상기 메시지의 도달 시간을 측정하는 적어도 하나의 제3 측정부를 포함하고,

상기 데이터 처리부는 상기 제1 내지 상기 제3 측정부 각각에 의한 측정 시간의 차이들 각각이 미리 정해진 범위에 포함되는지 여부를 판단하고, 상기 미리 정해진 범위에 포함되는 차이의 개수의 비율이 미리 정해진 비율을 초과하는 경우 상기 메시지를 정상 메시지로 판단하는,

노드 위치 추정 장치.

청구항 6

각각이, 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들;

상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부;

상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함하고,

상기 통신부는 상기 복수의 측정부들 중 적어도 하나의 측정부로부터 상기 메시지를 수신하거나 상기 차량 내부 네트워크의 버스로부터 상기 메시지를 수신하고,

상기 데이터 처리부는,

상기 메시지의 ID를 추출하고,

상기 복수의 측정부들 각각에 의해 측정된 도달 시간의 차이가, ID 별로 구별되어 미리 저장되어 있는 도달 시간의 차이에서 추출된 ID에 대응하는 차이로부터 미리 정해진 오차 범위를 벗어나는지 여부를 판단하고,

상기 미리 정해진 오차 범위를 벗어나는 경우, 상기 메시지를 악의적인 메시지로 결정하는,

노드 위치 추정 장치.

청구항 7

노드 위치 추정 장치에 의해 수행되는 노드 위치 추정 방법에 있어서,

차량의 내부 네트워크 상에서 미리 정해진 측정 지점들에 메시지가 도달하는 도달 시간을 측정하는 단계;

상기 도달 시간의 차이를 연산하는 단계;

연산된 도달 시간의 차이를 미리 저장된 도달 시간의 차이를 비교하는 단계; 및

연산된 도달 시간의 차이가 미리 저장된 도달 시간의 차이로부터 미리 정해진 오차 범위를 벗어나는 경우 상기 메시지를 악의적인 메시지로 판단하는 단계를 포함하고,

상기 도달 시간을 측정하는 단계는, 버스 상의 아날로그 신호의 전압이 임계치에 도달하는 시점을 상기 도달 시간으로 측정하는,

노드 위치 추정 방법.

청구항 8

삭제

발명의 설명

기술 분야

[0001] 본 발명은 차량의 내부 네트워크에서 부품의 신호의 이동 시간을 통해 위치를 추정하여 부품을 식별하는 방법에 관한 것이다.

배경 기술

[0003] CAN(controller area Network) 프로토콜은 차량 내부 네트워크로 가장 많이 사용되는 프로토콜이다. 해당 프로토콜의 개발 당시에는 차량의 내부 네트워크가 외부와 단절되어 있었기 때문에 보안 기능이 고려되지 않았다. 이로 인하여 데이터 기밀성, 인증, 접근 제어 등이 제공되지 않는다. 특히, 차량의 내부 네트워크 상의 노드들은 CAN 버스(bus)에 유선으로 연결되어 있으며 메시지를 브로드캐스트 방식으로 전송한다. 메시지에는 CAN ID가 존재하나, CAN 프로토콜 상에는 메시지 인증 기능이 존재하지 않기 때문에 악의적인 노드가 CAN ID를 조작하여 송신하여도 수신 노드들은 해당 메시지를 정상 메시지로 인식할 수 있다. 이를 악용하여 차량을 대상으로 한 사이버 공격이 다수 발생하였다. 이러한 공격을 식별하기 위해서 차량의 내부 네트워크 상 메시지가 정상 노드가 전송한 메시지인지를 식별하는 기술이 필요하다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 공개특허 제2018-0057503호 (2018.05.30. 공개)
(특허문헌 0002) 미합중국 공개특허 US2012/0140861 A1 (2012.06.07. 공개)
(특허문헌 0003) 대한민국 등록특허 제1334017호 (2013.12.12. 공고)

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는 차량의 내부 네트워크 상 두 지점에서 측정한 신호의 도달 시간 차이를 비교함으로써, 해당 신호가 정상적인 노드에서 발송된 신호임을 확인할 수 있는 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따른 노드 위치 추정 장치는, 각각이 차량의 내부 네트워크 상에서 미리 정해진 측정 지점에 메시지가 도달하는 도달 시간을 측정하는 복수의 측정부들, 상기 복수의 측정부들 각각으로부터 도달 시간을 수신하는 통신부, 상기 복수의 측정부들 각각에 의해 측정된 도달 시간이 차이를 이용하여, 상기 메시지의 ID의 위조 여부 또는 변조 여부를 결정하는 데이터 처리부를 포함한다.

[0009] 또한, 본 발명의 일 실시예에 따른 노드 위치 추정 방법은 노드 위치 추정 장치에 의해 수행되고, 차량의 내부 네트워크 상에서 미리 정해진 측정 지점들에 메시지가 도달하는 도달 시간을 측정하는 단계, 상기 도달 시간의 차이를 연산하는 단계, 연산된 도달 시간의 차이를 미리 저장된 도달 시간의 차이를 비교하는 단계, 및 연산된 도달 시간의 차이가 미리 저장된 도달 시간의 차이로부터 미리 정해진 오차 범위를 벗어나는 경우 상기 메시지를 악의적인 메시지로 판단하는 단계를 포함한다.

발명의 효과

[0011] 본 발명의 실시 예에 따르면, 메시지의 도달 시간 차이를 통해 해당 메시지가 비정상적인 메시지의 여부를 판단할 수 있다.

[0012] 또한, 비정상적인 메시지를 감지함으로써 차량 내부 네트워크 상 침입 탐지가 가능하여 안전한 차량 내부 네트

워크 시스템을 구축할 수 있다.

도면의 간단한 설명

- [0014] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
도 1은 CAN 프레임 포맷을 도시한다.
도 2는 본 발명의 일 실시예에 따른 노드 위치 추정 시스템을 도시한다.
도 3은 도 2에 도시된 복수의 측정부들에 의한 메시지 도달 시간 측정 동작을 설명하기 위한 도면이다.
도 4는 도 2에 도시된 노드 위치 추정 장치에 의해 수행되는 노드 위치 추정 방법을 설명하기 위한 흐름도이다.
도 5는 본 발명의 다른 실시예에 따른 노드 위치 추정 시스템을 도시한다.
도 6은 도 5에 도시된 노드 위치 추정 장치에 의해 수행되는 노드 위치 추정 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명들은 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.
- [0016] 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.
- [0017] 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.
- [0018] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "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" 있다거나 "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.
- [0019] 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.
- [0020] 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.
- [0021] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0023] 차량의 내부 네트워크(예컨대, CAN)의 노드들(예컨대, ECU들)은 버스(bus, 예컨대 CAN 버스)에 유선으로 연결되어 있기 때문에, 노드의 위치를 추정할 수 있다면 노드를 식별하는 것 또한 가능하다. CAN 버스 상의 노드가 전

송한 메시지의 아날로그 신호의 이동 시간을 측정하면 위치 측정 기기와의 거리를 예측할 수 있다. 하지만, CAN 프로토콜에는 전역 시간(global time)이 존재하지 않기 때문에 송신 노드에서 메시지를 송신한 절대 시간을 알 수 없다. 이러한 문제를 해결하기 위하여, 본 발명에서는 메시지의 아날로그 신호가 2개 이상의 위치에 도달하는 시간 차를 이용하여 CAN 버스 상 송신 노드의 위치를 추정한다. 또한, 송신 노드 위치 추정을 통해 전송된 메시지가 정상적인 메시지인지 확인함으로써 공격 메시지의 발생 여부를 판단할 수 있다. 또한, CAN 프로토콜의 특성상 중재 필드(Arbitration Field)에서 다수의 노드들이 메시지를 전송하고, 우선 순위를 결정하고 중재 필드 이후 우선 순위가 높은 노드만 메시지를 전송한다. 즉, 중재 이전에는 여러 노드들이 메시지를 전송하므로 중재 이후의 아날로그 신호를 분석해야만 CAN 버스 상에 전송된 메시지 ID(CAN ID)에 해당하는 시간 차이를 구할 수 있다. 도 1에는 CAN 프레임 포맷이 도시되어 있다.

- [0025] 도 2는 본 발명의 일 실시예에 따른 노드 위치 추정 시스템을 도시한다.
- [0026] 노드 위치 추정 시스템은 차량의 내부 네트워크와 노드 위치 추정 장치를 포함한다. 차량의 내부 네트워크는 CAN(Controller Area Network)일 있으나, 본 발명이 이에 제한되는 것은 아니며, 실시예에 따라 FlexRay, LIN(Local Interconnect Network) 등을 포함할 수도 있다.
- [0027] 노드 위치 추정 장치는 통신부와 데이터 처리부를 포함한다. 실시예에 따라, 노드 위치 추정 장치는 저장부 및/또는 복수의 측정부들을 더 포함할 수도 있다. 또한, 노드 위치 추정 장치는 버스(예컨대, CAN 버스)로부터 메시지(예컨대, CAN 메시지)를 직접 수신하거나 복수의 측정부들 중 적어도 하나의 측정부를 경유하여 수신할 수도 있다. 즉, 복수의 측정부들 중 적어도 하나의 측정부는 버스 상에서 전송(브로드캐스트)되는 메시지를 수신하여 통신부로 송신할 수도 있다.
- [0028] 복수의 측정부들 각각은 버스 상에서 미리 정해진 측정 지점에 메시지가 도달하는 시간을 측정하고, 측정된 시간을 통신부로 전송할 수 있다. 또한, 복수의 측정부들 중 적어도 하나의 측정부는 메시지 자체를 버스 상에서 수신하고 측정 시간과 함께 통신부에 전송할 수도 있다.
- [0029] 통신부는 복수의 측정부들 각각으로부터 메시지의 도달 시간 및/또는 메시지를 수신하고, 수신된 도달 시간 및/또는 메시지를 저장부에 저장할 수 있다.
- [0030] 데이터 처리부는 통신부에 의해 수신된 도달 시간 및/또는 메시지, 또는 저장부에 저장된 도달 시간 및/또는 메시지를 이용하여 메시지를 송신한 노드의 위치를 추정하고, 추정된 위치를 이용하여 해당 메시지가 악의적인 메시지인지 여부(또는 메시지의 ID 위조 및/또는 변조 여부)를 결정할 수 있다.
- [0031] 노드 위치 추정 장치는 각종 연산 처리 및 신호 생성이 가능한 적어도 하나의 전자 장치를 포함할 수 있다. 여기서, 적어도 하나의 전자 장치는 프로세서 및/또는 프로세서가 설치된 컴퓨팅 장치를 포함할 수 있다. 여기서, 프로세서는, 예를 들어, 중앙 처리 장치(CPU, Central Processing Unit), 마이크로 컨트롤러 유닛(MCU, Micro Controller Unit), 마이컴(Micom, Micro Processor), 애플리케이션 프로세서(AP, Application Processor), 전자 제어 유닛(ECU, Electronic Controlling Unit), 그래픽 처리 장치(GPU, Graphic Processing Unit) 및/또는 각종 연산 처리 및 제어 신호의 생성이 가능한 처리 장치 등을 포함할 수 있다. 이들 처리 장치는 예를 들어 하나 또는 둘 이상의 반도체 칩 및 관련 부품을 이용하여 구현될 수 있다.
- [0032] 노드 위치 추정 장치는 도 2에 도시된 바와 같이 저장부 및/또는 복수의 측정부와 데이터 송수신이 가능하도록 직접 또는 간접적으로 연결되어 있을 수 있다. 저장부는 통신부에 의해 수신된 메시지의 측정 시간, 데이터 처리부 또는 노드 위치 추정 장치의 제어, 연산 또는 처리 과정에서 생성된 적어도 하나의 데이터를 일시적으로 또는 비일시적으로 저장할 수 있다. 저장부는 주기억장치 및 보조기억장치 중 적어도 하나를 포함할 수 있으며, 주기억장치는 롬(ROM) 및/또는 램(RAM) 등을 포함할 수 있고, 보조기억장치는 플래시 메모리 장치, SD(Secure Digital) 카드, 솔리드 스테이트 드라이브(SSD, Solid State Drive), 하드 디스크 드라이브(HDD, Hard Disc Drive) 컴팩트 디스크(CD), 디브이디(DVD) 및/또는 레이저 디스크 등을 포함할 수 있다.
- [0033] 노드 위치 추정 장치는 저장부에 저장된 애플리케이션을 구동시켜, 메시지의 도달 시간 연산, 비정상적인 메시지의 감지 등 다양한 동작을 수행할 수도 있다. 여기서, 애플리케이션은, 설계자에 의해 직접 작성되어 저장부에 저장 또는 갱신된 것일 수도 있고, 또는 유선 또는 무선 통신 네트워크를 통해 접속 가능한 전자 소프트웨어 유통망 등을 통하여 획득 또는 갱신된 것일 수도 있다.
- [0035] 도 3은 도 2에 도시된 복수의 측정부들에 의한 메시지 도달 시간 측정 동작을 설명하기 위한 도면이다.
- [0036] 측정부는 버스 상의 미리 결정된 지점에서 전송(브로드캐스트)되는 메시지의 도달 시간을 측정하고, 측정된 도

달 시간을 통신부로 송신할 수 있다. 예컨대, 측정부는 중재 필드(arbitration field) 이후에 버스 상의 아날로그 신호의 전압이 특정 임계값(δ)에 도달한 시점을 메시지의 도달 시간으로 측정할 수 있다. 임의의 노드(예컨대, ECU)로부터 제1 측정부 및 제2 측정부 각각까지의 거리가 상이하기 때문에, 도 3에 도시된 바와 같이 메시지가 제1 측정부와 제2 측정부에 도달하는 시간에 차이가 발생한다. 결국, 제1 측정부는 메시지가 제1 측정부의 측정 지점에 도달하는 시간, 즉 버스 상의 아날로그 신호의 전압이 특정 임계값(δ)에 도달한 시간(t_1)을 측정한 후 측정 시간(t_1)을 통신부로 전송하고, 제2 측정부는 메시지가 제2 측정부의 측정 지점에 도달하는 시간, 즉 버스 상의 아날로그 신호의 전압이 특정 임계값(δ)에 도달한 시간(t_2)을 측정한 후 측정 시간(t_2)을 통신부로 전송한다.

[0037] 데이터 처리부는 복수의 측정부들 각각에 의해 측정된 측정 시간의 차이($\Delta t = t_1 - t_2$)를 연산한다. 측정 시간의 차이는 노드의 위치에 의존적이다. 따라서, 데이터 처리부는 측정 시간의 차이를 통해 메시지를 송신한 노드의 위치를 추정할 수 있다. 이를 위해, 데이터 처리부는 메시지 ID 별로 미리 저장된 측정 시간 차이와 연산된 측정 시간의 차이를 비교함으로써, 송신된 메시지가 비정상적인 메시지(악의적인 메시지)인지 여부를 결정할 수 있다. 또한, 데이터 처리부는 임의의 노드로부터 송신된 메시지로부터 ID를 추출할 수도 있다. 따라서, 추출된 ID에 대응하는 미리 저장된 측정 시간 차이와 연산된 측정 시간의 차이가 미리 정해진 오차 범위를 벗어나는 경우, 데이터 처리부는 메시지를 악의적인 메시지로 판단할 수 있다.

[0039] 도 4는 도 2에 도시된 노드 위치 추정 장치에 의해 수행되는 노드 위치 추정 방법을 설명하기 위한 흐름도이다.

[0040] 우선, 복수의 측정부들 각각은 측정 지점에 메시지가 도달하는 시간을 측정한다(S100). 측정 시간은 통신부로 송신될 수 있다.

[0041] 노드 위치 추정 장치의 데이터 처리부는 측정 시간의 차이(Δt)를 연산한다(S200). 추가적으로, 데이터 처리부는 메시지로부터 ID를 추출할 수도 있다. 이후, 데이터 처리부는 연산된 측정 시간의 차이와 ID 별로 미리 저장된 측정 시간의 차이를 비교하여, 연산된 측정 시간의 차이가 미리 정해진 범위 내인지 여부를 판단할 수 있다(S300). 연산된 측정 시간의 차이가 미리 정해진 범위 내인 경우, 메시지가 추정된 위치(추정된 노드)로부터 송신된 것으로 볼 수 있으므로, 해당 메시지는 정상적인 메시지로 판단될 수 있다. 이 경우, 노드 위치 추정 방법을 종료되거나 S100 단계가 재차 수행될 수 있다.

[0042] 연산된 측정 시간의 차이가 미리 정해진 범위를 벗어나는 경우, 메시지가 추정된 위치(추정된 노드)로부터 송신된 것으로 볼 수 없으므로, 해당 메시지는 비정상적인 메시지로 판단될 수 있다(S400). 이와 같이, 악의적인 메시지 여부를 판단함으로써, 차량의 내부 네트워크에 대한 침입을 탐지할 수 있다.

[0044] 도 5는 본 발명의 다른 실시예에 따른 노드 위치 추정 시스템을 도시한다.

[0045] 도 5의 노드 위치 추정 시스템을 설명함에 있어, 앞선 기재와 중복되는 내용에 관하여는 그 기재를 생략하기로 한다.

[0046] 노드 위치 추정 시스템은 차량의 내부 네트워크와 노드 위치 추정 장치를 포함한다. 노드 위치 추정 장치는 통신부와 데이터 처리부를 포함한다. 실시예에 따라, 노드 위치 추정 장치는 저장부 및/또는 복수의 측정부들을 더 포함할 수도 있다. 또한, 노드 위치 추정 장치는 버스(예컨대, CAN 버스)로부터 메시지(예컨대, CAN 메시지)를 직접 수신하거나 복수의 측정부들 중 적어도 하나의 측정부를 경유하여 수신할 수도 있다. 즉, 복수의 측정부들 중 적어도 하나의 측정부는 버스 상에서 전송(브로드캐스트)되는 메시지를 수신하여 통신부로 송신할 수도 있다.

[0047] 복수의 측정부들 각각은 버스 상에서 미리 정해진 측정 지점에 메시지가 도달하는 시간을 측정하고, 측정된 시간을 통신부로 전송할 수 있다. 또한, 복수의 측정부들 중 적어도 하나의 측정부는 메시지 자체를 버스 상에서 수신하고 측정 시간과 함께 통신부에 전송할 수도 있다.

[0048] 차량의 내부 네트워크에 k 개의 서브네트워크가 존재하는 경우, 측정부의 개수는 $k+2$ 개 이상일 수 있다. 측정부에 의한 측정 지점은 차량 내부 네트워크의 양단과 서브네트워크의 말단을 포함할 수 있다. 각 측정부에서 수신한 메시지의 아날로그 신호가 arbitration field 이후 특정 임계치에 도달하는 시점을 측정하고, 측정 시간을 통신부로 송신할 수 있다.

[0049] 통신부는 복수의 측정부들 각각으로부터 메시지의 도달 시간 및/또는 메시지를 수신하고, 수신된 도달 시간 및/또는 메시지를 저장부에 저장할 수 있다.

- [0050] 데이터 처리부는 통신부에 의해 수신된 도달 시간 및/또는 메시지, 또는 저장부에 저장된 도달 시간 및/또는 메시지를 이용하여 메시지를 송신한 노드의 위치를 추정하고, 추정된 위치를 이용하여 해당 메시지가 악의적인 메시지인지 여부를 결정할 수 있다.
- [0051] 내부 네트워크가 존재하는 경우(즉, $k+2$ 개의 측정부가 존재하는 경우), 데이터 처리부는 측정 시간들($t_1, t_2, \dots, t_{k+2}$)의 차이로 이루어진 시간 차 행렬($\Delta t_{1,2}, \Delta t_{1,k+2}, \dots, \Delta t_{k+1,k+2}$)을 생성(연산)한다. 시간 차 행렬은 $(1 \times_{k+2} C_2)$ 행렬이다. 실시예에 따라, 시간 차 행렬을 생성하지 않고 측정 시간들의 차이들과 미리 ID 별로 저장되어 있는 차이들을 비교할 수도 있다. 또한, 데이터 처리부는 ID 별로 저장되어 있는 시간 차 행렬과 연산된 시간 차 행렬을 비교한다. 각 행렬의 성분의 차이가 임계값 이내에 존재하는지 여부를 판단함으로써 악의적인 메시지 여부를 판단할 수 있다. 예컨대, 임계값 이내의 행렬 성분이 임계 비율(α)보다 클 경우, 정상적인 메시지로 판단할 수 있다.
- [0053] 도 6은 도 5에 도시된 노드 위치 추정 장치에 의해 수행되는 노드 위치 추정 방법을 설명하기 위한 흐름도이다.
- [0054] 우선, 복수의 측정부들 각각은 측정 지점에 메시지가 도달하는 시간을 측정한다(S500). 측정 시간은 통신부로 송신될 수 있다.
- [0055] 노드 위치 추정 장치의 데이터 처리부는 시간 차 행렬을 연산한다(S600). 추가적으로, 데이터 처리부는 메시지로부터 ID를 추출할 수도 있다. 이후, 데이터 처리부는 연산된 시간 차 행렬과 ID 별로 미리 저장된 시간 차 행렬을 비교하여, 미리 정해진 범위를 만족하는 행렬 성분의 개수를 산정한다(S700).
- [0056] 미리 정해진 범위를 만족하는 행렬 성분의 비율이 미리 정해진 비율을 초과하는 경우, 메시지가 추정된 위치(추정된 노드)로부터 송신된 것으로 볼 수 있으므로, 해당 메시지는 정상적인 메시지로 판단될 수 있다(S800의 YES). 이 경우, 노드 위치 추정 방법을 종료되거나 S500 단계가 재차 수행될 수 있다.
- [0057] 미리 정해진 범위를 만족하는 행렬 성분의 비율이 미리 정해진 비율을 초과하지 않는 경우, 메시지가 추정된 위치(추정된 노드)로부터 송신된 것으로 볼 수 없으므로, 해당 메시지는 비정상적인 메시지로 판단될 수 있다(S900). 이와 같이, 악의적인 메시지 여부를 판단함으로써, 차량의 내부 네트워크에 대한 침입을 탐지할 수 있다.
- [0059] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시 예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로 컴퓨터, 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(Operation System, 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 기술 분야에서 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 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.
- [0060] 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, 구성 요소(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.
- [0061] 실시 예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시 예를 위하여 특별히 설계

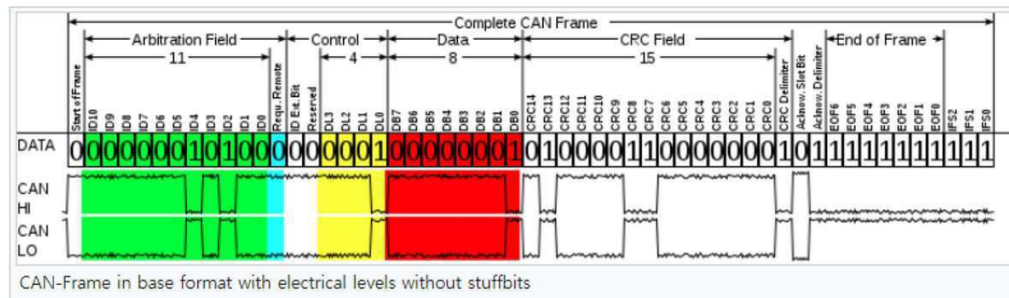
되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시 예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0063]

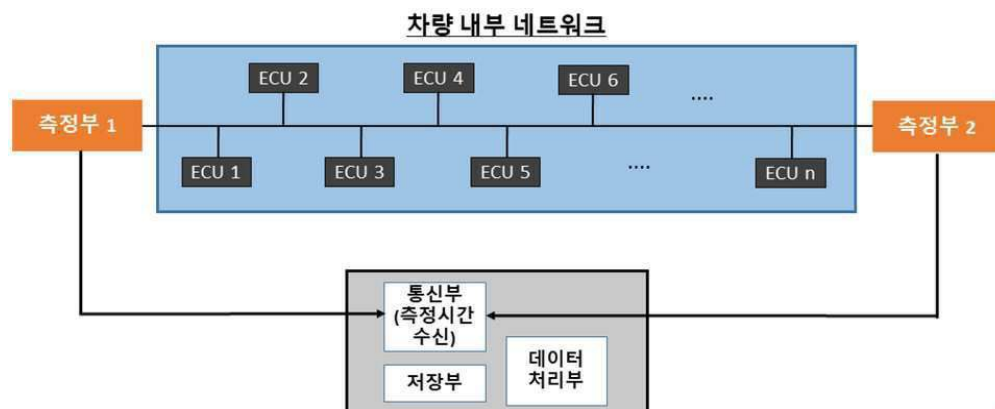
본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

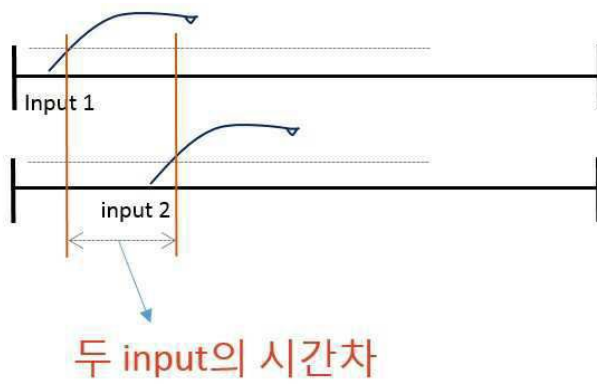
도면1



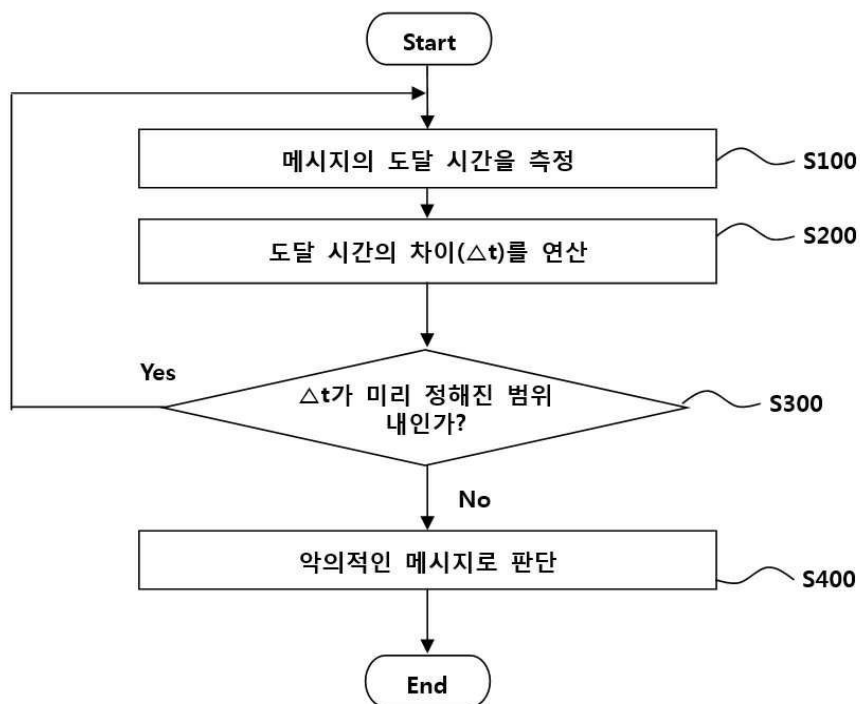
도면2



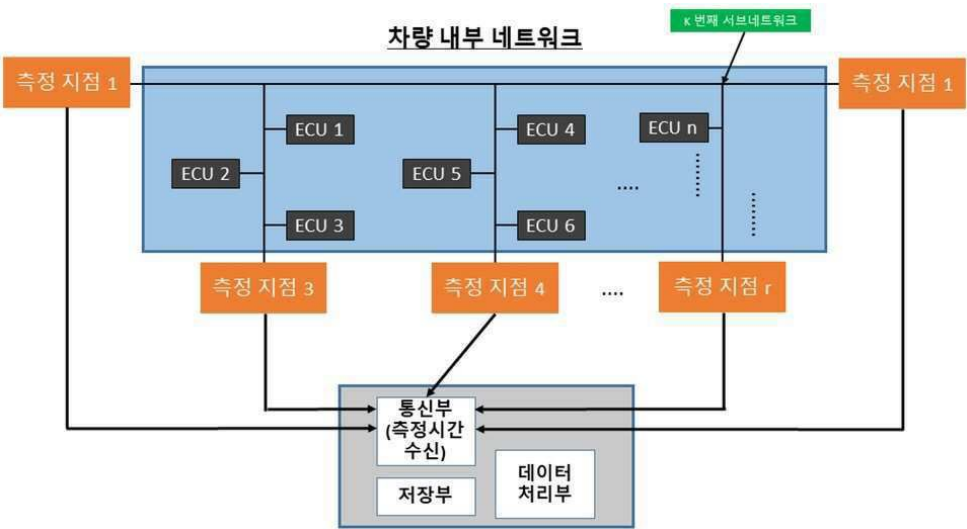
도면3



도면4



도면5



도면6

