(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0015791
(43) 공개일자 2018년02월14일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/40* (2006.01)
(52) CPC특허분류
H04L 63/1408 (2013.01)
H04L 12/40 (2013.01)
(21) 출원번호 10-2016-0099162
(22) 출원일자 2016년08월03일
심사청구일자 2016년08월03일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
고동우
대구광역시 남구 현충로5길 86-3 2층 (대명동)
송현민
서울특별시 성북구 안암로9가길 87-6 (안암동5가)
김휘강
서울특별시 서초구 태봉로2길 65 404동 302호 (우면동,네이처힐4단지)
(74) 대리인
김등용, 김홍석

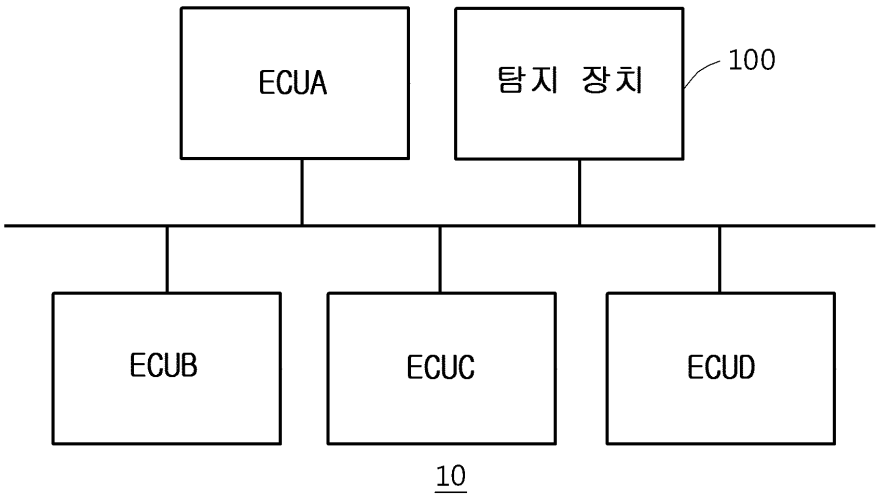
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **시퀀스 마이닝 기반의 차량 이상 징후 탐지 장치**

(57) 요 약

탐지 장치가 개시된다. 상기 탐지 장치는 패턴 생성부를 포함하고, 상기 패턴 생성부는 통신 시스템 내에서 순차적으로 발생하는 복수의 메시지들을 수신하는 제1 메시지 수신부, 상기 복수의 메시지들 각각으로부터 송신 아이디를 추출하여 아이디 시퀀스를 출력하는 제1 아이디 추출부, 및 상기 아이디 시퀀스로부터 아이디의 패턴을 생성하는 정상 패턴 생성부를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 2012/40273 (2013.01)

명 세 서

청구범위

청구항 1

패턴 생성부를 포함하는 탐지 장치에 있어서,

상기 패턴 생성부는,

통신 시스템 내에서 순차적으로 발생하는 복수의 메시지들을 수신하는 제1 메시지 수신부;

상기 복수의 메시지들 각각으로부터 송신 아이디를 추출하여 아이디 시퀀스를 출력하는 제1 아이디 추출부; 및

상기 아이디 시퀀스로부터 아이디의 패턴을 생성하는 정상 패턴 생성부를 포함하는,

탐지 장치.

청구항 2

제1항에 있어서,

상기 통신 시스템은 차량 통신 시스템이고,

상기 복수의 메시지들 각각은 CAN(Controller Area Network) 메시지인,

탐지 장치.

청구항 3

제1항에 있어서,

상기 정상 패턴 생성부는 서열 정렬(Sequence Alignment) 기법을 이용하여 상기 아이디의 패턴을 생성하는,

탐지 장치.

청구항 4

제1항에 있어서,

상기 정상 패턴 생성부는,

상기 아이디 시퀀스를 미리 정해진 단위로 분할하여 복수의 분할된 아이디 시퀀스들을 생성하고, 상기 복수의 분할된 아이디 시퀀스들 각각을 재정렬하여 상기 아이디의 패턴을 생성하는,

탐지 장치.

청구항 5

제1항에 있어서,

상기 탐지 장치는 이상 탐지부를 더 포함하고,

상기 이상 탐지부는,

상기 통신 시스템 내에서 순차적으로 발생하는 복수의 제2 메시지들을 수신하는 제2 메시지 수신부;

상기 복수의 제2 메시지들 각각으로부터 송신 아이디를 추출하여 제2 아이디 시퀀스를 출력하는 제2 아이디 추

출부; 및

상기 제2 아이디 시퀀스와 미리 저장되어 있는 복수의 아이디 패턴들 각각과 비교하여 차량의 이상 여부를 결정하는 유사도 계산부를 포함하는,

탐지 장치.

청구항 6

제5항에 있어서,

상기 유사도 계산부는 미리 정해진 길이를 갖는 상기 제2 아이디 시퀀스와 상기 복수의 아이디 패턴들 각각의 편집 거리(edit distance)를 계산하고, 계산된 편집 거리 중 가장 작은 값을 갖는 편집 거리를 유사도로 결정하는,

탐지 장치.

청구항 7

제6항에 있어서,

상기 유사도 계산부는 상기 유사도의 값이 미리 정해진 값보다 큰 경우 상기 차량의 상태를 비정상 상태로 결정하는,

탐지 장치.

청구항 8

이상 탐지부를 포함하는 탐지 장치에 있어서,

상기 이상 탐지부는,

통신 시스템 내에서 순차적으로 발생하는 복수의 메시지들을 수신하는 메시지 수신부;

상기 복수의 메시지들 각각으로부터 송신 아이디를 추출하여 아이디 시퀀스를 출력하는 아이디 추출부; 및

상기 아이디 시퀀스와 미리 저장되어 있는 복수의 아이디 패턴들을 비교하여 차량의 이상 여부를 결정하는 유사도 계산부를 포함하고,

상기 유사도 계산부는 미리 정해진 길이를 갖는 상기 아이디 시퀀스와 상기 복수의 아이디 패턴들 각각의 편집 거리를 계산하고, 계산된 편집 거리 중 가장 작은 값을 갖는 편집 거리를 유사도로 결정하는,

탐지 장치.

청구항 9

제8항에 있어서,

상기 유사도 계산부는 상기 유사도의 값이 미리 정해진 값보다 큰 경우 상기 차량의 상태를 비정상 상태로 결정하는,

탐지 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 차량 이상 징후 탐지 장치에 관한 것으로, 특히 시퀀스 마이닝 기법을 이용하여 CAN 메시지의 ID 시퀀스로부터 패턴을 생성하고, 이를 통하여 차량의 이상 여부를 결정할 수 있는, 시퀀스 마이닝 기반의 차량 이상 징후 탐지 장치에 관한 것이다.

배 경 기 술

[0003] IT(Information Technology)의 발전과 함께 차량 제어 시스템이 기계식에서 전자식으로 전환되는 비율이 증가하는 추세를 보이며, 전자식 제어로 인해 OBD-Ⅱ(On-Board Diagnostics) 단자를 통한 연결과 텔레매틱스 서비스를 통해 차량 내부 네트워크로의 접근이 용이해졌다.

[0004] 또한, 차량에 정보통신기술을 융합시키기 위해 ECU(Electronic Control Unit)의 사용이 필수적으로 요구된다. 차량 내부에는 복수의 ECU들이 탑재되며, ECU들 사이의 효율적인 통신을 위해 CAN(Controller Area Network), LIN(Local Interconnect Network), MOST(Media Oriented System Transport), FlexRay 등 다양한 통신 기법들이 차량 내부 네트워크에 적용되고 있다.

[0005] CAN은 차량 네트워크에 사용하기 위해 개발된 네트워크 프로토콜로 복수의 ECU들이 서로 통신할 수 있도록 경제적이며 안정적인 네트워크를 제공하는 기술이다. 각각이 ECU는 CAN 버스에 브로드캐스팅되는 모든 메시지를 확인하여 자신과 관련된 메시지만을 필터링하여 제어를 수행하게 된다.

[0006] 하지만, CAN은 모든 ECU에 메시지를 전달하는 브로드캐스팅 프로토콜임에도 불구하고 데이터 암호화나 인증 기능을 대부분 제공하지 않기 때문에 메시지 주입 등의 공격에 취약하다. 본 발명은 차량 내부 네트워크의 메시지, 특히 CAN 메시지의 시퀀스를 분석하여 차량의 이상 징후를 탐지하고자 한다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허 제1446525호(2014.09.25. 등록)

(특허문헌 0002) 일본국 공개특허 제2013-048374호(2013.03.07. 공개)

(특허문헌 0003) 미합중국 공개특허 제2008-0133955호(2008.06.05. 공개)

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적인 과제는 시퀀스 마이닝 기법을 이용하여 CAN 메시지의 ID 시퀀스로부터 패턴을 생성하고, 이를 통하여 차량의 이상 여부를 결정할 수 있는, 시퀀스 마이닝 기반의 차량 이상 징후 탐지 장치를 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명의 실시 예에 따른 차량 이상 징후 탐지 장치는, 패턴 생성부를 포함하고, 상기 패턴 생성부는 통신 시스템 내에서 순차적으로 발생하는 복수의 메시지들을 수신하는 제1 메시지 수신부, 상기 복수의 메시지들 각각으로부터 송신 아이디를 추출하여 아이디 시퀀스를 출력하는 제1 아이디 추출부, 및 상기 아이디 시퀀스로부터 아이디의 패턴을 생성하는 정상 패턴 생성부를 포함한다.

[0012] 또한, 본 발명의 다른 실시 예에 따른 차량 이상 징후 탐지 장치는, 이상 탐지부를 포함하고, 상기 이상 탐지부는 통신 시스템 내에서 순차적으로 발생하는 복수의 메시지들을 수신하는 메시지 수신부, 상기 복수의 메시지들

각각으로부터 송신 아이디를 추출하여 아이디 시퀀스를 출력하는 아이디 추출부, 및 상기 아이디 시퀀스와 미리 저장되어 있는 복수의 아이디 패턴들을 비교하여 차량의 이상 여부를 결정하는 유사도 계산부를 포함하고, 상기 유사도 계산부는 미리 정해진 길이를 갖는 상기 아이디 시퀀스와 상기 복수의 아이디 패턴들 각각의 편집 거리를 계산하고, 계산된 편집 거리 중 가장 작은 값을 갖는 편집 거리를 유사도로 결정한다.

발명의 효과

[0014] 본 발명의 실시 예에 따른 시퀀스 마이닝 기반의 차량 이상 징후 탐지 장치에 의할 경우, 주행 중인 차량을 대상으로 하는 메시지 주입 공격 등을 실시간으로 탐지할 수 있는 효과가 있다.

[0015] 또한, 차량의 CAN 메시지 시퀀스를 통해 외부 공격 또는 내부 이상을 탐지하기 때문에 필요한 컴퓨팅 자원이 적고, 신속하게 차량의 이상 여부를 탐지할 수 있으며, 차량의 이상 징후를 운전자에게 신속히 알려 교통 사고를 예방할 수 있는 효과가 있다.

도면의 간단한 설명

[0017] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 통신 시스템을 도시한다.

도 2는 본 발명의 일 실시 예에 따른 CAN 프로토콜의 데이터 프레임의 일 예를 도시한다.

도 3은 도 1에 도시된 탐지 장치의 기능 블럭도이다.

도 4는 분할된 ID 시퀀스로부터 정상 패턴을 생성하는 과정의 일 예를 도시하는 도면으로, 도 4a는 분할된 ID 시퀀스의 일 예(좌)와 서열 정렬된 ID 시퀀스의 일 예(우)를, 도 4b는 서열 정렬된 ID 시퀀스의 일 예(좌)로부터 추출된 패턴의 일 예(우)를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] 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.

[0024] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0026] 도 1은 본 발명의 일 실시 예에 의한 통신 시스템을 도시한다. 통신 시스템(10)은 차량용 통신 시스템을 의미할 수 있으며, 구체적으로는 CAN(Controller Area Network) 통신 시스템일 수 있다. 그러나 본 발명이 통신 시스템(10)의 종류에 제한되는 것은 아니며, 실시 예에 따라 통신 시스템(10)은 CAN FD(CAN with Rlexible Data-Rate), FlexRay, LIN(Local Interconnect Network) 또는 MOST(Multimedia Oriented Systems Transport) 통신 시스템일 수도 있다.

[0027] 도 1을 참조하면, 통신 시스템(10)은 복수의 ECU(Electronic Control Unit)들, 탐지 장치(100), 및 버스(bus; 12)를 포함한다. 도 1에는 총 4개의 ECU들(ECUA 내지 ECUD)만이 도시되어 있으나, 통신 시스템(10)에 포함된 ECU의 개수는 n(n은 2 이상의 자연수)일 수 있다.

[0028] 상기 복수의 ECU들은 제1 ECU(ECUA), 제2 ECU(ECUB), 제3 ECU(ECUC), 제4 ECU(ECUD)를 포함한다. 또한, 버스(12)는 두 개의 통신선, CAN-H(또는 CAN High) 및 CAN-L(또는 CAN Low)을 포함할 수 있다. 이때, 디지털 '0'(dominant state)의 값을 전송하는 경우 CAN-H에 약 3.5V, CAN-L에 약 1.5V의 전압이 흐를 수 있으며, 디지털 '1'(recessive)의 값을 전송하는 경우 CAN-H 및 CAN-L에 약 2.5V의 전압이 흐를 수 있다.

[0029] 차량의 이상징후 탐지 장치, 이상 탐지 장치 등으로 명명될 수도 있는 탐지 장치(100)는 ECU의 일종으로 구현될 수 있다. 탐지 장치(100)는 통신 시스템(10) 내에서 발생하는 또는 전송되는 메시지, 예컨대 CAN 메시지를 모니터링하여 차량의 이상 여부를 감지할 수 있다.

[0030] 도 1에서, 탐지 장치(100)는 통신 시스템(10)의 일부 구성으로 도시되고 설명되었으나, 실시 예에 따라서는 탐지 장치(100)는 통신 시스템(10)과는 별도로 구현될 수도 있다. 구체적으로, 통신 시스템(10)이 CAN 통신 시스템일 때 탐지 장치(100)는 소정의 단자, 예컨대 OBD-2(On Board Diagnostics) 단자를 통하여 통신 시스템(10)으로부터 메시지를 수신할 수도 있다.

[0031] 상기 복수의 ECU들 각각은 대응되는 전자 장치의 동작을 제어할 수 있으며, 버스(12)를 통하여 다른 ECU와 통신할 수 있다. 이때, 상기 복수의 ECU들 각각은 메시지를 송신하거나 수신하기 위한 송수신기를 포함할 수 있으며, 실시 예에 따라 상기 송수신기는 대응되는 ECU와 별도로 구현될 수도 있다.

[0032] ECU들은 버스(12), 예컨대 CAN 통신 버스에 연결되어 있고 브로드캐스트(broadcast) 방식으로 통신할 수 있다. 데이터(또는 메시지)를 전송하고자 하는 ECU가 CAN 데이터 규격에 수신 ECU의 ID와 전송하고자 하는 정보를 포함하여 버스(12)에 브로드캐스트하면, 버스(12)에 연결된 모든 ECU가 수신하고 CAN 데이터 규격에 포함된 수신 ECU의 ID에 해당하는 ECU만이 CAN 데이터를 처리하는 방식이다.

[0034] 도 2는 본 발명의 일 실시 예에 따른 CAN 프로토콜의 데이터 프레임의 일 예를 도시한다.

[0035] 도 2를 참조하면, 데이터 프레임(또는 CAN 메시지)은 SOF(Start of Frame) 필드, ID(arbitration) 필드, RTR 필드, Control 필드, Data 필드, CRC 필드, ACK 필드, 및 EOF(End of Frame) 필드로 구성될 수 있다.

[0036] SOF 필드는 데이터 프레임의 시작을 나타내는 필드로서 1 비트가 할당되며, ID 필드는 데이터 프레임의 송신자를 식별할 수 있는 ID 정보를 나타내며 11 비트가 할당될 수 있다. RTR 필드는 리모트 프레임과 데이터 프레임을 구별하는 필드로서 1 비트가 할당되며, 리모트 프레임일 경우의 신호 종류는 1, 데이터 프레임일 경우의 신호 종류는 0이다. 본 발명에서는 상기 ID 필드에 포함된 송신자의 ID를 이용하여 CAN 메시지를 송신한 ECU의 ID를 추출할 수 있으며, 본 명세서에서 ID라 함은 CAN 메시지를 송신한 ECU의 ID를 의미할 수 있다.

[0037] Control 필드에는 총 6 비트가 할당되는데, 그 중에서 2 비트는 예약 비트로서 고정값 '00'을 출력하고, 나머지

4 비트는 다음에 연속되는 Data 필드의 데이터 길이(length)를 나타낼 수 있다.

[0038] Data 필드에는 데이터 프레임의 데이터를 의미하며 최대 64 비트가 할당될 수 있다. CRC 필드에는 16 비트가 할당되며, 15 비트(CRC Sequence)는 데이터 프레임의 CRC 값을 의미하며, 1 비트(CRC delimiter)는 CRC 값의 끝을 의미하며 고정값 '1'을 출력할 수 있다.

[0039] ACK 필드에는 2 비트가 할당되며 데이터의 수신 여부를 알 수 있는 정보가 실린다. 즉, 임의의 데이터 송신자가 특정 데이터가 포함된 데이터 프레임을 CAN 버스(12)에 실어 주면, CAN 버스(12)에 연결된 모든 ECU는 현재 CAN 버스(12)에 실린 데이터가 자신에게 필요한 데이터인지를 확인하여, 필요한 데이터라고 판단되면 CAN 버스(12)에 실린 데이터를 수신한다. 이때, 데이터를 수신한 ECU는 데이터 송신자가 출력한 데이터 프레임의 ACK 필드에 자신이 데이터를 수신하였음을 알려주는 정보를 실어줌으로써, 데이터 송신자가 동일한 데이터를 계속해서 출력하지 않도록 한다. 즉, 임의의 데이터 송신자가 출력하는 데이터는 CAN 버스(12)에 실린 후 다시 자신에게 피드백(Feedback)될 수 있는데, 피드백되는 데이터 프레임의 ACK 필드에 실린 정보를 토대로 동일한 데이터를 재전송할 것인지의 여부를 결정하게 된다. 1 비트(ACK slot)는 ACK 비트이며, 나머지 1 비트(ACK delimiter)는 ACK 값의 끝을 의미하며 고정값 '1'을 출력한다.

[0040] 마지막으로, 프레임의 끝을 알리는 EOF(End of Frame) 필드에는 7 비트가 할당되며 고정값 '1111111'이 출력된다.

[0041] 상술된 예시적인 CAN 데이터 프레임은 실시 예에 따라 변화할 수 있음은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명할 것이다.

[0043] 도 3은 도 1에 도시된 탐지 장치의 기능 블럭도이다. 도 4는 분할된 ID 시퀀스로부터 정상 패턴을 생성하는 과정의 일 예를 도시하는 도면으로, 도 4a는 분할된 ID 시퀀스의 일 예(좌)와 서열 정렬된 ID 시퀀스의 일 예(우)를, 도 4b는 서열 정렬된 ID 시퀀스의 일 예(좌)로부터 추출된 패턴의 일 예(우)를 도시한다.

[0044] 도 1 내지 도 4를 참조하면, 탐지 장치(100)는 패턴 생성부(110)와 이상 탐지부(130) 중 적어도 하나를 포함할 수 있고, 실시 예에 따라 탐지 장치(100)는 DB(database, 150)를 더 포함할 수 있다.

[0045] 패턴 생성부(110)는 차량이 주행 중, 특히 정상적인 주행 중에 순차적으로 발생하는 메시지를 수신하여, 각각의 메시지로부터 송신 ECU의 ID를 추출하고, 추출된 ID로부터 소정의 패턴, 예컨대 정상 패턴(또는 정상 주행 패턴)을 생성할 수 있다. 또한, 생성된 패턴은 패턴 생성부(110)에 의해 DB(150)에 저장될 수 있다.

[0046] 이상 탐지부(130)는 차량의 주행(실제 주행) 중에 순차적으로 발생하는 메시지를 수신하여, 각각의 메시지로부터 송신 ECU의 ID를 추출하고, 추출된 ID의 시퀀스와 DB(150)에 저장되어 있는 패턴(또는 주행 패턴)을 비교하여 차량의 이상 여부를 감지할 수 있다.

[0047] DB(150)에는 발생되는 메시지의 송신 ID의 시퀀스에 관한 적어도 하나의 패턴이 저장되어 있을 수 있다. 상기 패턴은 패턴 생성부(110)에 의해 생성된 패턴이거나, 미리 저장된 패턴일 수 있다.

[0049] 구체적으로, 패턴 생성부(110)는 제1 메시지 수신부(111), 제1 ID 추출부(113), 및 정상 패턴 생성부(115)를 포함한다.

[0050] 제1 메시지 수신부(111)는 통신 시스템(10) 내에서 순차적으로 발생하는 CAN 메시지들을 수신할 수 있다. 제1 메시지 수신부(111)는 통신 시스템(10)의 버스(12)를 통하여 CAN 메시지들을 수신하거나 OBD-2 단자를 통하여 CAN 메시지들을 수신할 수 있다.

[0051] 제1 ID 추출부(113)는 순차적으로 수신된 CAN 메시지들 각각을 송신한 ECU의 ID, 즉 송신 ID를 추출할 수 있다. 제1 ID 추출부(113)은 ID 시퀀스를 출력할 수 있다.

[0052] 정상 패턴 생성부(115)는 제1 ID 추출부(113)로부터 출력된 ID 시퀀스로부터 소정의 패턴, 예컨대 정상 패턴(또는 정상 주행 패턴)을 생성할 수 있다. 생성된 정상 패턴은 DB(150)에 저장될 수 있다.

[0053] 정상 패턴 생성부(115)의 구체적인 동작은 다음과 같다.

[0054] 우선, 정상 패턴 생성부(115)는 상기 ID 시퀀스를 미리 정해진 단위(예컨대, k(k는 2 이상의 자연수) 개의 ID를

포함하는 ID 시퀀스)로 분할 할 수 있다. 분할된 ID 시퀀스의 일 예는 도 4a(좌)에 도시되어 있다.

[0055] 다음으로, 정상 패턴 생성부(115)는 서열 정렬(Sequence Alignment) 기법, 구체적으로는 다중 서열 정렬(Multiple Sequence Alignment) 기법을 이용하여 분할된 ID 시퀀스들 각각을 재정렬할 수 있다. 서열 정렬된 ID 시퀀스들의 일 예는 도 4a(우)에 도시되어 있다.

[0056] 마지막으로, 정상 패턴 생성부(115)는 서열 정렬된 ID 시퀀스들로부터 소정의 패턴을 생성할 수 있다. 정상 패턴 생성부(115)는 일정 길이 구간에 속하는 패턴만 정상 패턴으로 생성할 수 있다. 상기 일정 길이 구간이란 패턴의 포함되어야 하는 길이를 의미할 수 있다. 추출된 패턴의 일 예는 도 4b(우)에 도시되어 있다.

[0057] 이상과 같이, 정상 패턴 생성부(115)는 상기 과정을 반복 수행함으로써 복수개의 정상 패턴들을 생성할 수 있다.

[0059] 이상 탐지부(130)는 제2 메시지 수신부(131), 제2 ID 추출부(133), 및 유사도 계산부(135)를 포함한다.

[0060] 제2 메시지 수신부(131)는 통신 시스템(10) 내에서 순차적으로 발생하는 CAN 메시지들을 수신할 수 있다. 제1 메시지 수신부(131)는 통신 시스템(10)의 버스(12)를 통하여 CAN 메시지들을 수신하거나 OBD-2 단자를 통하여 CAN 메시지들을 수신할 수 있다.

[0061] 제2 ID 추출부(133)는 순차적으로 수신된 CAN 메시지들 각각을 송신한 ECU의 ID, 즉 송신 ID를 추출할 수 있다. 제2 ID 추출부(133)는 ID 시퀀스를 출력할 수 있다.

[0062] 유사도 계산부(135)는 제2 ID 추출부(133)로부터 출력된 ID 시퀀스와 DB(150)에 저장되어 있는 적어도 하나의 정상 패턴 사이의 유사도를 계산하고, 계산된 유사도에 따라 차량의 이상 유무를 판단할 수 있다. 상기 유사도는 편집 거리(edit distance)를 의미할 수 있다. 상기 편집 거리는 입력 문자열과 비교 문자열이 동일해지기 위해서 필요한 연산(수정, 삽입 또는 삭제)의 횟수를 의미하며, 거리(distance)라고도 한다. 연산의 횟수가 적을수록(즉, 거리(distance)가 낮을수록) 유사하다(유사도가 높다)고 정의될 수 있다.

[0063] 유사도 계산부(135)의 구체적인 동작은 다음과 같다.

[0064] 우선, 유사도 계산부(135)는 미리 정해진 개수만큼의 ID를 포함하는 ID 시퀀스를 추출한다. 실시 예에 따라 유사도 계산부(135)는 제2 ID 추출부(133)로부터 출력되는 미리 정해진 개수만큼의 ID를 포함하는 ID 시퀀스를 수신할 수도 있다.

[0065] 다음으로, 유사도 계산부(135)는 추출된 ID 시퀀스와 DB(150)에 저장되어 있는 복수의 정상 패턴들 각각과의 편집 거리(edit distance)를 계산할 수 있다. 이때, 가장 작은 값을 갖는 편집 거리를 추출된 ID 시퀀스와 정상 패턴 사이의 유사도라 할 수 있다.

[0067] 다음의 표 1은 임의의 ID 시퀀스({27, 17})와 임의의 정상 패턴({31, 17, 52, 41}) 사이의 편집 거리를 계산하는 일 예를 보여준다.

표 1

[0068]

횟수	연산 유형	변경 전	변경 후	입력 시퀀스	비교 시퀀스
0	초기상태			{27, 17}	{31, 17, 52, 41}
1	수정	27	31	{31, 17}	{31, 17, 52, 41}
2	삽입	없음	52	{31, 17, 52}	{31, 17, 52, 41}
3	삽입	없음	41	{31, 17, 52, 41}	{31, 17, 52, 41}

[0069] 우선, 입력 시퀀스 {27, 17}를 비교 시퀀스 {31, 17, 52, 41}와 동일하게 하기 위해서 입력 시퀀스 {27, 17}에 포함되어 있는 ID "27"을 "31"로 수정하는 연산이 필요하다.

[0070] 다음으로, 시퀀스 {31, 17}에 ID "52"와 ID "41"을 삽입하는 두 번의 삽입 연산을 수행함으로써, 입력 시퀀스 {27, 17}은 비교 대상 시퀀스인 {31, 17, 52, 41}과 동일해질 수 있다. 따라서, 입력 시퀀스 {27, 17}과 비교 대상 시퀀스 {31, 17, 52, 41} 사이의 편집 거리는 "3"이다.

[0071] 다음의 표 2는 임의의 ID 시퀀스 {27, 17, 33, 41}와 임의의 정상 패턴 {31} 사이의 편집 거리를 계산하는 일 예를 보여준다.

표 2

[0072]

횟수	연산 유형	변경 전	변경 후	입력 시퀀스	비교 시퀀스
0	초기상태			{27, 17, 33, 41}	{31}
1	삭제	41	삭제	{27, 17, 33}	{31}
2	삭제	33	삭제	{27, 17}	{31}
3	삭제	17	삭제	{27}	{31}
4	수정	27	31	{31}	{31}

[0073] 입력 시퀀스 {27, 17, 33, 41}을 비교 시퀀스 {31}와 동일하게 하기 위해서 입력 시퀀스 {27, 17, 33, 41}에 포함되어 있는 ID "41", "33", 및 "17"을 삭제하는 연산을 수행한 후에 ID "27"을 "31"로 수정하는 연산이 필요하다. 따라서, 입력 시퀀스 {27, 17, 33, 41}과 비교 대상 시퀀스 {31} 사이의 편집 거리는 "4"이다.

[0074] 다음의 표 3은 임의의 ID 시퀀스 {27, 17, 33, 41}와 임의의 정상 패턴 {31, 17, 52, 41} 사이의 편집 거리를 계산하는 일 예를 보여준다.

표 3

[0075]

횟수	연산 유형	변경 전	변경 후	입력 시퀀스	비교 시퀀스
0	초기상태			{27, 17, 33, 41}	{31, 17, 52, 41}
1	수정	27	31	{31, 17, 33, 41}	{31, 17, 52, 41}
2	수정	33	52	{31, 17, 52, 41}	{31, 17, 52, 41}

[0076] 입력 시퀀스 {27, 17, 33, 41}를 비교 시퀀스 {31, 17, 52, 41}과 동일하게 하기 위해서 입력 시퀀스 {27, 17, 33, 41}에 포함되어 있는 ID "27"과 "33"을 "31"과 "52"로 수정하는 연산을 수행하여야 한다. 따라서, 입력 시퀀스 {27, 17, 33, 41}과 비교 대상 시퀀스 {31, 17, 52, 41} 사이의 편집 거리는 "2"이다.

[0078] 마지막으로, 유사도 계산부(135)는 추출된 ID 시퀀스와 DB(150)에 저장되어 있는 정상 패턴 사이의 유사도가 미리 정해진 유사도보다 작은 경우, 다시 말해 추출된 ID 시퀀스와 DB(150)에 저장되어 있는 정상 패턴 사이의 편집 거리가 미리 정해진 편집 거리보다 큰 경우, 차량의 상태를 "비정상 상태"로 결정할 수 있다. 또한, 실시 예에 따라, 유사도 계산부(135)는 차량의 상태를 운전자에게 알리기 위하여 도시되지 않았으나 탐지 장치(100)에 포함되거나 탐지 장치(100)와는 별도로 구비된 디스플레이 장치 또는 스피커를 통하여 알림 메시지를 출력하거나 알림음을 출력할 수 있다.

[0080] 도 3에 도시된 탐지 장치(100)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 전문가는 용이하게 추론할 수 있을 것이다.

[0081] 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.

[0083] 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

[0085] 10 : 통신 시스템

100 : 탐지 장치

110 : 패턴 생성부

111 : 제1 메시지 수신부

113 : 제1 ID 추출부

115 : 정상 패턴 생성부

130 : 이상 탐지부

131 : 제2 메시지 수신부

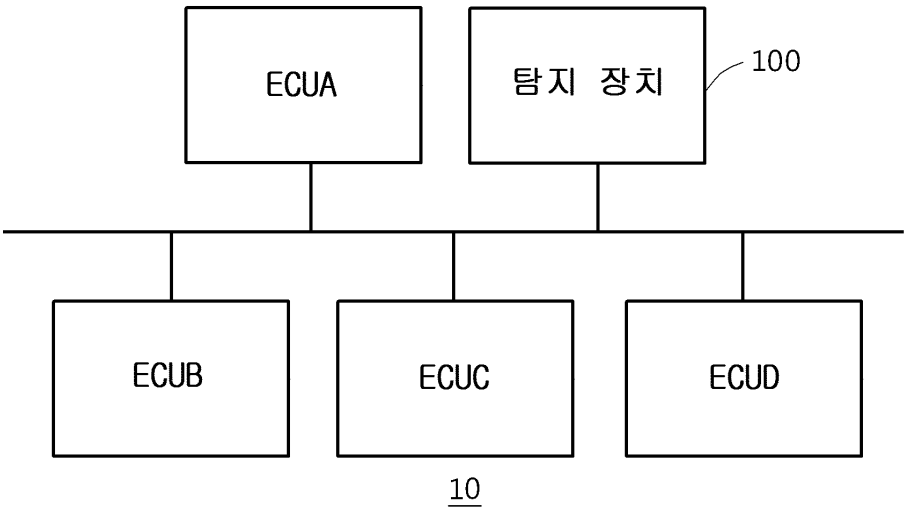
133 : 제2 ID 추출부

135 : 유사도 계산부

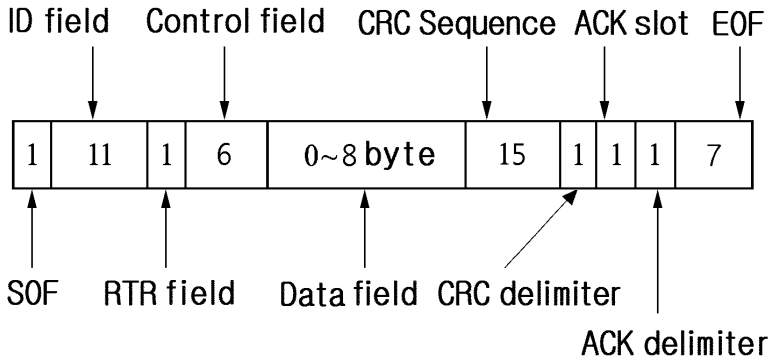
150 : DB

도면

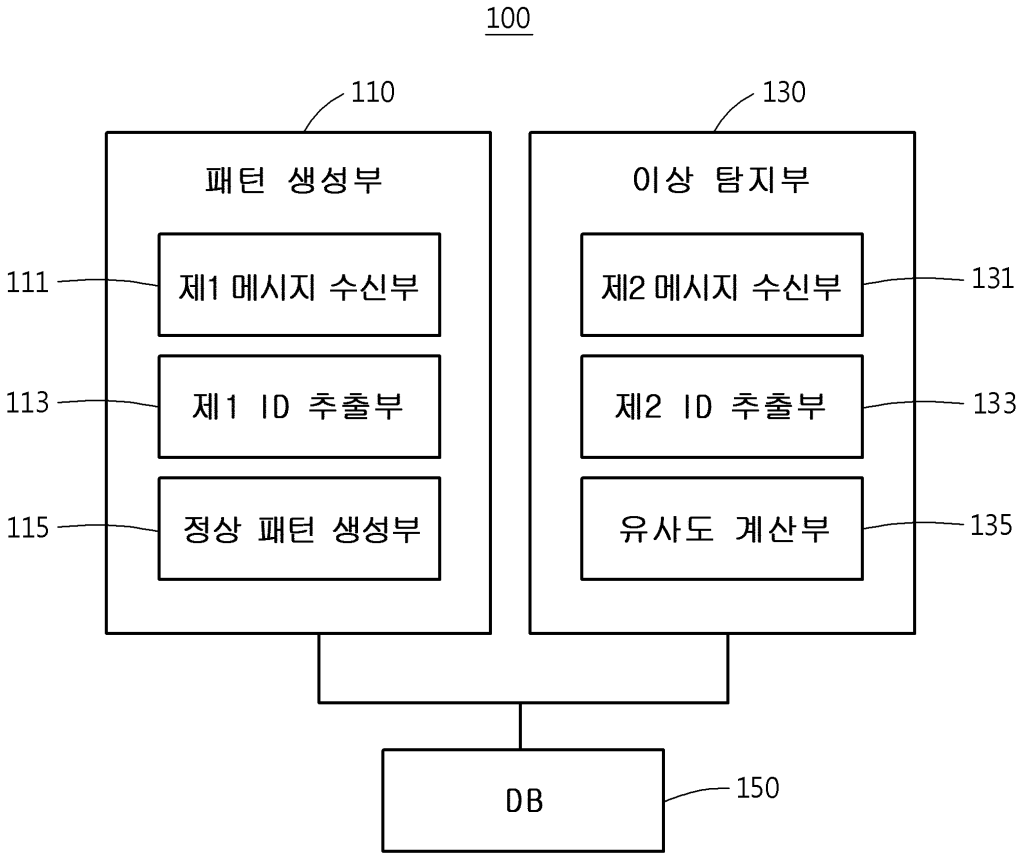
도면1



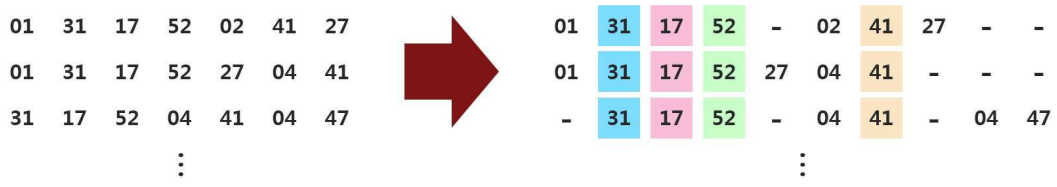
도면2


ID field
Control field
CRC Sequence
ACK slot
EOF
1
11
1
6
0~8 byte
15
1
1
1
7
SOF
RTR field
Data field
CRC delimiter
ACK delimiter

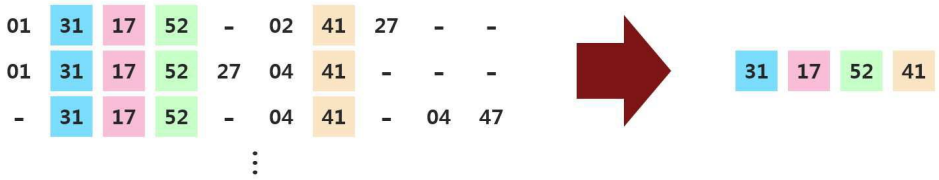
도면3


100
110
130
패턴 생성부
이상 탐지부
111
제1 메시지 수신부
131
제2 메시지 수신부
113
제1 ID 추출부
133
제2 ID 추출부
115
정상 패턴 생성부
135
유사도 계산부
DB
150

도면4a


01 31 17 52 02 41 27
01 31 17 52 27 04 41
31 17 52 04 41 04 47
01 31 17 52 - 02 41 27 - -
01 31 17 52 27 04 41 - - -
- 31 17 52 - 04 41 - 04 47

도면4b


01 31 17 52 - 02 41 27 - -
01 31 17 52 27 04 41 - - -
- 31 17 52 - 04 41 - 04 47
31 17 52 41