



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0067446
(43) 공개일자 2018년06월20일

(51) 국제특허분류(Int. Cl.)
H04L 12/40 (2006.01) H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 12/40104 (2013.01)
H04L 63/1416 (2013.01)
(21) 출원번호 10-2017-0169765
(22) 출원일자 2017년12월11일
심사청구일자 2017년12월11일
(30) 우선권주장
1020160167497 2016년12월09일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
한미란
서울시 성북구 안암동 고려대학교 자연계 캠퍼스 로봇융합관 313호
박병일
경기도 고양시 일산서구 킨텍스로 456, 103동 501호(일산동 후곡마을1단지아파트)
김휘강
서울특별시 서초구 태봉로2길 65 404동 302호 (우면동, 네이처힐4단지)
(74) 대리인
김동용, 김홍석

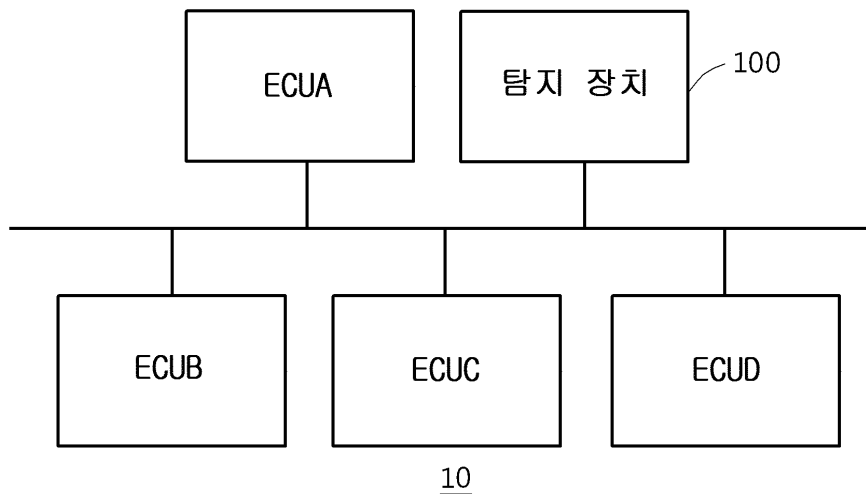
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 해저드 모델 기반의 차량 네트워크 이상 징후 탐지 장치

(57) 요약

차량의 이상 징후 탐지 장치가 개시된다. 상기 탐지 장치는 차량 네트워크에서 순차적으로 발생하는 복수의 메시지들을 수신하는 메시지 수신부, 상기 복수의 메시지들 각각의 ID를 추출하는 ID 추출부, 추출된 복수의 ID들을 이용하여 ID 별 구간 생존율을 산출하는 생존율 산출부 및 산출된 구간 생존율에 기초하여 이상 징후 유무를 판단하는 이상 징후 탐지부를 포함한다.

대표도 - 도1



(52) CPC특허분류
H04L 2012/40273 (2013.01)

명세서

청구범위

청구항 1

차량 네트워크에서 순차적으로 발생하는 복수의 메시지들을 수신하는 메시지 수신부;
상기 복수의 메시지들 각각의 ID를 추출하는 ID 추출부;
추출된 복수의 ID들을 이용하여 ID 별 구간 생존율을 산출하는 생존율 산출부; 및
산출된 구간 생존율에 기초하여 이상 징후 유무를 판단하는 이상 징후 탐지부를 포함하는 차량의 이상 징후 탐지 장치.

청구항 2

제1항에 있어서,
상기 차량 네트워크는 CAN(Controller Area Network)이고,
상기 복수의 메시지들 각각은 CAN 메시지인,
차량의 이상 징후 탐지 장치.

청구항 3

제1항에 있어서,
상기 생존율 산출부는 상기 복수의 ID들을 미리 정해진 구간으로 분할하고,
분할된 구간 각각에서 미리 정해진 적어도 하나의 ID의 구간 생존율을 산출하는,
차량의 이상 징후 탐지 장치.

청구항 4

제3항에 있어서,
상기 생존율 산출부는 분할된 각 구간이 동일한 시간 주기를 갖도록 상기 복수의 ID들을 분할하는,
차량의 이상 징후 탐지 장치.

청구항 5

제3항에 있어서,
상기 생존율 산출부는 분할된 각 구간에 동일한 개수의 ID가 포함되도록 상기 복수의 ID들을 분할하는,
차량의 이상 징후 탐지 장치.

청구항 6

제4항 또는 제5항에 있어서,

상기 이상 징후 탐지부는 산출된 구간 생존율이 미리 정해진 범위를 벗어나는 경우에 이상 징후가 발생한 것으로 판단하는,

차량의 이상 징후 탐지 장치.

청구항 7

제1항에 있어서,

상기 차량 네트워크는 CAN FD(Flexible Data), FlexRay, LIN(Local Interconnect Network) 또는 MOST(Media Oriented Systems Transport)인,

차량의 이상 징후 탐지 장치.

발명의 설명

기술 분야

[0001] 본 발명은 차량 또는 차량 네트워크의 이상 징후 탐지 장치에 관한 것으로, 특히 해저드 모델을 이용하여 차량 네트워크에서 발생하는 메시지의 ID별 구간 생존율에 기초하여 이상 징후 여부를 판단할 수 있는 이상 징후 탐지 장치에 관한 것이다.

배경 기술

[0003] 차량에 대한 기술들이 ICT(Information and Communication Technologies)와 융합되면서 커넥티드카(connected Car) 환경으로 변화하고 있다. 또한, 자율주행에 대한 기술들이 빠르게 발전하면서 차량 보안에 대한 중요성이 증가하고 있다. 차량에 탑재되어 있는 많은 부품 및 장치들이 전자적으로 제어되는 ECU(Electronic Control Unit)에 연결되며, 이를 통해 효율적으로 차량이 제어되며 관리되고 있다. 그러나, 이러한 ECU는 차량 내부의 다른 센서 및 부품들과 CAN(Controller Area Network), LIN(Local Interconnect Network) 등의 다양한 통신 프로토콜을 통해 메시지들을 주고받기 때문에 이에 대한 보안 조치가 필요하다.

[0004] 특히, 자율주행 자동차의 경우 일반 차량과는 다르게 운전자의 개입이 적으므로 외부 및 내부에서 발생 가능한 공격에 대한 연구가 필요하다. 자율주행 자동차의 경우 외부 장애물에 대해 스스로 감지하고 회피하는 기술은 상당 부분 개발되고 있고, 이를 더 발전시켜 나가고 있는 중이다. 또한, 다양한 방법으로 도로에 있는 장애물 및 갑작스럽게 들어오는 차량들을 파악하여 이를 미리 회피하는 기술도 개발하고 있는 중이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허 제1998-0038543호 (1998.08.05. 공개)
(특허문헌 0002) 대한민국 공개특허 제1994-0011939호 (1994.06.22. 공개)
(특허문헌 0003) 대한민국 공개특허 제2016-0014026호 (2016.02.05. 공개)

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 차량의 이상 징후를 탐지하기 위해 각각의 CAN ID 해석이 요구되지 않는 CAN ID에 비종속적인 이상 징후 탐지 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

- [0009] 본 발명의 실시 예에 따른 차량의 이상 징후 탐지 장치는 차량 네트워크에서 순차적으로 발생하는 복수의 메시지들을 수신하는 메시지 수신부, 상기 복수의 메시지들 각각의 ID를 추출하는 ID 추출부, 추출된 복수의 ID들을 이용하여 ID 별 구간 생존율을 산출하는 생존율 산출부 및 산출된 구간 생존율에 기초하여 이상 징후 유무를 판단하는 이상 징후 탐지부를 포함한다.

발명의 효과

- [0011] 본 발명에 의한 경우, 차량의 제조사와 제조 연도에 따라 다르게 구성되는 CAN 메시지 해석의 어려움을 해결하여, CAN ID 해석이 요구되지 않는 CAN ID에 비종속적인 이상 징후 탐지 기법을 제공할 수 있다.
- [0012] 또한, 차량의 CAN 네트워크에 대한 ID별 생존율을 구하는 것이기 때문에 ID를 가지는 통신 프로토콜의 경우 사용이 가능하며, CAN 네트워크 통신을 사용하는 차량의 경우 차량의 종류에 관계없이 이상 징후를 탐지할 수 있는 효과가 있다.
- [0013] 또한, 이를 통해 의사결정에 필요한 정보들을 신속하게 처리하고, 운전자 및 동승자에게 현재 차량이 정상인지 비정상인지에 대한 알림 및 차량 관제센터나 차량 관제 회사에 알림을 통해서 현재 차량의 이상 상태 여부에 대한 보다 구체적인 대응이 가능하도록 할 수 있다.

도면의 간단한 설명

- [0015] 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 탐지 장치의 기능 블록도이다.
- 도 3은 도 2에 도시된 생존율 산출부에 의해 분할된 구간을 설명하기 위한 도면으로, 도 3a는 정상적인 주행에서의 발생하는 CAN ID를, 도 3b는 비정상적인 주행에서 발생하는 CAN ID를 도시한다.
- 도 4는 청크에 포함되는 CAN ID의 개수를 달리하였을 경우 구간 생존율 도시한 도면으로, 도 4a는 DoS 공격이 있는 경우의 구간 생존율을, 도 4b는 Fuzzing 공격이 있는 경우의 구간 생존율을, 도 4c는 RPM 공격이 있는 경우의 구간 생존율을, 도 4d는 Gear 공격이 있는 경우의 구간 생존율을 도시한다.
- 도 5는 현대자동차에서 2010년에 제작한 소나타의 CAN ID 주기를 도시한 도면이다.
- 도 6은 현대자동차의 2010년형 소나타 차량을 대상으로 공격 유형별 탐지 정확도를 측정한 결과를 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0016] 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 형태로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0017] 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.
- [0018] 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.

- [0019] 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.
- [0020] 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.
- [0021] 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.
- [0022] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.
- [0024] 본 발명은 자율주행 환경이나 차량 IoT(Internet of Things) 환경에서 발생할 수 있는 비정상적인 차량 상태를 클라이언트 측면에서 탐지하는 방법으로써, 해저드 모델(Hazard Model) 기법을 적용하여 차량 상태에 대한 안전성 여부를 결정할 수 있는 방법을 제시한다.
- [0025] 차량은 차량에 탑재된 여러 차량 부품, 센서들이 서로 통신하기 위해서 CAN(Controller Area Network) 프로토콜을 이용해 통신을 수행한다. CAN 메시지들은 지속적으로 각 센서 및 부품들로부터 생성되어 ECU로 모이게 되며, 이러한 데이터들을 이용해서 차량은 그 기능을 수행해 나간다.
- [0026] 차량의 상태 정보 및 차량 제어 정보들이 CAN 네트워크를 통해서 차량 내부에 돌아다니는데, 이러한 CAN 메시지들의 이상 여부 및 공격 여부를 탐지하는 것은 차량에 대한 안전성 및 운전자의 안전을 위해 필수적인 요소이다.
- [0027] CAN 네트워크에서 전송되는 CAN 메시지는 로 데이터(raw data)의 경우 각 차량의 제조사와 제조 연도마다 상이하며, 차량 안의 부품들마다 생성 및 적용하는 부분이 다르게 구성되어 있다. 즉, 동일한 CAN ID라고 할지라도 차량에 따라 다른 기능을 수행할 수 있다.
- [0028] 특히, 자율주행 환경에서는 주행 중 발생하는 CAN 메시지 데이터가 주기적이고 반복적으로 생성될 것이며, 운전자 측면에서 볼 때 수동적이고 소극적인 주행 환경에서는 차량의 상태가 주기적으로 모니터링되고, 이상 징후를 탐지하여 알람을 해주는 즉각적인 시스템이 필요할 것이다.
- [0030] 또한, 본 발명에서는 해저드 모델(Hazard Model)을 사용하여 차량의 이상 징후를 탐지한다. 해저드 모델은 생존 기간을 분석하여 생존 함수(Survival function) 또는 생존 곡선(Survival curve)를 추정하는 통계 기법이며, 사건이 일어나는 시간까지의 기간을 대상으로 분석하는 방법이다. 생존 기간과 현재 상태 정보가 필요하며, 여기서 말하는 현재 상태란 생존 기간을 측정한 시점에서 측정하고자 하는 대상이 생존해 있는지 아닌지를 확인하는 것이다.
- [0031] 생존 함수 또는 생존 곡선을 추정하는 방법은 Life table method, Kaplan-Meier, Cox 비례위험 모델로 세 가지 방법이 존재하지만, 본 발명에서는 Kaplan-Meier 개념을 적용하여 이상 징후를 탐지한다.
- [0032] Kaplan-Meier 추정 방법을 통해서 관찰 기간(시간 혹은 청크 단위)의 순서대로 자료를 정리한 뒤 관찰 대상 수 중 생존자수의 비율로 수학적 1과 같은 구간 생존율($P(t)$)을 측정할 수 있다.

수학적식 1

$$P(t) = \frac{t\text{시점에서 생존 대상 수}}{t\text{시점에서 관찰 대상 수}}$$

차량이 정상적으로 주행하고 있는 상태인 경우, 주행 시에 발생하는 개별 CAN ID의 생존 확률은 대부분 일정하게 유지되지만, 차량 주행 중 DoS(Denial of Service) 공격, Fuzzing 공격, Spoofing 공격이 발생했을 경우에는 데이터의 생존 확률이 변화하는 패턴이 발생한다.

CAN 프로토콜을 사용하는 차량 내부에서 발생 가능한 공격 유형은 표 1과 같다.

표 1

공격 유형	내용
DoS	· DoS 공격은 차량 내 CAN 버스에 할당된 자원을 모두 점유하여 차량 내 ECU 사이의 통신을 제한하고 정상적인 주행을 방해하는 공격 차량의 본래 기능을 수행하기 위한 CAN 메시지의 전달을 지연시키거나 차단시킴 · CAN 메시지의 Arbitration ID를 0 혹은 대상 차량에서 사용되는 값보다 낮게 설정하여 CAN 메시지를 무제한으로 차량에 주입
Fuzzing Attack	· CAN 메시지에 포함될 Arbitration ID, data, DLC를 매번 임의로 결정하여 차량으로 송신 · Injection messages of totally random CAN ID and DATA values every 0.5 milliseconds.
Spoofing Attack (RPM/Gear)	· Injecting messages of certain CAN ID related to RPM/gear information every 1 millisecond.

도 1은 본 발명의 일 실시 예에 따른 시스템을 도시한다.

도 1을 참조하면, 차량 시스템일 수 있는 시스템(10)은 복수의 ECU(Electronic Control Unit, ECUA 내지 ECU D)들과 탐지 장치(100)를 포함한다. 각각의 ECU들(ECUA 내지 ECU D) 또는 탐지 장치(100)는 CAN(Controller Area Network)를 통해 통신할 수 있다. 즉, 각각의 ECU들(ECUA 내지 ECU D) 또는 탐지 장치(100)는 CAN 버스에 CAN 메시지를 브로드캐스팅함으로써 메시지 또는 데이터를 주고 받을 수 있다. 또한, 시스템(10)에 포함되는 ECU의 개수에 본 발명의 권리범위가 제한되는 것이 아님은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명할 것이다.

탐지 장치(100)는 CAN 버스를 통해 브로드캐스트되는 CAN 메시지들을 수신하고, CAN 메시지들 각각의 CAN ID를 이용하여 차량의 이상 징후를 탐지할 수 있다. 도 1에는 ECU로 구현된 탐지 장치(100)가 도시되어 있으나, 실시 예에 따라 탐지 장치(100)는 별도의 장치로 구현될 수 있고, OBD-2(On Board Diagnostics-2) 단자를 통해 CAN 메시지를 수신할 수도 있다.

또한, 시스템(10)은 CAN 네트워크 시스템에 제한되는 것은 아니며, 실시 예에 따라 시스템(10)에서 사용되는 통신 프로토콜 또는 네트워크는 플렉스레이(FlexRay), 린(Local Interconnect Network, LIN), CAN FD(Flexible Data) 또는 모스트(Media Oriented Systems Transport, MOST)일 수도 있다. 이 경우, 탐지 장치(100)는 각각의 네트워크에서 발생하는 메시지의 ID를 추출함으로써 차량의 이상 징후 또는 차량 네트워크의 이상 징후를 탐지할 수 있다.

도 2는 도 1에 도시된 탐지 장치의 기능 블록도이다.

도 1과 도 2를 참조하면, 탐지 장치(100)는 메시지 수신부(110), ID 추출부(130), 생존율 산출부(150) 및 이상 징후 탐지부(170)를 포함한다. 실시 예에 따라 탐지 장치(100)는 저장부(190)를 더 포함할 수 있다.

메시지 수신부(110) CAN 버스를 통해 브로드캐스트되는 복수의 CAN 메시지들을 수신할 수 있다. 메시지 수신부(110)는 CAN 버스에 직접 접속되어 상기 복수의 CAN 메시지들을 수신하거나, OBD-2 단자를 통해 상기 복수의

CAN 메시지들을 수신할 수 있다. 메시지 수신부(110)에 의해 수신된 복수의 CAN 메시지들을 저장부(190)에 저장될 수 있다.

- [0047] ID 추출부(130)는 메시지 수신부(110)에 의해 수신된 복수의 메시지들 또는 저장부(190)에 저장된 복수의 메시지들 각각의 CAN ID를 추출할 수 있다. ID 추출부(130)에 의해 추출된 ID는 저장부에 저장될 수 있다.
- [0049] 생존율 산출부(150)는 순차적으로 발생한 CAN ID 또는 순차적으로 브로드캐스팅된 CAN ID를 미리 정해진 구간으로 분할하고, 분할된 구간에서 미리 정해진 적어도 하나의 CAN ID 각각의 구간 생존율($P(t)$)을 산출할 수 있다. 생존율 산출부(150)에 의해 산출된 각 CAN ID의 구간 생존율($P(t)$)은 저장부(190)에 저장될 수 있다. 생존율 산출부(150)의 구체적인 동작은 후술하기로 한다.
- [0051] 이상 징후 탐지부(170)는 산출된 CAN ID 각각의 구간 생존율($P(t)$)에 기초하여 차량의 이상 징후 여부(또는 차량 네트워크의 이상 징후 여부)를 탐지할 수 있다. 구체적으로, CAN ID의 미리 정해진 범위를 벗어나는 경우 차량에 이상 징후가 발생한 것으로 판단할 수 있다. 일 예로, CAN ID "4f0"의 구간 생존율이 0.1~0.3을 벗어나는 경우 이상 징후로 판단할 수 있다.
- [0052] 또한, 이상 징후 탐지부(170)는 차량에 이상 징후가 발생한 경우 알림 메시지를 전송할 수도 있다. 실시 예에 따라 이상 징후 탐지부는 상기 알림 메시지를 CAN 버스를 통해 브로드캐스트하거나, 별도의 유무선 통신망을 통하여 별도의 서버로 송신할 수도 있다. 또한, 개별 CAN ID의 구간 생존율에 기초하여 차량의 이상 징후를 판단하기 때문에, 어떤 CAN ID에서 문제가 발생했는지에 대해서 구체적으로 경고 메시지를 제공할 수 있다.
- [0054] 저장부(190)에는 메시지 수신부(110)에 의해 수신된 복수의 CAN 메시지들, ID 추출부(130)에 의해 추출된 복수의 CAN ID들 및/또는 생존율 산출부(150)에 의해 산출된 각 CAN ID의 구간 생존율이 저장될 수 있다.
- [0056] 도 2에 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 전문가가 용이하게 추론할 수 있을 것이다.
- [0057] 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.
- [0059] 도 3은 도 2에 도시된 생존율 산출부에 의해 분할된 구간을 설명하기 위한 도면으로, 도 3a는 정상적인 주행에서의 발생하는 CAN ID를, 도 3b는 비정상적인 주행에서 발생하는 CAN ID를 도시한다.
- [0060] 도 1 내지 도 3을 참조하면, 생존율 산출부(150)는 순차적으로 발생(또는 브로드캐스팅 또는 수신)되는 복수의 CAN 메시지(또는 CAN ID)가 미리 정해진 개수만큼 포함되도록 청크를 설정할 수 있다. 여기서 말하는 청크는 미리 정해진 CAN ID가 포함되는 구간을 의미하는 것으로 각 청크별 마다 시간 주기는 상이할 수 있다.
- [0061] 일 예로, 생존율 산출부(150)는 20개의 CAN ID가 포함되도록 구간, 즉 청크를 설정할 수 있다. 이때, 도 3에서 각 청크는 CAN ID를 중복하여 포함하지 않도록 설정되었으나, 실시 예에 따라 임의의 청크와 이전 청크가 미리 정해진 비율 또는 미리 정해진 개수의 CAN ID를 중복하여 포함하도록 각 청크를 설정할 수도 있다.
- [0062] 다른 예로, 생존율 산출부(150)는 시간을 기준으로 구간을 설정할 수 있다. 구체적으로 생존율 산출부(150)는 $a(a$ 는 0 이상의 실수) 초를 주기로 갖도록 구간을 설정할 수 있다. 이 경우, 각 구간에 포함되는 CAN ID의 개수는 서로 상이할 수 있다. 이때에도 임의의 구간은 이전 구간과 미리 정해진 비율 또는 미리 정해진 시간이 중복

되도록 각 구간을 설정할 수도 있다.

- [0063] 또한, 생존율 산출부(150)는 각 구간에서 미리 정해진 적어도 하나의 CAN ID의 구간 생존율을 산출할 수 있다.
- [0064] 정상적인 주행의 경우(도 3a), 제1 청크(chunk1) 내지 제4 청크(chunk4)에서 CAN ID "4f0"의 구간 생존율을 다음과 같다.
- [0065] chunk1에서 CAN ID 4f0의 구간 생존율 $P(t) = 5 / 20 = 0.25$
- [0066] chunk2에서 CAN ID 4f0의 구간 생존율 $P(t) = 5 / 20 = 0.25$
- [0067] chunk3에서 CAN ID 4f0의 구간 생존율 $P(t) = 4 / 20 = 0.2$
- [0068] chunk4에서 CAN ID 4f0의 구간 생존율 $P(t) = 4 / 20 = 0.2$
- [0069] 상술한 바와 같이, 정상적인 주행에서의 CAN ID의 구간 생존율은 일정하게 유지되나, DoS와 같은 주입 공격이 이루어졌을 경우에는 이와는 다른 구간 생존율을 보인다.
- [0070] 비정상적인 주행의 경우(도 3b), 제1 청크(chunk1) 내지 제4 청크(chunk4)에서 CAN ID "4f0"의 구간 생존율은 다음과 같다.
- [0071] chunk1에서 CAN ID 4f0의 구간 생존율 $P(t) = 5 / 20 = 0.25$
- [0072] chunk2에서 CAN ID 4f0의 구간 생존율 $P(t) = 5 / 20 = 0.25$
- [0073] chunk3에서 CAN ID 4f0의 구간 생존율 $P(t) = 1 / 20 = 0.05$
- [0074] chunk4에서 CAN ID 4f0의 구간 생존율 $P(t) = 1 / 20 = 0.05$
- [0076] 도 4는 청크에 포함되는 CAN ID의 개수를 달리하였을 경우 구간 생존율 도시한 도면으로, 도 4a는 DoS 공격이 있는 경우의 구간 생존율을, 도 4b는 Fuzzing 공격이 있는 경우의 구간 생존율을, 도 4c는 RPM 공격이 있는 경우의 구간 생존율을, 도 4d는 Gear 공격이 있는 경우의 구간 생존율을 도시한다.
- [0077] 실제 차량에 가해진 공격 유형에 따라 구간 생존율이 다르게 나타나는 것을 확인하였다. 하나의 청크를 100개의 CAN ID로 구분하였을 때, 각 공격에 해당되는 CAN ID의 구간 생존율을 총 300개까지 순차적으로 측정하였다.
- [0078] 도 4a를 참조하면, CAN ID "0000"으로 DoS 공격을 시행하였을 때 CAN ID "04f0"의 생존율(빨강색)과 공격이 없을 때 CAN ID "04f0"의 생존율(회색)이 명확하게 차이남을 알 수 있다.
- [0079] 도 4b를 참조하면, Fuzzing 공격을 시행하였을 때 CAN ID "04f0"의 생존율(빨강색)과 공격이 없을 때 CAN ID "04f0"의 생존율(회색)이 명확하게 차이남을 알 수 있다.
- [0080] 도 4c를 참조하면, CAN ID "0316"으로 RPM 공격을 시행하였을 때 CAN ID "0316"의 생존율(빨강색)과 공격이 없을 때 CAN ID "0316"의 생존율(회색)이 명확하게 차이남을 알 수 있다.
- [0081] 도 4d를 참조하면, CAN ID "0329"으로 Gear 공격을 시행하였을 때 CAN ID "0329"의 생존율(빨강색)과 공격이 없을 때 CAN ID "0329"의 생존율(회색)이 명확하게 차이남을 알 수 있다.
- [0082] CAN 메시지 주기는 CAN ID 번호가 낮을수록 우선 순위가 높다. 우선 순위가 높다는 것은 브로드캐스트(broadcast) 지향의 통신 프로토콜인 CAN에서 우선 순위가 높은 CAN ID가 먼저 실행이 된다는 의미이다. 현대자동차에서 2010년에 제작한 소나타의 CAN ID 주기를 도시한 도 5를 살펴보면, 일부 CAN ID(690, 5a0, 5a2, 5f0 등)를 제외하고 주기가 매우 일정함을 알 수 있다. 이러한 CAN ID 주기의 일정성에 착안하여 본 발명의 발명자는 CAN ID의 구간 생존율만을 가지고 차량의 이상 징후를 탐지할 수 있는 방안을 제시하였다.
- [0083] 현대자동차의 2010년형 소나타 차량을 대상으로 공격 유형별 탐지 정확도를 측정한 결과를 도시한 도 6을 참조하면, 본 발명에 의한 경우 매우 높은 정확도를 제공할 수 있다.
- [0085] 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.

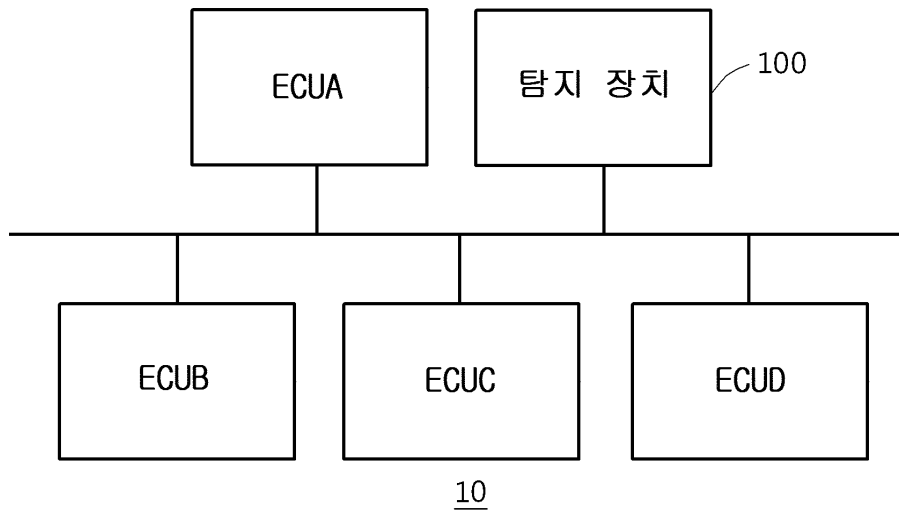
부호의 설명

[0087]

- 10 : 시스템
- 100 : 탐지 장치
- 110 : 메시지 수신부
- 130 : ID 추출부
- 150 : 생존율 산출부
- 170 : 이상 징후 탐지부
- 190 : 저장부

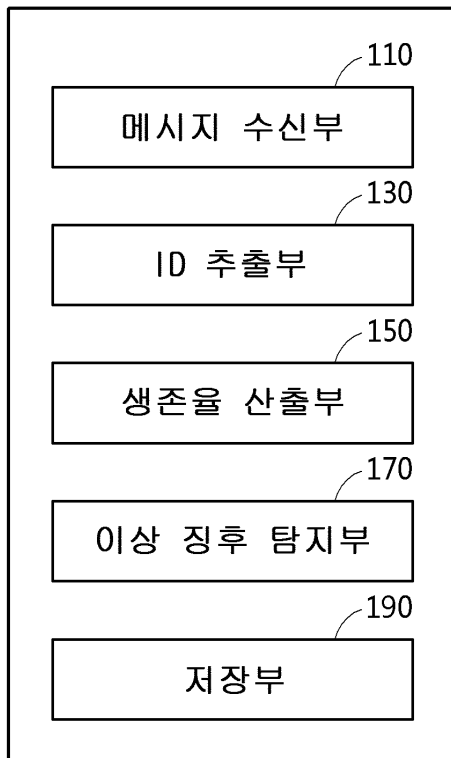
도면

도면1



도면2

100



도면3a

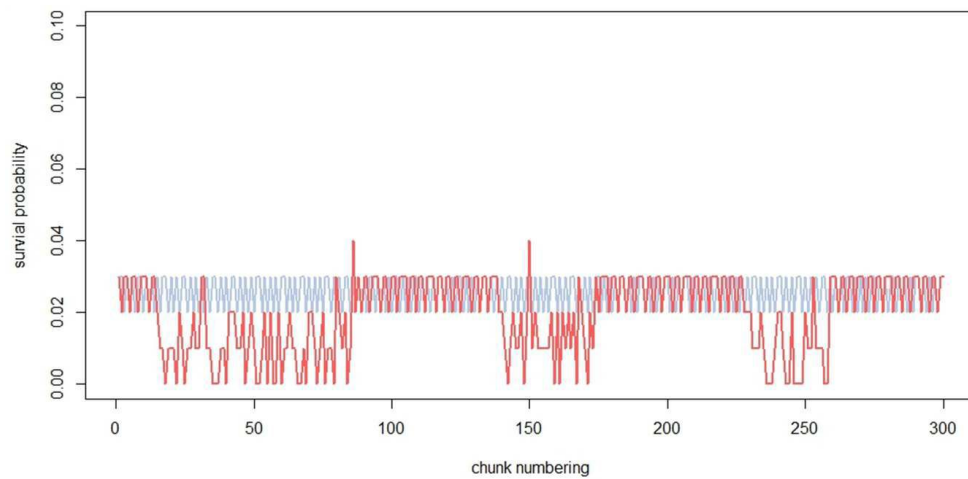
	time →			
	chunk1	chunk2	chunk3	chunk4
no	chunk1	chunk2	chunk3	chunk4
1	5f0	4f0	5f0	690
2	4f0	5f0	690	4f0
3	5f0	690	4f0	690
4	690	4f0	690	4f0
5	4f0	690	4f0	130
6	690	4f0	130	131
7	4f0	130	131	140
8	130	131	140	4f0
9	131	140	4f0	130
10	140	4f0	130	131
11	4f0	130	131	140
12	130	131	140	5f0
13	131	140	5f0	4f0
14	140	5f0	4f0	130
15	5f0	4f0	130	131
16	4f0	130	131	140
17	130	131	140	430
18	131	140	430	4b1
19	140	430	4b1	1f1
20	430	4b1	1f1	153

도면3b

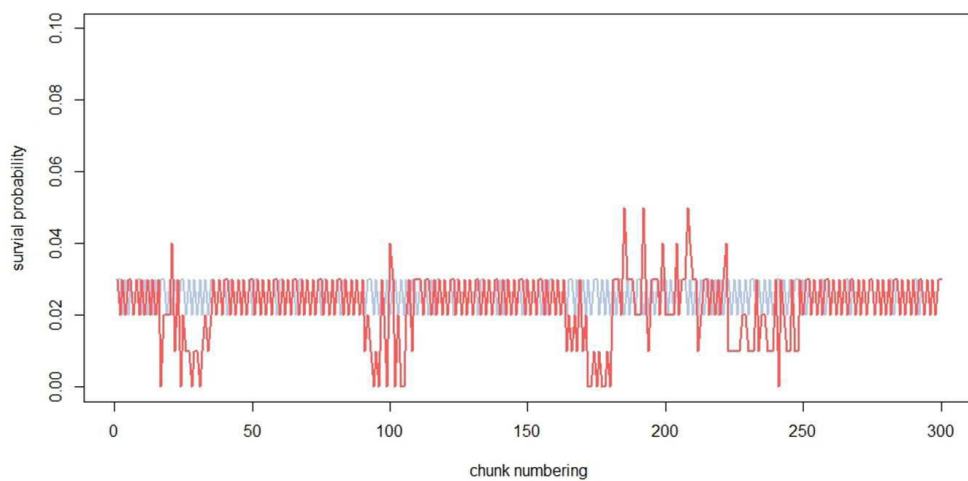
	time			
	chunk1	chunk2	chunk3	chunk4
no	chunk1	chunk2	chunk3	chunk4
1	5f0	4f0	5f0	690
2	4f0	5f0	690	4f0
3	5f0	690	4f0	690
4	690	4f0	690	2ab
5	4f0	690	2ab	2ab
6	690	4f0	2ab	2ab
7	4f0	130	2ab	2ab
8	130	131	2ab	2ab
9	131	140	2ab	2ab
10	140	4f0	2ab	2ab
11	4f0	130	2ab	2ab
12	130	131	2ab	2ab
13	131	140	2ab	2ab
14	140	5f0	2ab	2ab
15	5f0	4f0	2ab	2ab
16	4f0	130	2ab	2ab
17	130	131	2ab	2ab
18	131	140	2ab	130
19	140	430	130	131
20	430	4b1	131	140

DoS 주입 공격

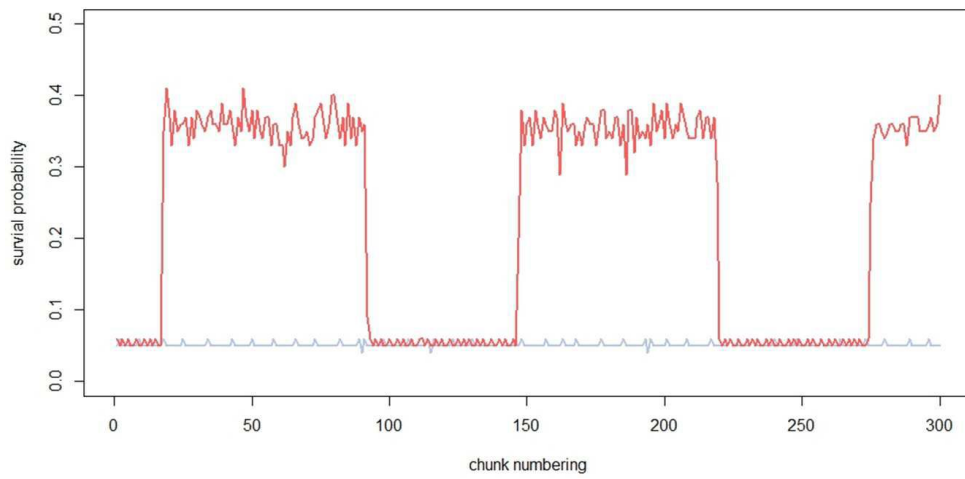
도면4a



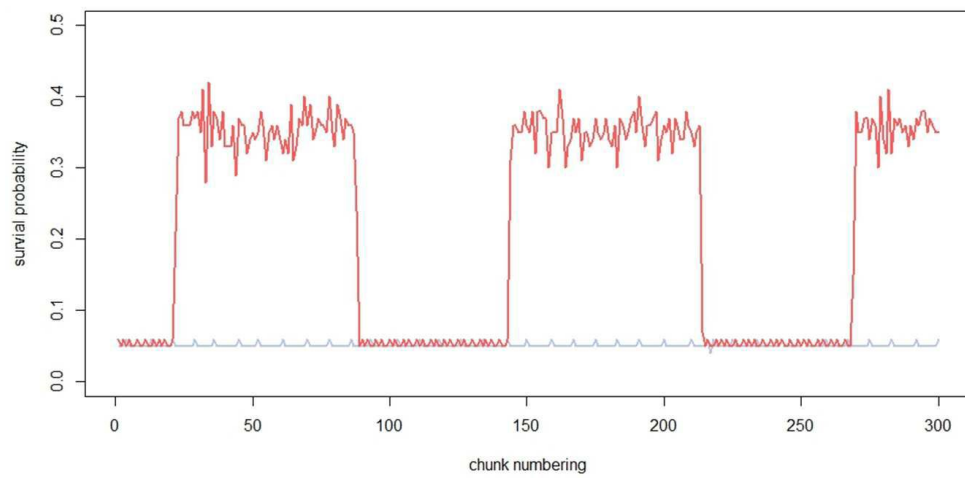
도면4b



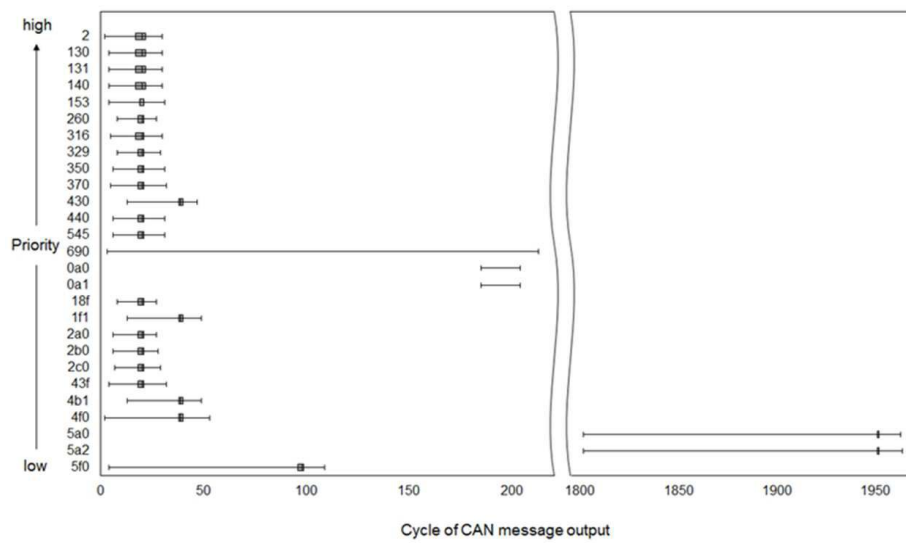
도면4c



도면4d



도면5



도면6

Attack Type	TP + FN = 1		FP + TN = 1		검색된 자료들 중 관련 있는 자료들의 비율		
	True Positive	False Negative	False Positive	True Negative	Accuracy	Precision	Recall
DoS Attack	0.985	0.015	0.052	0.947	0.959	0.890	0.985
Fuzzing Attack	0.986	0.014	0.039	0.945	0.970	0.930	0.986
Spoofing Attack RPM	0.987	0.013	0.027	0.973	0.980	0.968	0.987
Spoofing Attack Gear	0.987	0.013	0.030	0.970	0.977	0.961	0.987

↓ 이싱징후를 이싱징후라고 탐지한 비율 (탐지률) ↓ 정상을 이싱징후라고 탐지한 비율 (오탐률) ↓ 정확도 ↓ 관련 있는 자료들 중에서 실제로 검색된 자료들의 비율